R G B WH GR BL Grey Scale #13 C M Y K
DANES PICTA .COM
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19

AKADEMIA
OBRONY NARODOWEJ

Mgr inż. Andrzej WÓJCIK

OCHRONA OBIEKTÓW WOJSKOWYCH NA POTRZEBY OBRONNOŚCI PAŃSTWA

Rozprawa doktorska

60943

BIBLIOTEKA GŁÓWNA AKADEMII OBRONY NARODOWEJ Nr ewid.

Biblioteka Główna
Akademii Obrony Narodowej
V/4128
05-004128-001-0

WARSZAWA 1999

Colour Chart #13
Blue Cyan Green Yellow Red Magenta White 3/Color Black
Inches Centimetres
DANES PICTA .COM

AKADEMIA
OBRONY NARODOWEJ

Mgr inż. Andrzej WÓJCIK

OCHRONA OBIEKTÓW WOJSKOWYCH NA POTRZEBY OBRONNOŚCI PAŃSTWA

Rozprawa doktorska

60943

Biblioteka Główna
Akademii Obrony Narodowej
S/4128
05-004128-001-0

WARSZAWA 1999

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ STRATEGICZNO-OBRONNY

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 60943
II
Akademii Obrony Narodowej

mgr inż. Andrzej WÓJCIK

OCHRONA OBIEKTÓW WOJSKOWYCH NA POTRZEBY OBRONNOŚCI PAŃSTWA

ROZPRAWA DOKTORSKA

Opracowano pod kierunkiem naukowym
gen. bryg. prof. dr. hab. Michała KRAUZE

WARSZAWA Czerwiec 1999

BIBLIOTEKA GŁÓWNA
Nr ewid. 9/4128
Archiwum Zbiorów Zwartych

SPIS TREŚCI

WSTĘP 5

1. PODSTAWY METODOLOGICZNE 8

1.1. Problematyka rozprawy 8
1.2. Cel rozprawy 11
1.3. Problemy badawcze 11
1.4. Obszar badań 11
1.5. Hipotezy badawcze 12
1.6. Wybrane metody badawcze 13
1.7. Krytyczna analiza literatury przedmiotu 15

2. SYSTEM OBRONNY PAŃSTWA - OCENA WRAŻLIWOŚCI NA ZAGROŻENIA .. 21

2.1. Charakterystyka wybranych elementów systemu obronnego państwa 21
2.2. Źródła i formy zagrożenia elementów systemu obronnego państwa 34
2.3. Wpływ zagrożeń na funkcjonowanie systemu obronnego państwa 36
Wnioski 51

3. ANALIZA PORÓWNAWCZA SYSTEMÓW SYGNALIZACJI ZAGROŻEŃ I OCHRONY OBIEKTÓW WOJSKOWYCH WYKORZYSTYWANYCH W POLSCE I WYBRANYCH PAŃSTWACH NATO 53

3.1. Potrzeby systemu obronnego państwa w zakresie ochrony obiektów wojskowych 53
3.2. Istniejące rozwiązania w zakresie ochrony obiektów wojskowych oraz ogólna charakterystyka wybranych systemów ochrony 56
3.2.1. Ocena stanu krajowych rozwiązań ochrony obiektów wojskowych 72
3.2.2. Rozwiązania w zakresie ochrony obiektów wojskowych stosowane w niektórych państwach NATO 75
3.3. Wymagania stawiane systemom ochrony obiektów wojskowych w kontekście członkostwa Polski w NATO 83
Wnioski 88

4. MODEL SYSTEMU OCHRONY OBIEKTÓW WOJSKOWYCH 90

4.1. Projektowanie systemu ochrony obiektu 90
4.1.1. Czynniki decydujące o doborze elementów systemu ochrony obiektu 106
4.1.2. Określenie stanu bezpieczeństwa obiektu 113
4.2. Modelowanie systemu ochrony obiektu 119
4.3. Weryfikacja modelu systemu ochrony obiektu 150
Wnioski 162

ZAKOŃCZENIE 165

WYKAZ TABEL 168

WYKAZ RYSUNKÓW I SCHEMATÓW 168

WYKAZ WYKRESÓW I MODELI GRAFICZNYCH 169

SPIS ZAŁĄCZNIKÓW 170

BIBLIOGRAFIA 171

ZAŁĄCZNIKI – w odrębnym opracowaniu

WSTĘP

Burzliwy rozwój elektroniki oraz powszechne jej zastosowanie w życiu społecznym i gospodarczym, spowodowało powstanie nowej dziedziny teoretycznej i praktycznej zajmującej się systemami sygnalizacji zagrożeń. Systemy te przeznaczone są do ochrony mienia i życia ludzkiego. Ich istota działania polega na sygnalizowaniu różnorodnych zagrożeń przy pomocy odpowiednich urządzeń elektronicznych. Obszar zastosowań tych systemów jest bardzo rozległy i obejmuje m.in. systemy informujące o zagrożeniach przemysłowych, ekologicznych, radiacyjnych i chemicznych.

Dostęp do informacji stał się kluczem do dobrobytu i rozwoju. Informacja jest w swojej istocie dziedziną przenikającą wszelkie obszary działalności ludzkiej. Wzrost ilości informacji i środków ich przekazu spowodował, że informacja obok materii i energii traktowana jest współcześnie jako trzeci podstawowy element otaczającej nas rzeczywistości.

Istota kierowania państwem, zarządzania gospodarką narodową i organizacji bytu społecznego polega między innymi na sprawnym przesyłaniu sygnałów o zagrożeniu. Staje się to możliwe dzięki stosowaniu coraz to nowocześniejszych środków technicznych. W ciągu kilku lat rozwój telekomunikacji uległ przyspieszeniu, dzięki rozwojowi nowoczesnej technologii opartej na technice komputerowej. Umożliwiło to szybkie wdrożenie postępu technicznego, poszerzenie oferty świadczonych usług, stworzyło dynamiczny rynek, wpłynęło na skrócenie okresu amortyzacji realizowanych inwestycji, itp.

Od efektywności działania systemu ochrony obiektów[1] zależy skuteczność systemu obronnego państwa i jakość dowodzenia wojskami. Celem podstawowym obrony Rzeczpospolitej Polskiej jest zachowanie suwerenności, niepodległości i integralności państwa. Osiąga się to przez przygotowanie sił zbrojnych, rozbudowę i utrzymanie infrastruktury obronnej państwa, odpowiednie przygotowanie obronne społeczeństwa, a ponadto poprzez podjęcie działań zapobiegających kryzysom i wybuchowi wojny, a w przypadku agresji, skupienie całego wysiłku sił zbrojnych na jej odparciu.

W ostatnich latach obserwujemy w Polsce systematyczny wzrost przestępczości i wykroczeń różnego typu. Charakteryzują 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);

---

[1] System ochrony obiektu wojskowego w ujęciu rozprawy jest pojęciem ogólnym systemu sygnalizacji zagrożeń i alarmowego.

- stosowanie broni palnej, materiałów wybuchowych i innych przedmiotów niebezpiecznych;
- umiędzynarodowienie (przemyt samochodów, narkotyków i broni);
- agresja;
- okrucieństwo.

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

W strukturach administracyjnego zarządzania i kierowania bezpieczeństwem państwa zarówno jednostki wojskowe, jak i odpowiednie instytucje ministerstwa obrony narodowej, resortu spraw wewnętrznych i administracji oraz obrony cywilnej stanowią podstawową formę organizacyjną systemu obronnego kraju. Ich organizacja, spełnianie różnorodnych funkcji, wzajemne relacje oraz liczba, utrudnia stworzenie wzorcowego modelu ochrony przed różnego typu zagrożeniami. Należy nadmienić, że zagrożenia przestępcze będą się szczególnie wzmagać w czasie klęsk ekologicznych, katastrof, niepokojów społecznych 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, centra sterujące i decyzyjne wraz z wyposażeniem i całą infrastrukturą.

Istnieje więc konieczność ochrony obiektów i mienia przed różnorodnymi zagrożeniami. Urządzenia sygnalizacji zagrożeń stają się coraz bardziej powszechnymi i skutecznymi środkami neutralizacji zagrożeń przestępczych i cywilizacyjnych, tak w środowisku cywilnym i wojskowym, jak również w strukturach zarządzających krajem.

Obecność Polski w NATO nie tylko wzmocniła w sposób zdecydowany bezpieczeństwo naszego kraju, ale także postawiła szereg nowych obowiązków do wypełnienia. Dotyczą one w szczególności sił zbrojnych. Sojusz Atlantycki stawia swoim członkom wysokie wymagania. Nowe zadania dotyczą całej gospodarki kraju, są przyczyną radykalnych zmian w sferze planistyczno-organizacyjnej, wymagają zastosowania innych procedur dowodzenia oraz rozwiązań technicznych. Doskonalone jest także prawo, co najwyraźniej widać w dziedzinie dotyczącej przestrzegania tajemnicy państwowej i służbowej. Zmiany obejmują ponadto cały kompleks przedsięwzięć związanych ze stosowaniem aktywnej i skutecznej ochrony elementów systemu obronnego kraju, jakimi są obiekty wojskowe.

Z przedstawionych wyżej rozważań wynika, iż konieczne staje się stworzenie metodologii i modeli ochrony obiektów wojskowych oraz opracowanie sposobów ich weryfikacji. Uczynić to należy dlatego, aby rzeczywiste systemy ochrony obiektów wojskowych były niezawodne i skuteczne.

Dlatego też przedstawione problemy skłoniły autora do sformułowania tematu niniejszej rozprawy „**Ochrona obiektów wojskowych na potrzeby obronności państwa**".

Niniejsza rozprawa jest efektem wieloletnich badań i doświadczenia zawodowego, nie tylko autora, ale także ogromnej rzeszy osób, zajmujących się profesjonalnie systemami ochrony fizycznej i technicznej obiektów.

Składam serdeczne słowa podziękowania gen. bryg. prof. dr. hab. Michałowi Krauze za podjęcie trudu promotora rozprawy doktorskiej, właściwe ukierunkowanie procesu badawczego oraz przekazanie wiedzy w poszczególnych fazach powstawania rozprawy – koncepcyjnej, badawczej, syntetyzującej wyniki badań i pisarskiej.

Dziękuję współpracownikom i kolegom za cierpliwość i wyrozumiałość okazaną w trakcie pisania rozprawy.

Pragnę podziękować wszystkim osobom, które zainspirowały mnie do podjęcia badań w dziedzinie ochrony obiektów oraz pozytywnie motywowały ich kontynuację.

1. PODSTAWY METODOLOGICZNE

1.1. Problematyka rozprawy

Głębokie przeobrażenia systemowe dokonujące się w Polsce w ostatnich latach dotyczą wszystkich podstawowych dziedzin życia. Przemianie podlegają niemalże wszystkie podsystemy funkcjonujące zwłaszcza w obszarach - politycznym, społecznym i ekonomicznym.

Zmianom tym towarzyszy wzrost zjawisk z zakresu patologii społecznej, szczególnie gwałtowny wzrost liczby przestępstw i ich brutalizacja. W 1998 r. liczba zarejestrowanych przestępstw zwiększyła się o 64.3% w stosunku do roku poprzedniego. Dynamiczny wzrost przestępczości dotyczy nie tylko poszczególnych obywateli, ale także w wysokim stopniu odnosi się do instytucji gospodarczych, politycznych i społecznych. Zjawiska patologiczne skierowane przeciwko tym instytucjom, zwłaszcza zaś zajmującym szczególną rolę w systemie obronnym państwa budzą szczególny niepokój ze względu na ich kluczowe znaczenie dla funkcjonowania całego systemu państwowego. Siły zbrojne stanowią złożony system, który jest sprzężony z całym układem społeczno - gospodarczym państwa. Ostatnio ukazało się wiele artykułów alarmujących o przestępczości w wojsku. Z tych relacji wynika, że:

- obiekty wojskowe są słabo chronione pod względem fizycznym i technicznym;
- obecny system ochrony organizacyjno-technicznej obiektów wojskowych umożliwia w dużej mierze ich penetrację przez elementy przestępcze;
- istnieje niski poziom wiedzy na temat ochrony obiektów praktycznie na wszystkich szczeblach kierowania i dowodzenia;
- występuje brak systemów ochrony i sygnalizacji zagrożeń oraz nadzoru nad służbami odpowiedzialnymi za te systemy.

Stąd rodzi się potrzeba ciągłego doskonalenia w zakresie organizacyjno - technicznego zabezpieczenia obiektów wojskowych.

W strukturze bezpieczeństwa państwa obiekty - jednostki wojskowe stanowią podstawowe ogniwo organizacyjne systemu obronnego państwa. Ich organizacja, różnorodność funkcjonalna, wzajemne relacje oraz duża liczba utrudnia stworzenie wzorcowego modelu ochrony przed zagrożeniami. Oczywiście niemały wpływ na wybór typu ochrony ma wielkość posiadanych środków finansowych na jej realizację.

Przesłanki te stanowiły punkt wyjścia w określeniu głównego celu rozprawy doktorskiej na temat „**Ochrona obiektów wojskowych na potrzeby obronności państwa**".

Rozwiązanie problemów doskonalenia systemu obronnego państwa, a także właściwego wykorzystania systemu ochrony obiektów wymaga prowadzenia dalszych systematycznych badań i prac wdrożeniowych specjalistycznych zespołów i placówek naukowo-badawczych.

Prowadzenie badań naukowych charakteryzuje określona metodologia postępowania:

- rozpoznanie problemu;
- sformułowanie celu badań;
- określenie problemu naukowego;
- określenie obszaru badań;
- sformułowanie hipotezy roboczej;
- wybór metod przeprowadzenia badań;
- wykonanie badań;
- dokonanie analizy wyników;
- opracowanie wniosków.

Przebieg procesu badań naukowych został przedstawiony na schemacie 1.1[1].

Na ochronę obiektu wojskowego składają się zarówno elementy organizacyjne, jak i techniczne. Aspekty techniczne odgrywają zasadniczą rolę w zakresie jakościowych wskaźników systemów ochrony obiektów wojskowych.

Dynamiczny rozwój wielu dziedzin wiedzy, zwłaszcza z zakresu mikroelektroniki, telekomunikacji i informatyki, umożliwia stworzenie szerokiego spektrum wyboru wariantów różnorodnych form organizacyjno - technicznych ochrony elektronicznej obiektów tej kategorii zagrożeń jakimi są obiekty należące do struktury systemu obronnego państwa (SOP).

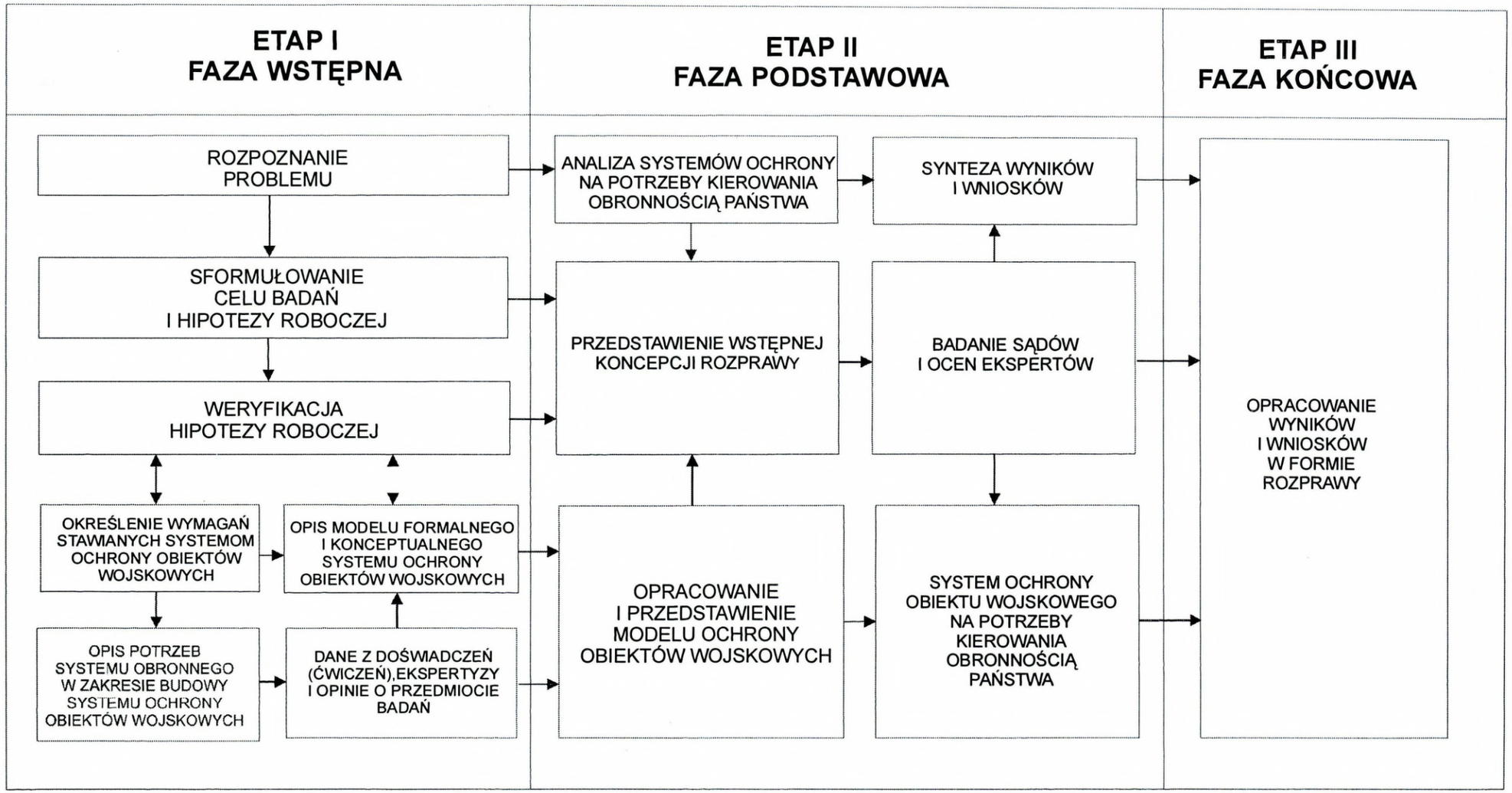
Budowa systemu ochrony obiektów wojskowych staje się jednym z problemów obronności państwa, który wymaga rozwiązania.

Weryfikacja teoretycznych podstaw i praktyczna realizacja budowy modelu systemu ochrony obiektu wojskowego na potrzeby obronności państwa stosownie do zaprezentowanych uwarunkowań oraz przewidywanych potrzeb stanowiły punkt wyjścia do określenia celu rozprawy.

Wyłania się więc potrzeba przedstawienia najkorzystniejszego modelu organizacyjnej i technicznej ochrony obiektu wojskowego z tak szerokiej gamy możliwości funkcjonalnych i technicznych urządzeń różniących się jakością i walorami funkcjonalno-użytkowymi.

---

[1] Opracowanie własne.



Schemat 1.1. Przebieg procesu badawczego.

1.2. Cel rozprawy

Za główny cel rozprawy przyjęto zaprojektowanie i przedstawienie modelu systemu ochrony obiektów wojskowych na potrzeby obronności państwa.

Z powyższego celu głównego wynikają cele szczegółowe:

- dokonanie oceny wrażliwości systemu obronnego na zagrożenia;
- określenie potrzeb i wymagań w zakresie ochrony obiektów wojskowych;
- ocena rozwiązań w zakresie ochrony obiektów – krajowych i stosowanych w niektórych państwach NATO;
- przedstawienie metodologii budowy modelu systemu ochrony;
- opracowanie modelu systemu ochrony obiektów;
- weryfikacja modelu systemu ochrony obiektów.

1.3. Problemy badawcze

Problem główny został sformułowany następująco:

Jaki powinien być model systemu ochrony obiektów wojskowych na potrzeby obronności państwa?

Przedstawione cele autor zamierza zrealizować poprzez rozwiązanie następujących problemów badawczych:

- Jakie są zagrożenia i jak one wpływają na system obronny państwa?
- Jakie są potrzeby i wymagania systemu obronnego państwa stawiane systemom ochrony obiektów wojskowych?
- Jakie rozwiązania systemów ochrony obiektów są stosowane w kraju a jakie w niektórych państwach NATO?
- Jakie czynniki wpływają na wybór elementów systemu ochrony obiektów?
- Jakie są zadania systemu ochrony obiektów oraz jaki należy przyjąć jego model?
- Jak stosowanie systemów ochrony obiektów może neutralizować zagrożenia systemu obronnego państwa?

1.4. Obszar badań

Sformułowane problemy zamierzam przedstawić ze szczególnym uwzględnieniem:

- uwarunkowań prawno - organizacyjnych i ograniczeń dotyczących systemów ochrony obiektów na potrzeby obronności państwa;
- dotychczasowej wiedzy teoretycznej z zakresu modelowania, projektowania i oceny systemów ochrony obiektów;
- wyników badań i wniosków uzyskanych z dotychczasowej eksploatacji systemów ochrony obiektów.

1.5. Hipotezy badawcze

Określenie celów pracy oraz poszukiwanie odpowiedzi na związane ze sobą i uzupełniające się problemy badawcze a także posiadana wiedza i doświadczenie, pozwoliły na sformułowanie następujących hipotez:

Hipoteza główna

Obecnie nie istnieje kompleksowy model systemu ochrony obiektów spełniający wymagania obronności państwa.

Hipotezy cząstkowe

- Istnieje potrzeba zwiększenia poczucia bezpieczeństwa społeczeństwa przez szersze wykorzystanie metod i technik ochrony obiektów.
- Jest możliwa identyfikacja zagrożeń i określenie ich wpływu na system obronny państwa.
- Jest możliwe dokonanie analizy porównawczej istniejących systemów ochrony obiektów w kraju i w niektórych wybranych państwach zachodnich.
- Dynamicznie rozwijająca się technika, nowe technologie i sposoby organizacji technicznej ochrony pozwalają na realizację systemów ochrony obiektów.
- Jest możliwe zaprojektowanie modelu systemu ochrony obiektów na potrzeby obronności państwa.
- Istnieje możliwość zweryfikowania zbudowanego modelu podsystemu ochrony obiektów i dostosowania go do wymagań systemu obronnego państwa.

Podstawą prowadzonych rozważań w zakresie budowy modelu będą uwarunkowania prawne, zarówno polskie jak i zagraniczne normy (wymagania), opracowania producentów, tendencje rozwojowe urządzeń ochrony.

Założenia i ograniczenia przyjęte w pracy

Założenia zakresu badawczego rozprawy dotyczą systemów ochrony obiektów wojskowych, ze szczególnym uwzględnieniem elektronicznych podsystemów sygnalizacji zagrożeń i alarmowania oraz elementów automatyki. W opracowanym modelu uwzględniono następujące podsystemy:

- alarmowe włamania i napadu;
- alarmowe pożaru;
- sterowania dostępem;
- telewizji użytkowej;
- ochrony elektromechanicznej;

- ochrony zewnętrznej;
- monitorowania i transmisji sygnałów alarmowych;
- zintegrowanych systemów sygnalizacji zagrożeń;
- telekomunikacyjnych i łączności;
- kierowania obronnością państwa.

Rozprawa obejmuje także zagadnienia dotyczące ochrony obiektów wojskowych przed działaniami terrorystycznymi i sabotażowymi.

W mniejszym stopniu zostały uwzględnione zagadnienia dotyczące ochrony przed penetracją radioelektroniczną. To zostało zaprezentowane tylko w sensie fizycznego utrudnienia w zbliżeniu się potencjalnego intruza na małą odległość do obiektu chronionego lub jego penetracji (strefy ochrony zewnętrznej i wewnętrznej).

Praca nie obejmuje następujących zagadnień: architektoniczno - budowlanych, systemów sygnalizacji zagrożeń przemysłowych, systemów zagrożeń środowiskowych, systemów wczesnego ostrzegania przed kataklizmami i innych pokrewnych sygnalizujących zagrożenia.

W rozprawie nie zostały rozwinięte problemy organizacji i procedur ochrony obiektów przez służby ochrony fizycznej, prawne dotyczące odpowiedzialności karnej za czyny przestępcze, aspektów, skutków socjospołecznych i moralnych stosowania systemów alarmowania i sygnalizacji zagrożeń.

1.6. Wybrane metody badawcze

Złożoność systemu ochrony jest tak obszerna, że konieczne było zastosowanie kilku metod badawczych, które w odniesieniu do określonych dziedzin i badanych problemów były najskuteczniejsze i pozwoliły na objęcie wszystkich elementów systemu i wzajemnych powiązań między nimi wraz z oddziaływaniem otoczenia.

W badaniach zastosowano podejście systemowe. Przedmiotem badań jest system, który funkcjonuje w określonym otoczeniu, posiada swą strukturę, a jego elementy są we wzajemnej relacji.

System rozpatrywany jest w dwóch aspektach, jako:

- system obronny państwa,
- system ochrony obiektów wojskowych systemu obronnego państwa.

Pomiędzy tymi systemami występuje także korelacja, przy czym system ochrony obiektów jest podsystemem systemu obronnego państwa.

W literaturze spotykamy szereg definicji systemu. Najogólniej przez system rozumie się zbiór elementów składowych, nazywanych obiektami, powiązanych ze sobą i realizujących pewne funkcje w określony sposób.

Systemem nazywać będziemy każdy złożony obiekt wyróżniony w badanej rzeczywistości, stanowiący całość tworzoną przez zbiór obiektów elementarnych (elementów) i powiązań (relacji) między nimi[2].

W badaniach stosowano metody empiryczne i teoretyczne metody badawcze.

W metodach empirycznych wykorzystywano głównie obserwacje naukowe (bezpośrednie i pośrednie), które będą przydatne w badaniach wstępnych do określania istniejących zagrożeń i oceny systemu obronnego państwa. Ważnym narzędziem wspomagającym badania były własne doświadczenia i bazy danych związanych z systemami ochrony obiektów.

W dalszej części badań posługiwano się metodami modelowania do utworzenia opisu werbalnego i formalnego modelu konceptualnego.

Wnioski z eksperymentu naukowego będą szeroko wykorzystane do budowy modelu systemu sygnalizacji zagrożeń i alarmu (ochrony obiektów) na potrzeby kierowania obronnością. Natomiast metoda badania sądów i ocen ekspertów posłużyły do określania kierunków i perspektyw rozwoju.

W opracowaniach naukowych można spotkać następującą definicję modelu „odwzorowanie rzeczy i zjawisk lub procesów, które zamierzamy stworzyć, śledzić ich przemiany lub określić (zdefiniować)". Innymi słowy: model powinien przedstawiać elementy systemu, wzajemne ich powiązanie i oddziaływanie.

Otaczającą nas rzeczywistość można odzwierciedlić za pomocą wielu form, jak również można spotkać wiele rodzajów modeli i sposobów ich klasyfikacji. Podział modeli na rodzaje, klasy czy grupy, przeprowadza się na podstawie kryteriów, przyjętych zależnie od konkretnych potrzeb i wynikających z celu, któremu klasyfikacja ma służyć.

Modelem systemu nazywać będziemy taki model, który odwzorowuje wszystkie podstawowe aspekty badań systemowych. W niniejszej pracy do opracowania systemu sygnalizacji zagrożeń i alarmu (ochrony obiektu) na potrzeby obronne państwa posłużono się modelem opisu formalnego i doświadczeniem empirycznym.

Za pomocą obserwacji naukowej, popartej własnym doświadczeniem i zgromadzoną bazą danych ochrony obiektów, będą badane istniejące systemy ochrony obiektów i procesy zachodzące podczas ich budowy i eksploatacji. Dokonana obserwacja naukowa pozwoliła poznać architekturę systemu i jego możliwości eksploatacyjne.

Modelowanie systemu zastosowano do badania istniejącego i tworzenia perspektywicznego systemu ochrony.

---

[2] A. Stabryła, J.Trzcieniecki, *Organizacja i zarządzanie. Zarys problematyki*, PWN, Warszawa 1986.

Metodę badania sądów i ocenę ekspertów wykorzystywano także do ustalenia rodzaju stosowanych systemów, ich elementów oraz ich oceny ze strony użytkowej w celu określenia koncepcji modelu systemu ochrony.

Zastosowano również metody teoretyczne takie jak: analiza, synteza, abstrahowanie, porównanie, analogia, uogólnienie, które wzbogaciły i uzupełniły metody empiryczne.

Analizę, jako główną metodę badawczą, zastosowano w trakcie studiowania literatury przedmiotu i opracowywania wniosków z badań, a także do określenia poziomu zagrożenia obiektu.

Synteza pozwoliła połączyć w określony zbiór wszystkie elementy systemu ochrony w zakresie zadań i wymagań przed nim stojących.

Podczas niektórych etapów badań było bardzo pomocne abstrahowanie, które pozwoliło wyeliminować cechy i elementy systemowe nie wywierające istotnego wpływu na realizację głównego celu badawczego.

Pozostałe metody teoretyczne pozwoliły na odtworzenie wybranych zjawisk i procesów oraz posłużyły do formułowania uogólnionych wniosków.

1.7. Krytyczna analiza literatury przedmiotu

Ochrona obiektów jest stosunkowo nową dyscypliną wiedzy, która w zakresie ochrony elektronicznej obiektów liczy około 30 - 35 lat w krajach zachodnich. W Polsce profesjonalne zastosowania elektroniki i systemów technicznych w ochronie obiektów datuje się zasadniczo od początku lat osiemdziesiątych.

Rozwój profesjonalnych systemów ochrony technicznej, systemów alarmowania i sygnalizacji zagrożeń do lat dziewięćdziesiątych miał miejsce w sektorze prywatnym i był oparty na urządzeniach i rozwiązaniach zachodnich. Państwo nie było, z różnych względów, zainteresowane powszechnym dostępem i napływem nowoczesnej techniki zabezpieczeń. Z drugiej zaś strony państwa zachodnie w pełni kontrolowały i strzegły najbardziej zaawansowanych technologii, szczególnie tych, które dotyczyły ochrony obiektów o wysokim poziomie ryzyka.[3]

Od początku lat dziewięćdziesiątych datuje się dynamicznie wzrastający napływ zaawansowanych technologii w zakresie systemów sygnalizacji zagrożeń i alarmowych. Obecnie systemy instalowane w Polsce poziomem technicznym nie ustępują rozwiązaniom zachodnim, a nawet – w niektórych wypadkach – stanowią nowość nawet dla fachowców z państw zachodnich.[4]

---

[3] W końcu lat osiemdziesiątych autor spowodował dostawę zaawansowanej technicznie czujki ultradźwiękowej ruchu.
[4] W latach 1997/98 autor brał udział w realizacji zaawansowanego systemu alarmowego w jednym z banków polskich.

Wiedza w tej branży jest zdobywana najczęściej w praktyce zawodowej i w zasadzie nie było w uczelniach i szkołach wyższych odpowiednich specjalizacji w zakresie zabezpieczenia technicznego[5]. Ostatnio w krajach zachodnich pojawiły się specjalizacje w tym zakresie, najczęściej są to studia zawodowe inżynierskie, często finansowane przez renomowanych producentów, a także branżowe organizacje zawodowe, stowarzyszenia i izby przemysłowe.

W Polsce od drugiej połowy lat dziewięćdziesiątych powstają nawet kierunki studiów podyplomowych w zakresie ochrony, np. studia podyplomowe na WAT oraz w niektórych szkołach niepublicznych. Często organizowane są szkolenia firmowane przez producentów oraz firmy koncesjonowane lub posiadające uprawnienia Kuratorium Oświaty. Należy wspomnieć o kursach dla rzeczoznawców systemów alarmowych, organizowanych przez Ogólnopolskie Stowarzyszenie Producentów, Projektantów i Instalatorów Systemów Alarmowych „POLALARM".

Pomimo takich niezaprzeczalnych osiągnięć branży i środowiska zajmującego się systemami alarmowymi oraz kontaktów z czołowymi producentami zachodnimi i ich obecnością na polskim rynku zabezpieczeń, nie ma praktycznie publikacji ujmującej kompleksowo przedmiot badań niniejszej rozprawy. Jedną z bardzo nielicznych prac, które podejmowały temat w ujęciu przekrojowym i systemowym jest praca zbiorowa.[6]

Natomiast brak jest opracowań modelowych systemów sygnalizacji zagrożeń i alarmowania w ujęciu wielopłaszczyznowym - zarówno normatywnym, jak i prawnym, a także organizacyjnym i technicznym, szczególnie kosztowym[7] - tak w opracowaniach krajowych, jak i w literaturze zachodniej. Istniejące opracowania cząstkowo i fragmentarycznie ujmują przedmiot badań. Brak jest analizy porównawczej i krytycznej oceny. Nie istnieje pełna metodologia wraz z rozwiniętymi procedurami sporządzania modelu systemu alarmowego.

Dobór literatury przedmiotu wynikał z tematu rozprawy i organizacji procesu badawczego. Charakter poszczególnych grup opracowań był związany z realizacją kolejnych etapów pracy i koniecznością rozwiązywania zbioru problemów szczegółowych.

Z punktu widzenia oceny przydatności poszczególnych pozycji literatury w procesie badawczym można je podzielić na trzy grupy:

- bezpośrednio przydatne w procesie badawczym;
- inspirujące do przyjętych rozwiązań;
- uzupełniające zakres wiedzy.

---

[5] W ostatnich latach w krajach zachodnich np. na uczelniach niemieckich można otrzymać specjalizację zawodową w zakresie ochrony obiektów.

[6] A. Ryczer, A. Wójcik i inni, *Techniczno -funkcjonalna charakterystyka urządzeń oraz systemów elektronicznego zabezpieczenia, a także procesu ich projektowania i realizacji*, Przewodnik Rzeczoznawcy Ogólnopolskiego Stowarzyszenia Producentów, Projektantów i Instalatorów Systemów Alarmowych. Zeszyt Nr 4. Warszawa 1994.

[7] A. Wójcik, *Zasady opracowywania kosztorysów sygnalizacji alarmowej*, TECHOM, Warszawa 1996.

W każdej z tych grup można wyróżnić kilka wartościowych pozycji, chociaż z uwagi na specyfikę badań nie zawsze były one w pełni przydatne w prowadzonym procesie badawczym.

Treść wielu materiałów dotyczyła eksploatowanych obecnie różnych typów systemów sygnalizacji zagrożeń i alarmowych oraz oceny ich właściwości w aspekcie wymagań systemowych. Sytuacja ta wymagała krytycznego i jednocześnie konstruktywnego podejścia autora do ich treści.

Oddzielny problem stanowiło wprowadzenie aktualnych wymagań normatywnych w zakresie systemów alarmowych. Aktualność rozprawie nadają wprowadzone nowe (projekty) norm, które praktycznie są już obowiązujące i stanowią odpowiedniki euronorm.

Przy opracowywaniu rozprawy doktorskiej autor wykorzystał pozycje literatury, które ze względu na ich charakter można podzielić na następujące grupy:

1. Publikacje dotyczące metodologii badań naukowych;
2. Dokumenty normatywno – prawne;
3. Literatura traktująca o systemie obronnym państwa i jego zagrożeniach;
4. Opracowania o charakterze techniczno – organizacyjnym;
5. Literatura uzupełniająca pośrednio związana z tematem rozprawy.

Ad 1. Do najistotniejszych pozycji z tego zakresu należą: J. Pietera „Ogólna metodologia pracy naukowej“ i „Z zagadnień pracy naukowej“, E. Wiśniewskiego „Metodyka badań wojskowych“ oraz Kupisiewicza „Podstawy dydaktyki ogólnej“, a także Sienkiewicza „Analiza systemowa“. Literatura ta, zwłaszcza z zakresu rozwiązania metodologicznego badanego problemu i podejścia systemowego była niezwykle pomocna przy realizacji procesu badawczego. Można stwierdzić, że wymienione pozycje pozwoliły właściwe ukierunkować prowadzone badania oraz dokonać wyboru odpowiednich metod badawczych, szczególnie przy opracowywaniu metodologii budowy modelu ochrony obiektu. W tej grupie należy także przytoczyć jedną z bardzo nielicznych pozycji ujmujących kompleksowo zagadnienia analizy zagrożeń oraz procedury ich neutralizacji – Z.T. Nowickiego “Alarm o przestępstwie“. Z. T. Nowicki za pomocą metody badawczej ZTN-3 ocenia i analizuje bezpieczeństwo obiektu. Wadą tej metody jest brak syntetycznego powiązania z aspektami technicznymi rozwiązań i analizą kosztową wybranego rozwiązania. Wymieniona metoda stanowi wspomagające narzędzie prowadzenia analizy zagrożeń i oceny poziomu bezpieczeństwa obiektu.

Ad 2. W zakresie systemu obronnego państwa, podstawową pozycję aktów normatywno-prawnych stanowi ustawa zasadnicza, Konstytucja RP z dnia 2 kwietnia 1997 roku. Natomiast grupa aktów normatywno-prawnych w zakresie organizacyjno-technicznym obejmuje przede wszystkim Polskie Normy dotyczące systemów alarmowych, tj. “Systemy alarmowe. Zbiór arkuszy Polskiej Normy. PN-93/E-08390-14: 1993“ oraz wymienione w bibliografii

projekty norm. Jedyny akt prawny w postaci ustawy dotyczy systemów alarmowych pożaru i ujmuje zasady i wymogi stosowania systemów automatycznego wykrywania pożaru oraz zasad certyfikacji tych urządzeń.

W zakresie wymagań dotyczących ochrony obiektów wojskowych należy wymienić:

- „Dyrektywę bezpieczeństwa ACE nr 70-1", NATO (jawne), 1997;[8]
- „Tymczasowe normy zabezpieczenia w techniczne urządzenia sygnalizacyjne i alarmowe terenów, obiektów i mienia wojskowego".[9]

Wymienione wyżej pozycje posłużyły do oceny stanu krajowych rozwiązań ochrony obiektów oraz rozwiązań w zakresie ochrony obiektów wojskowych stosowanych w niektórych państwach NATO i wymagań stawianych tym systemom w kontekście członkostwa Polski w NATO. Uzupełnieniem są akty normatywne i wytyczne obowiązujące w krajach zachodnich w zakresie wymagań i stosowania systemów alarmowych np. „Richtlinien für Einbruchmeldeanlagen. Planung und Einbau"; „VdS 2311 12/93 (01)", „Verband der Sachversicherer e.V. Köln". Materiały powyższe stanowiły niezbędne uzupełnienie i wzór porównawczy dla aktów normatywnych i wymagań obowiązujących w Polsce.

Wymagania prawne w zakresie ochrony informacji niejawnych i wynikających z tego tytułu zadaniach i obowiązkach zawarto w ustawie o ochronie informacji niejawnych z dnia 22 stycznia 1999. Natomiast ustawa o ochronie osób i mienia (Dz. U. Nr 114, poz.740) reguluje wymagania i zasady wykorzystywania formacji ochrony fizycznej i technicznej do ochrony obiektów.

Ad 3. Charakterystykę systemu obronnego państwa opracowano wykorzystując głównie pozycje następujących autorów: S. Kozieja „Podstawowe założenia polityki bezpieczeństwa i strategii obronnej", B. Balcerowicza „Wybrane problemy obronności państwa", z których zostały wykorzystane podstawowe pojęcia z zakresu bezpieczeństwa, polityki i strategii obronnej RP oraz systemu obronnego, a z pracy S. Dworeckiego „Współczesne konflikty zbrojne" - problemy powstawania konfliktów zbrojnych i zagrożeń, podobna tematyka była przedmiotem rozważań w pracach: R. Kulczyckiego „Perspektywiczny model kierowania obronnością RP..." i M. Krauzego „Wojskowe aspekty współczesnych zagrożeń ekologicznych".

Opracowania J. Pawłowskiego, B. Tarasiuka i innych autorów z DSO i DBM MON, a także prace prowadzone w Akademii Obrony Narodowej pod kryptonimami np. „Kierunki" i „Kappa" stanowiły podstawę analizy systemu obronnego państwa w aspekcie zagrożeń i ich wpływu na bezpieczeństwo powszechne. Literatura ta, prezentując trendy przemian struktury systemu obronnego państwa, była pomocna na etapie opracowywania jego charakterystyki.

---

[8] ACE z ang. Allied Command Europe Zjednoczone Dowództwo Europejskie.
[9] Sztab Generalny WP, Zarząd Obrony Terytorialnej, Warszawa 1999.

Pozycje te, jako prace rozwojowe, koncentrowały się na rozwiązaniach perspektywicznych, przedstawiając stan istniejący i to w aspekcie jego wad. Motorycznym uzupełnieniem tych pozycji były obowiązujące obecnie akty normatywne i instrukcje określające strukturę systemu i zakresy zadań jego poszczególnych ogniw.

Powyższe materiały były pomocne przy opracowywaniu metodologii modelu systemu sygnalizacji zagrożeń i alarmowania na potrzeby obronności państwa.

Ad 4. W tej grupie znajdują się opracowania, na ogół w postaci referatów lub artykułów w pismach fachowych, dotyczące cząstkowych zagadnień, które były pomocne i inspirowały do dalszych badań. Można tu wymienić następujące prace z zakresu teorii projektowania systemów alarmowych: A. Wójcik "Wprowadzenie do projektowania systemów alarmowych sygnalizacji zagrożeń.", opracowania dotyczące konkretnych typów systemów zarówno krajowe, np. J. Ciszewski "Zasady projektowania instalacji sygnalizacji pożarowej.", jak i zagraniczne, np. A. Wege "Video-Überwachungstechnik. CCTV-Handbuch für Planer, Berater und Anwender".

Dla przybliżenia zagadnień technicznych, które zostały zaprezentowane w postaci rozszerzonej w załącznikach, wykorzystano opracowania wdrożonych rozwiązań przodujących producentów urządzeń i systemów alarmowych, np. „Produktsliste 98. Einbruchmeldesysteme effeff", czy Videor Technical "CCTV Technische Änderungen vorbehalten" November '97.

Wśród przytoczonych publikacji znajdują się także opracowania dotyczące tendencji rozwojowych w zakresie technicznej ochrony systemów alarmowych, np. „Schulungsunterlagen effeff. Materiały szkoleniowe".

Ad 5. Ze względu na interdyscyplinarny charakter przedmiotu badań, w tej grupie literatury znajdują się pozycje powiązane pośrednio lub bezpośrednio z zagadnieniami omawianymi w niniejszej pracy. Są to często wartościowe pozycje naukowe z różnych dziedzin, a mianowicie:

- kryminologii i kryminalistyki, np. B. Hołyst "Kryminologia" i referat pt.: "Ocena bezpieczeństwa w Polsce", J. Świerczyński "Wybrane zagadnienia taktyczne stosowania kryminalistycznych systemów zabezpieczających z wykorzystaniem urządzeń elektronicznych";
- socjologii, np. U. Świętochowska "Patologie cywilizacji współczesnej";
- organizacji i zarządzania, np. praca zbiorowa pod kierunkiem Z. Michnowskiego.

Rozprawa składa się z czterech zasadniczych części.

W części pierwszej metodologicznej zostały przedstawione cele, problemy, hipotezy badawcze oraz narzędzia zastosowane do ich rozwiązania, jak również krytyczna analiza literatury przedmiotu.

W drugiej części została zaprezentowana ocena wrażliwości systemu obronnego z jego elementami struktury i funkcjami oraz źródła i rodzaje zagrożeń i ich wpływ na system obronny państwa.

Rozdział trzeci obejmuje potrzeby systemu obronnego państwa w zakresie ochrony obiektów, wraz z istniejącymi rozwiązaniami oraz charakterystykę i analizę systemów, rozwiązań krajowych i występujących w niektórych państwach NATO, jak również wymagania stojące przed systemami ochrony.

Rozdział czwarty zawiera metodologię projektowania, model systemu ochrony oraz jego weryfikację.

Zakończenie zawiera wnioski końcowe dotyczące projektu modelu i prowadzenia dalszych prac i badań nad systemami ochrony obiektów.

2. SYSTEM OBRONNY PAŃSTWA - OCENA WRAŻLIWOŚCI NA ZAGROŻENIA

2.1. Charakterystyka wybranych elementów systemu obronnego państwa

W celu przeciwdziałania różnym zagrożeniom w czasie pokoju i realizacji zarówno wewnętrznych, jak i zewnętrznych zadań obronnych utrzymuje się i rozwija na czas zagrożenia i wojny system obronny Rzeczypospolitej.

W literaturze funkcjonuje kilka definicji systemu obronnego państwa, jedna z nich brzmi: „zbiór wzajemnie powiązanych elementów (ludzi, organizacji i urządzeń) działających na rzecz zachowania bezpieczeństwa i nienaruszalności terytorialnej kraju.[1]"

System obronny państwa, zdefiniowany w ramach pracy naukowo-badawczej, to: „zbiór wzajemnie powiązanych elementów (ludzi, organizacji, urządzeń) działających na rzecz bezpieczeństwa państwa". Natomiast bezpieczeństwo państwa definiowane jest jako „zdolność państwa do ochrony jego wartości przed zagrożeniami."

Wzajemne powiązanie i oddziaływanie na siebie wszystkich elementów systemu obronnego państwa stwarza możliwość efektywnej integracji potencjału obronnego z odpowiednio przygotowaną administracją i gospodarką oraz zorganizowanym i przygotowanym do obrony społeczeństwem.

Funkcjonowanie systemu obronnego państwa polega na realizacji różnorodnych zadań i przedsięwzięć obronnych przez wszystkie ogniwa przygotowujące państwo do działania w okresie wzrostu zagrożenia jego bezpieczeństwa i na czas wojny. W funkcjonowaniu poszczególnych elementów i ogniw systemu obronnego państwa zakłada się:

- kompleksowość i spójność rozwiązywania wielu wzajemnie zależnych i powiązanych ze sobą zadań ogólnopolitycznych, społeczno-gospodarczych i militarnych w ramach przygotowań obronnych;
- możliwość skutecznego przeciwstawienia się wszelkim zagrożeniom godzącym w bezpieczeństwo narodowe.

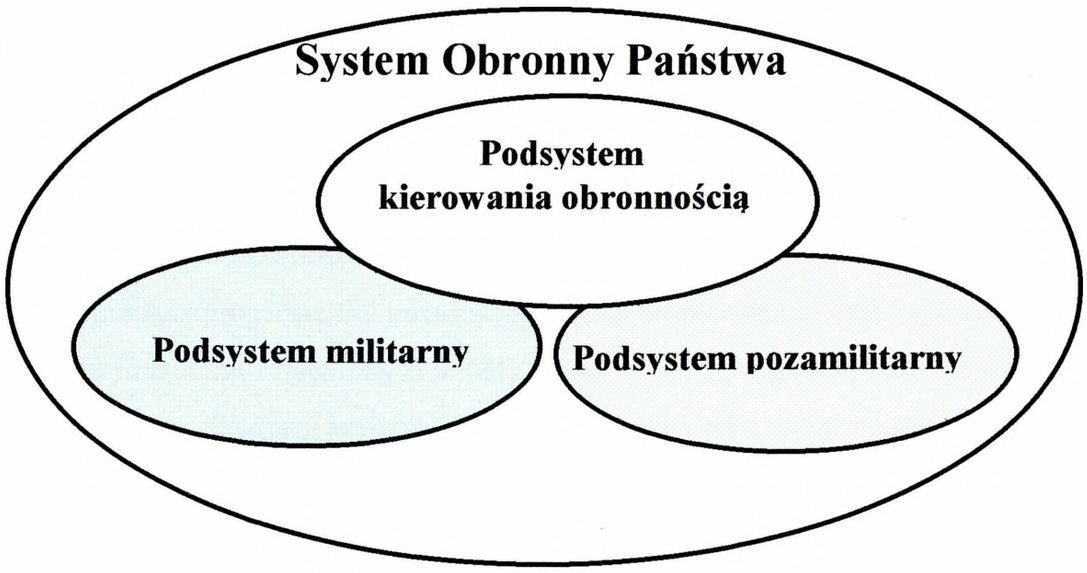
W skład systemu obronnego państwa wchodzą trzy podstawowe podsystemy:[2]

- podsystem militarny, który stanowią i tworzą siły zbrojne;
- podsystem pozamilitarny, w skład którego wchodzą siły szeroko pojmowanej obrony cywilnej oraz wszelkie pozamilitarne ogniwa ochrony i obrony instytucji państwa;
- podsystem kierowania obronnością, który tworzą najwyższe organa władzy i administracji państwowej.

---

[1] B. Balcerowicz, *Słownik podstawowych terminów dotyczących bezpieczeństwa państwa,* AON, Warszawa 1996.
[2] A. Komański, i inni, *Perspektywiczny model systemu obronnego państwa. Kierunki*, AON 1993.

Rysunek 2.1.1 przedstawia schemat ogólny systemu obronnego państwa.



Rys. 2.1.1. Ogólny schemat systemu obronnego państwa

Podsystem militarny - Siły Zbrojne Rzeczypospolitej Polskiej

Zgodnie z Konstytucją Rzeczpospolitej Polskiej Siły Zbrojne służą obronie niepodległości państwa i niepodzielności jego terytorium oraz bezpieczeństwa i nienaruszalności granic. Realizują to poprzez ciągłą zdolność i gotowość do reagowania na zewnętrzne zagrożenia kryzysowe oraz do przeprowadzenia, samodzielnie lub wspólnie z sojusznikami, niezbędnych do obrony państwa kampanii i operacji militarnych.

Miejsce i rolę sił zbrojnych w systemie obronnym wyznaczają stojące przed nimi zadania, dostosowane do charakteru i skali zagrożeń. W sytuacji sporów, napięć i konfliktów wojennych, które mogą wystąpić w bezpośrednim otoczeniu Polski, stwarzających zagrożenie dla bezpieczeństwa kraju, główny wysiłek sił zbrojnych skierowany będzie na zapewnienie militarnej osłony granic państwa jednocześnie realizując przedsięwzięcia z zakresu osłony strategicznej stosownie do charakteru i stopnia zagrożeń.

W sytuacji udziału polskich sił zbrojnych, w ramach sił międzynarodowych, w rozwiązywaniu kryzysów polityczno-militarnych (również konfliktów zbrojnych oddalonych od granic RP) wydzielają one, na podstawie mandatu organizacji międzynarodowych, kontyngent wojskowy przeznaczony do wykonywania określonego zadania, utrzymując jednocześnie na obszarze kraju gotowość do wsparcia sił resortu spraw wewnętrznych i administracji w wypadku ewentualnych, odwetowych zamachów terrorystycznych za zaangażowanie się Polski w konflikt.

W przypadku lokalnej (ograniczonej) agresji głównym zadaniem sił zbrojnych jest przeprowadzenie kampanii obronno - zaczepnej w celu zatrzymania oraz rozbicia lub wyparcia

Nr ewid.
Działu Zbiorów Jawnych - Akademii

zgrupowania przeciwnika, odzyskania zajętego terytorium, a w razie potrzeby przeprowadzenie działań na jego terytorium.

W przypadku wojny powszechnej głównym zadaniem sił zbrojnych jest przygotowanie i prowadzenie kampanii obronnej, obejmującej działania regularne o charakterze przede wszystkim manewrowych operacji obronnych połączonych z obroną ważnych rejonów i obiektów oraz działaniami nieregularnymi (przede wszystkim sił obrony terytorialnej) na terenach zajętych przez przeciwnika.

Nowa treść zadań strategicznych i operacyjnych RP oraz zmienione warunki ich realizacji stymulują istotne zmiany w siłach zbrojnych. Trwają dalsze prace nad nowym modelem wojska. Równocześnie ze zmniejszeniem jego liczebności następują sukcesywne przeobrażenia strukturalne, przesunięcia dyslokacyjne, modernizacja techniczna.

Wojsko polskie składa się z trzech rodzajów sił zbrojnych: wojsk lądowych zorganizowanych w okręgi wojskowe, sił powietrznych (wojsk lotniczych i obrony powietrznej) oraz marynarki wojennej. Przewiduje się stopniowe doprowadzenie do bardziej równomiernego rozmieszczenia wojsk na obszarze kraju.

Wojska lądowe składać się będą z dwóch części:

- wojsk operacyjnych - składających się z jednostek wojskowych wyposażonych w najlepszy sprzęt wojskowy (objęty limitami porozumień wiedeńskich), kadrę stanowić będą żołnierze zawodowi;
- wojsk obrony terytorialnej - wyposażonych przede wszystkim w lekką broń przeciwpancerną, przeciwlotniczą i strzelecką.

Na rysunku 2.1.2. zaprezentowana jest struktura systemu kierowania siłami zbrojnymi w czasie pokoju.[3] Struktura organizacyjna systemu ma typowy charakter hierarchiczny, na jej czele znajduje się urząd prezydenta jako zwierzchnika sił zbrojnych.

Rysunek 2.1.3. przedstawia jeden z wariantów struktury systemu kierowania siłami zbrojnymi w czasie wojny z uwzględnieniem struktur NATO.[4]

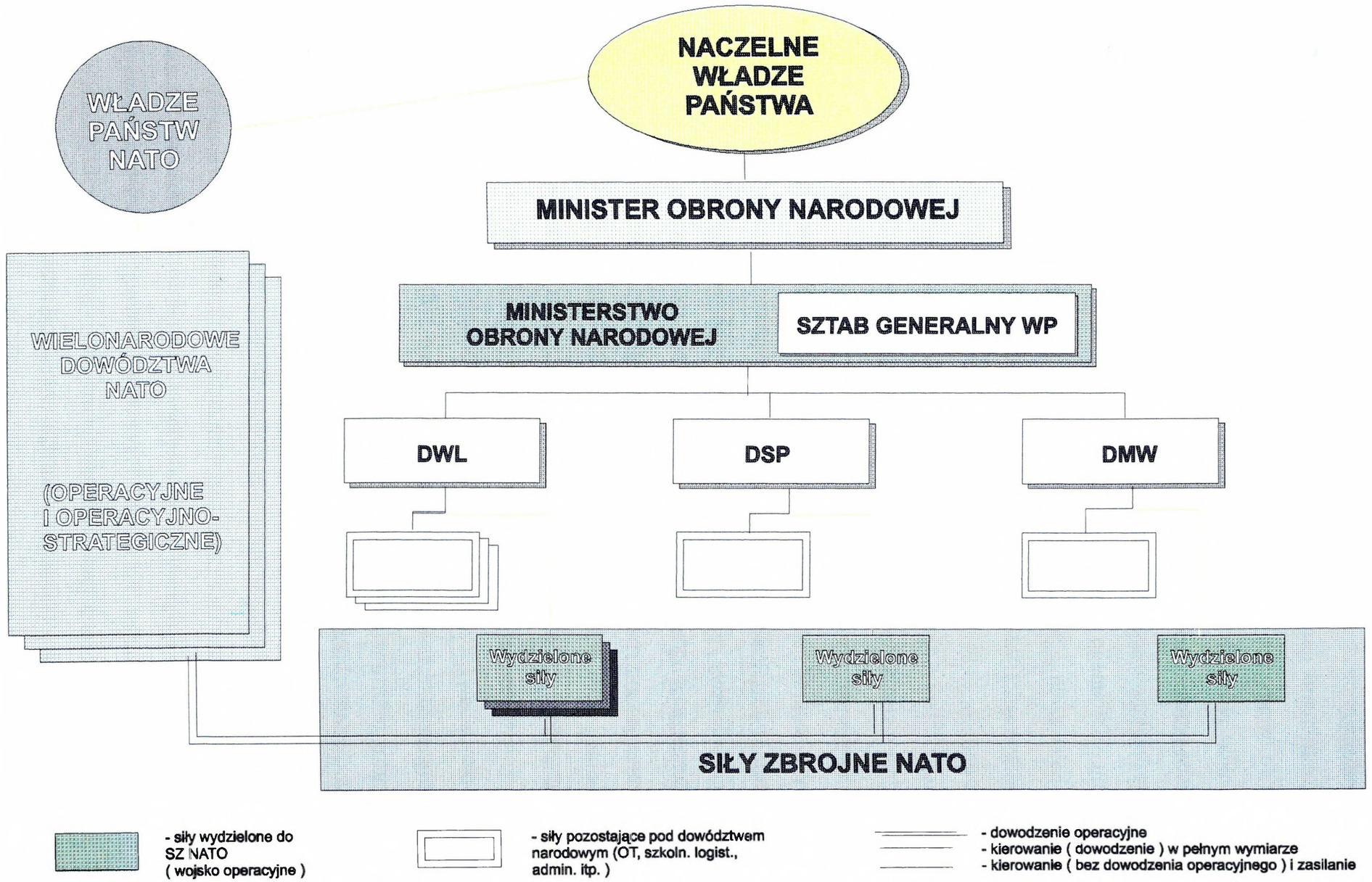
---

[3] S. Koziej, F. Wołkowicz, *Podstawowe założenia polityki bezpieczeństwa i strategii obronnej*, AON, DSO MON, Warszawa 1998.

[4] B. Tarasiuk i inni, *Kierowanie obronnością państwa w czasie pokoju, kryzysu i wojny. Materiał studyjny*, Warszawa 1998.



Rys. 2.1.2. STRUKTURA SYSTEMU KIEROWANIA SIŁAMI ZBROJNYMI (w czasie pokoju) - wariant



Rys.2.1.3.Struktura systemu kierowania siłami zbrojnymi (w czasie wojny) - wariant

Podsystem pozamilitarny

Układ pozamilitarny jest bardzo ważnym elementem systemu obronnego państwa. Przeznaczony jest do tworzenia niezbędnych warunków przygotowania i działania sił zbrojnych oraz funkcjonowania pozostałych struktur państwa, a także zapewnienia materialnych i duchowych podstaw przetrwania narodu w czasie zagrożenia i wojny.

Zgodnie z powinnościami konstytucyjnymi zadania obronne spoczywają na wszystkich ogniwach systemu obronnego państwa, jak również na organizacjach politycznych, gospodarczych, społecznych i religijnych. Podstawą siły obronnej kraju jest świadomość obronna każdego obywatela, kształtowana w rodzinie, szkole, pracy i we wszystkich sferach działalności publicznej.

Układ pozamilitarny obejmuje ogniwa ochronne, gospodarczo-obronne i polityczno-społeczne, realizujące zadania obronne. W ich skład wchodzą:

- ogniwa ochronne, w tym:
  - ogniwa ochrony struktur państwa, Urząd Ochrony Państwa, Wojskowe Służby Informacyjne, Policja Państwowa, Straż Graniczna, Wojska MSWiA, Trybunał Konstytucyjny, sądy, prokuratura (resort Ministerstwa Sprawiedliwości), Najwyższa Izba Kontroli;
  - ogniwa ochrony ludności, Sztab Obrony Cywilnej Kraju, formacje ochrony cywilnej, jednostki straży pożarnej, siły i środki Ministerstwa Zdrowia i Opieki Społecznej, Ministerstwa Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa oraz wydzielone siły i środki z pozostałych resortów (równorzędnych) i województw;
- ogniwa gospodarczo-obronne, w tym:
  - ogniwa resortowe, zwłaszcza siły i środki resortów: Ministerstwa Gospodarki Przestrzennej i Budownictwa, Ministerstwa Przemysłu i Handlu, Ministerstwa Transportu i Gospodarki Morskiej, Ministerstwa Rolnictwa i Gospodarki Żywnościowej, Ministerstwa Łączności, Ministerstwa Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa, Ministerstwa Przekształceń Własnościowych, Ministerstwa Współpracy Gospodarczej z Zagranicą, Ministerstwa Finansów, Narodowego Banku Polskiego, Państwowej Agencji Atomistyki, Głównego Urzędu Miar, Polskiego Komitetu Normalizacyjnego, Urzędu Patentowego, Komitetu Badań Naukowych, Polskiej Akademii Nauk, Centralnego Urzędu Planowania;

- ogniwa wojewódzkie, podmioty gospodarcze i inne jednostki organizacyjne rozmieszczone na terenie województwa (których organem założycielskim jest wojewoda), a na które zostały nałożone zadania obronne;

- ogniwa polityczno-obronne, w tym:
  - ogniwa polityczne, resort spraw zagranicznych, Polska Agencja Prasowa, organizacje polityczne, paramilitarne i religijne, na które nałożono zadania obronne;
  - ogniwa społeczne, resorty Ministerstwa Edukacji Narodowej, Ministerstwa Kultury i Sztuki, Urząd Kinematografii, Krajowa Rada Radiofonii i Telewizji, Urząd Kultury Fizycznej i Turystyki, media publiczne i prywatne, organizacje społeczne i zawodowe, na które nałożono zadania obronne.

Podsystem kierowania obronnością państwa

Kierowanie obroną państwa jest to celowa działalność wszystkich organów władzy i administracji państwowej, samorządowej i gospodarczej zmierzająca do utrzymania określonego potencjału obronnego w czasie pokoju oraz zapewniająca sprawną realizację tych zadań w okresie zagrożenia i wojny.

Kierowanie, rozumiane jako funkcja systemu obronnego państwa jest rodzajem więzi informacyjnych i decyzyjnych jakie zachodzą pomiędzy określonymi elementami systemu obronnego.

Istotą kierowania obroną państwa warunkującą ciągłość działania całego systemu obronnego jest należycie pojmowane i zorganizowane sterowanie zasadniczymi jego elementami. Kierowanie całokształtem działań obronnych państwa polega więc na koordynacji, zgrywaniu działalności najważniejszych organów władzy i administracji państwowej, sił zbrojnych oraz wszystkich elementów obrony niemilitarnej w celu należytego ich funkcjonowania zarówno w czasie pokoju jak i na okres zagrożenia państwa oraz wojny.

Strukturę podmiotową kierowania obronnością kraju stanowią generalnie ogniwa i jednostki organizacyjne państwa. Zgodnie z konstytucyjnym trójpodziałem władzy w kraju na ustawodawczą, wykonawczą i sądowniczą wydaje się celowe aby wszystkie te ogniwa były, w ramach swych kompetencji, odpowiedzialne za bezpieczeństwo kraju i brały czynny udział w procesie kierowania jego obronnością.

Kierowanie obronnością jest integralną częścią systemu kierowania państwem. W czasie pokoju uczestniczą w tym procesie naczelne oraz centralne organa władzy i administracji rządowej, wojewódzkie organa administracji rządowej, organa samorządu terytorialnego, kierownicy podmiotów gospodarczych, instytucji i organizacji zobowiązanych do realizacji zadań obronnych, a także organa dowodzenia sił zbrojnych funkcjonujące

w strukturach czasu pokoju. Wyjątkową odpowiedzialnością obciążone są naczelne organa polityczne. Do ich kompetencji należy ocena potencjalnych zagrożeń oraz określenie środków zaradczych stosownie do zagrożeń i możliwości państwa.

Podsystem kierowania państwem, w tym również obronnością opiera się w większości na strukturze liniowo-sztabowej. Polega na tym, że przy każdym organie (decydencie) działa komórka organizacyjna (zespół) wykonująca czynności o charakterze przygotowawczym i organizacyjnym.

Nie zwalnia to jednak decydenta od osobistego podejmowania decyzji i od konsekwencji z tego wynikających. Szczególnie ważna, ze względu na omawiany problem, jest zasada precyzyjnego określenia kompetencji organów w zakresie kierowania. Wynikają z tego obowiązki i uprawnienia oraz określone miejsce i rola poszczególnych organów w całym systemie kierowania obronnością państwa. Sprawy te są ogólnie uregulowane w Konstytucji RP. Bardziej szczegółowe uregulowania znajdują się w ustawach dotyczących urzędów państwowych, w tym również w ustawie o urzędzie ministra obrony narodowej, aktach prawnych uchwalanych przez Radę Ministrów oraz w dotychczas obowiązujących uchwałach Komitetu Obrony Kraju (KOK). Zgodnie z postanowieniami zawartymi w ww. aktach poszczególne organa sprawują określone funkcje w kierowaniu obronnością Rzeczypospolitej Polskiej w czasie pokoju. Zadania dla poszczególnych ogniw systemu obronnego państwa ustalają właściwe organa władzy i administracji państwowej drogą aktów prawnych.

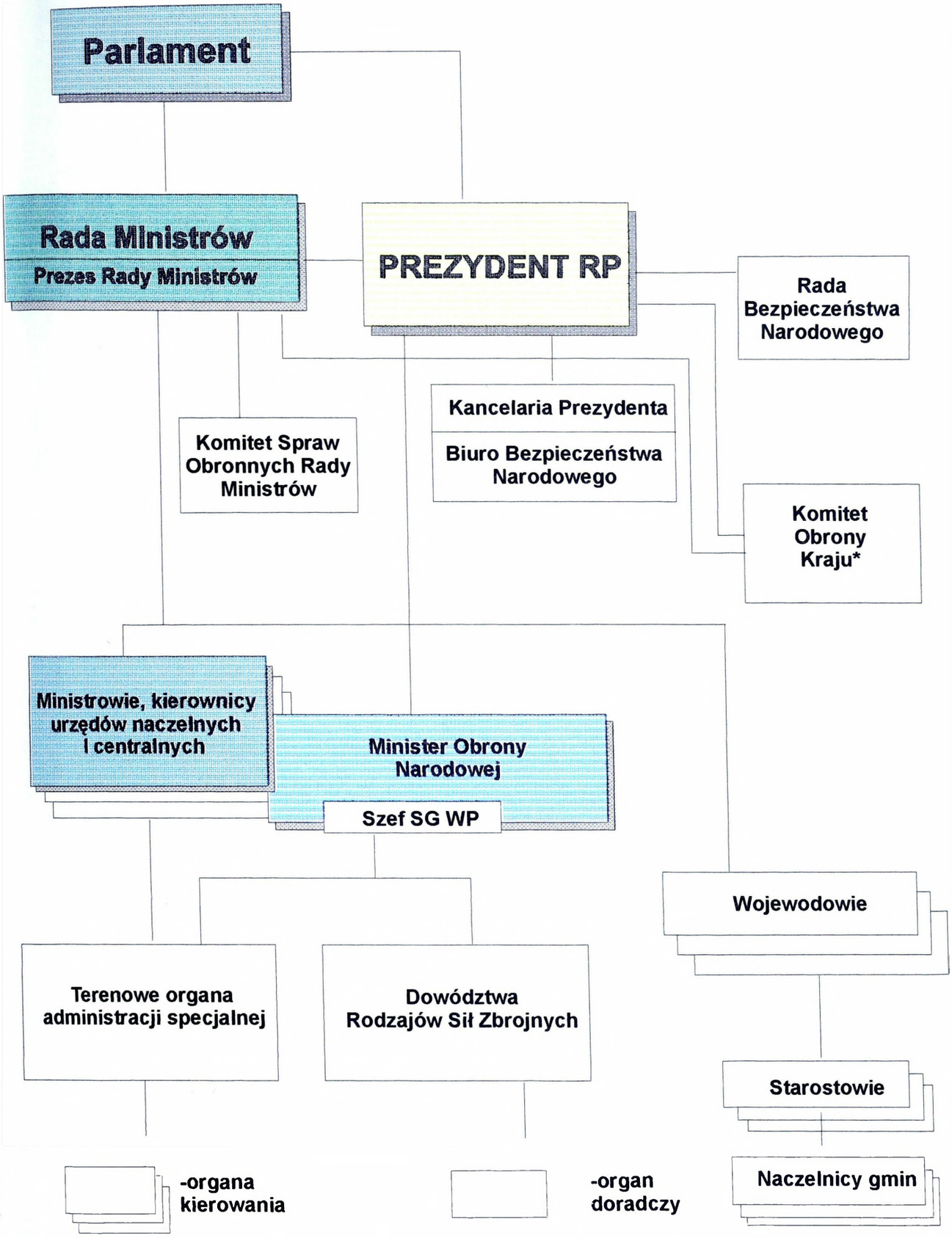
Podsystem kierowania obronnością przeznaczony jest do przygotowania i zapewnienia sprawnego funkcjonowania państwa w czasie zagrożenia i wojny. Celem sytemu kierowania obronnością państwa w czasie pokoju jest przygotowywanie i utrzymywanie na odpowiednim poziomie potencjału obronnego oraz zapewnienie jego sprawnego rozwinięcia do koniecznego wymiaru w okresie zagrożenia i w czasie wojny.

Ogólną strukturę podsystemu kierowania obronnością przedstawiono na rys. 2.1.4.

Podsystem kierowania obronnością jest integralną częścią systemu kierowania państwem. Jego rola polega na sprzężeniu elementów systemu obronnego państwa w jednolitą sprawnie funkcjonującą całość. Obejmuje organa państwowe oraz samorządowe, na które nakłada się obowiązki realizacji zadań obronnych.

Podstawowymi ogniwami podsystemu kierowania państwa są:

- naczelne organa władzy i administracji państwowej, parlament (sejm i senat), Prezydent RP i KOK, Rada Ministrów, premier i Komitet Spraw Obronnych Rady Ministrów (KSORM), ministrowie, komisje i komitety sprawujące funkcje naczelnych organów administracji państwowej;



* Dotychczas funkcjonuje. Nowa konstytucja nie uwzględnia KOK

Rys.2.1.4. Ogólna struktura podsystemu kierowania obronnością państwa

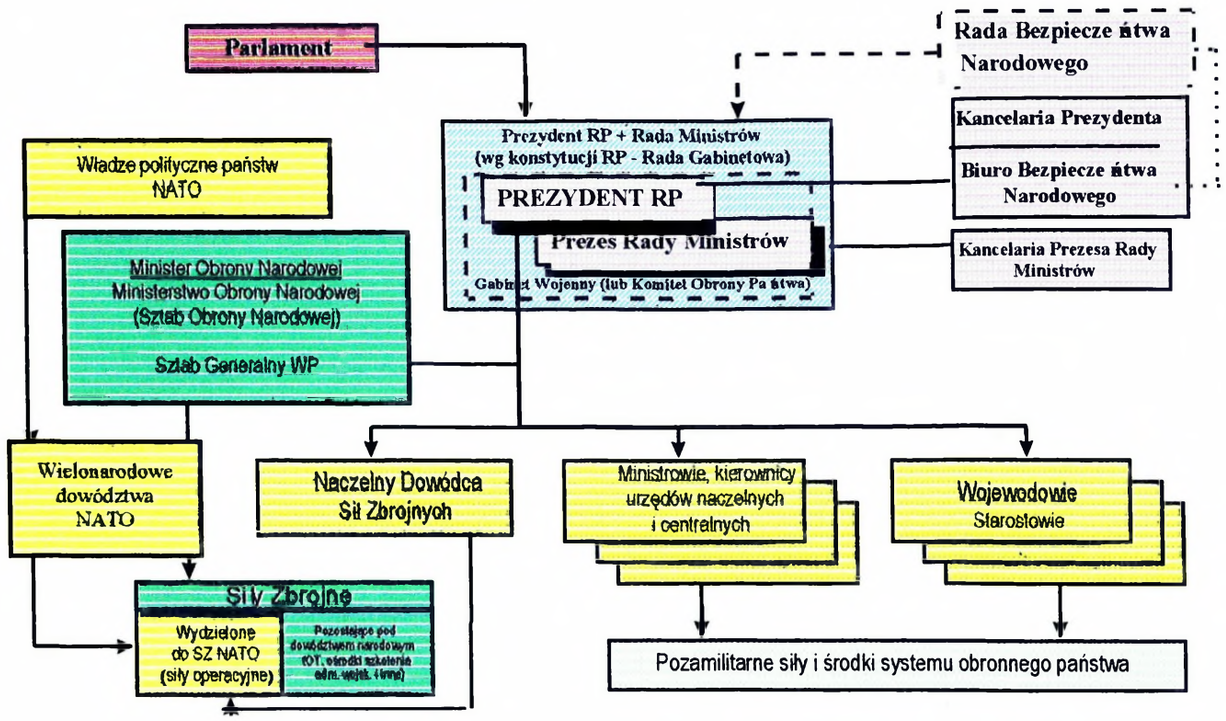
- centralne organa administracji państwowej, centralne i generalne dyrekcje i zarządy w resortach (np. Centralna Dyrekcja PKP, Centralna Dyrekcja Dróg Publicznych, Generalna Dyrekcja Lasów Państwowych, Centralny Zarząd Poczty Polskiej, itp.), komendy główne: Policji, Państwowej Straży Pożarnej, Straży Granicznej;
- terenowe organa administracji rządowej, wojewodowie;
- okręgowe i regionalne dyrekcje w resortach podległe centralnym organom administracji (np. Dyrekcje Okręgowe Dróg Publicznych, Okręgowe Dyrekcje Gospodarki Wodnej, Regionalne Dyrekcje Lasów Państwowych, Okręgowe Dyrekcje Kolei Państwowych, itp.);
- samorząd terytorialny;
- organa dowodzenia Siłami Zbrojnymi RP, Sztab Generalny WP, dowództwa okręgów wojskowych i rodzajów sił zbrojnych, dowództwa związków taktycznych i oddziałów.

W kierowaniu obronnością obowiązują podobne zasady jak w każdym kierowaniu.

Szczególnie ważna, ze względu na omawiany problem, jest zasada precyzyjnego określenia kompetencji organów w zakresie kierowania. Z tego wynikają obowiązki i uprawnienia oraz określone miejsce i rola poszczególnych organów w całym systemie kierowania obronnością państwa. Sprawy te są ogólnie uregulowane w Konstytucji RP.

Bardziej szczegółowe uregulowania znajdują się w ustawach dotyczących urzędów państwowych, w tym również w ustawie o urzędzie ministra obrony narodowej, aktach prawnych uchwalonych przez Radę Ministrów oraz w dotychczas obowiązujących uchwałach Komitetu Obrony Kraju. Zgodnie z obowiązującymi postanowieniami zawartymi w wyżej wymienionych aktach poszczególne organa sprawują określone funkcje w kierowaniu obronnością Rzeczpospolitej Polskiej w czasie pokoju. Schemat podsystemu kierowania obronnością państwa uwzględniający obecne uwarunkowania przedstawiono na rys. 2.1.5.

Parlament jest organem stanowiącym prawo, w tym również prawo dotyczące bezpieczeństwa i obronności państwa. Parlament jest dwuizbowym organem władzy ustawodawczej tj. Sejmu Rzeczpospolitej Polskiej i Senatu Rzeczpospolitej Polskiej. Sejm Rzeczpospolitej Polskiej, uchwala każdego roku wysokość środków na bezpieczeństwo i obronę państwa w ramach ustawy budżetowej, jak również inne regulacje ustawowe dotyczące problematyki bezpieczeństwa i obronności państwa oraz kontroluje ich stosowanie. Senat Rzeczpospolitej Polskiej dzieli z Sejmem wykonywaniem funkcji ustawodawczej, włącznie z uchwalaniem wysokości wydatków na bezpieczeństwo i obronę państwa. Parlament w głównej mierze, decyduje o wielkości potencjału obronnego państwa utrzymywanego w czasie pokoju.



Rys.2.1.5.Schemat podsystemu kierowania obroną państwa (wariant)

Wszelkie decyzje dotyczące bezpieczeństwa i obronności państwa powodują określone skutki głównie ekonomiczne i gospodarcze, a nieraz także polityczne i inne. Szczególnie w czasie pokoju ściśle przestrzega się przyjętych procedur legislacyjnych. Projekty ustaw dotyczące obronności (mogą je wnosić tylko organa posiadające prawo inicjatywy ustawodawczej) niezależnie od opinii Komisji Sejmowej i Senackiej zawsze są opiniowane przez Radę Ministrów. Rząd każdorazowo, w takich sprawach, obowiązany jest przedstawić parlamentowi skutki jakie może spowodować przyjęcie określonej ustawy. Dopiero po zaopiniowaniu projektu ustawy przez rząd, dalsze procedury legislacyjne są identyczne jak dla innych ustaw uchwalanych przez parlament. Specjalistycznymi organami parlamentu w sprawach obronności są Senacka i Sejmowa Komisja Obrony Narodowej. Oprócz funkcji ustawodawczej parlament, podobnie jak w stosunku do innych dziedzin działalności państwa, spełnia funkcję kontrolną. W stosunku do Rady Ministrów uprawnienia kontrolne posiada tylko Sejm.

Zgodnie z postanowieniami określonymi w Konstytucji RP Sejm decyduje w imieniu RP o stanie wojny i o zawarciu pokoju. Natomiast parlament nie uczestniczy bezpośrednio w kierowaniu obronnością, gdyż ani on, ani jego komisje nie mają uprawnień wykonawczych.

Prezydent Rzeczypospolitej Polskiej, zgodnie z zapisami Konstytucji RP, stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium. Jako reprezentant państwa w stosunkach zewnętrznych ratyfikuje i wypowiada umowy międzynarodowe, o czym ma obowiązek powiadomić Sejm i Senat. Jest on najwyższym

zwierzchnikiem Sił Zbrojnych Rzeczypospolitej Polskiej. W sprawach szczególnej wagi może on zwołać Radę Gabinetową (jest to Rada Ministrów obradująca pod przewodnictwem Prezydenta RP), z tego uprawnienia nie wynikają dla Prezydenta RP dodatkowe kompetencje. Radzie Gabinetowej nie przysługują kompetencje Rady Ministrów, chociaż jej postanowienia mogą mieć istotny wpływ na decyzje Rady Ministrów. Prezydent uczestniczy w ustanawianiu prawa w dziedzinie obronności (posiada on prawo inicjatywy ustawodawczej, prawo veta i podpisuje ustawy). Organem doradczym Prezydenta RP w zakresie wewnętrznego i zewnętrznego bezpieczeństwa państwa jest Rada Bezpieczeństwa Narodowego, o jej składzie i trybie powoływania decyduje Prezydent RP.

Komitet Obrony Kraju, zgodnie z dotychczas obowiązującą ustawą o powszechnym obowiązku obrony jest organem właściwym w sprawach obronności i bezpieczeństwa państwa, posiadającym bardzo szerokie kompetencje w zarządzaniu i administrowaniu obronnością. Należy tu zaznaczyć, że jest to sprzeczne z nową Konstytucją, która zadania te powierza Radzie Ministrów.

Rada Ministrów jest głównym organem wykonawczym w dziedzinie działalności państwa. Realizuje ona politykę wewnętrzną i zagraniczną Rzeczypospolitej Polskiej. Do jej szczególnych obowiązków należy: zapewnienie wykonania ustaw, w tym również ustaw dotyczących obronności, zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa oraz porządku publicznego, sprawowanie ogólnego kierownictwa w dziedzinie obronności kraju, zawieranie umów międzynarodowych wymagających ratyfikacji oraz zatwierdzanie i wypowiadanie innych umów międzynarodowych. Rada Ministrów, poprzez ministrów i wojewodów, kieruje realizacją zadań obronnych, koordynuje, kontroluje i nadzoruje pracę wszystkich organów administracji rządowej. Jej też przysługuje prawo inicjatywy ustawodawczej.

Prezes Rady Ministrów kieruje pracami Rady Ministrów, kontroluje i koordynuje prace członków Rady Ministrów, jest zwierzchnikiem służbowym pracowników administracji rządowej i korpusu służby cywilnej, posiada uprawnienia występowania z wnioskiem do Rady Ministrów o uchylenie rozporządzenia lub zarządzenia ministra.

Wewnętrznym organem rządu w sprawach bezpieczeństwa i obronności państwa jest Komitet Spraw Obronnych Rady Ministrów (KSORM). Do jego głównych zadań należy koordynowanie działań organów administracji państwowej w zakresie obronności w celu przygotowania stosownych projektów aktów normatywnych. Konkretne sprawy, po rozpatrzeniu przez KSORM, kierowane są do Rady Ministrów lub właściwego ministra, gdzie podejmuje się stosowne decyzje.

Ministrowie (kierownicy urzędów centralnych) kierują określonymi działami administracji rządowej, odpowiedzialni są za realizację zadań obronnych przez podległe i nadzorowane jednostki organizacyjne w ramach powszechnego obowiązku obrony. W strukturze organizacyjnej bezpośrednio podległych im urzędów występują specjalistyczne komórki ds. obronności, tworzą je departamenty lub biura spraw obronnych. Poszczególne resorty w swojej strukturze posiadają terenowe organa administracji specjalnej. W strukturze organów administracji specjalnej są etatowi pracownicy ds. obronnych.

Minister obrony narodowej sprawuje szczególną funkcję w systemie kierowania obronnością państwa. Jest naczelnym organem administracji państwowej w dziedzinie obronności państwa. Zgodnie z ustawą jest on odpowiedzialny za przygotowanie założeń obronnych państwa, w tym propozycji dotyczących rozwoju i struktury sił zbrojnych. Odpowiada przed Radą Ministrów za realizację jej generalnych założeń, decyzji i wytycznych dotyczących obronności państwa. W zakresie ustalonym przez Radę Ministrów sprawuje nadzór nad realizacją zadań obronnych, jest koordynatorem planowania obronnego oraz przygotowań obronnych realizowanych przez organa administracji państwowej, instytucje państwowe, organa samorządu terytorialnego, podmioty gospodarcze i inne podmioty. Kierowanie i dowodzenie siłami zbrojnymi realizowane będzie w zależności od sytuacji polityczno – militarnej.

Obecnie, w sytuacji członkowstwa Polski w NATO, wydzielone siły operacyjne podlegają pod wielonarodowe dowództwo Paktu Północnoatlantyckiego, natomiast pozostałymi siłami, poprzez dowództwa rodzajów sił zbrojnych dowodzi minister obrony narodowej.

Ministrowi obrony narodowej bezpośrednio podlegają: sekretarz stanu, podsekretarze stanu, szef Sztabu Generalnego, dowódcy rodzajów sił zbrojnych.

Szef Sztabu Generalnego WP jest najwyższym pod względem pełnionej funkcji żołnierzem czynnej służby wojskowej. W imieniu ministra w czasie pokoju dowodzi siłami zbrojnymi. Jest odpowiedzialny przed ministrem obrony narodowej za kierowanie kompleksowym planowaniem mobilizacyjnego i strategiczno-operacyjnego rozwinięcia oraz użycia sił zbrojnych, a także za ich gotowość bojową i mobilizacyjną. Do obowiązków szefa Sztabu Generalnego należy również współuczestniczenie w opracowaniu koncepcji i planów rozwoju sił zbrojnych.

Dowództwa rodzajów sił zbrojnych (Dowództwo Wojsk Lądowych, Dowództwo Marynarki Wojennej, Dowództwo Sił Powietrznych) podlegają bezpośrednio ministrowi obrony narodowej, odpowiadają za gotowość bojową i mobilizacyjną podległych wojsk. W hierarchii dowodzenia siłami zbrojnymi szczeblem równorzędnym dowództwom rodzajów sił zbrojnych były dotychczas dowództwa okręgów wojskowych. Pełniły one dwojakiego rodzaju funkcję. Jako bezpośrednio podległe ministrowi obrony narodowej funkcjonowały na zasadach

administracji specjalnej realizując określone zadania ministra, jednocześnie w stosunku do podległych wojsk są organami dowodzenia i realizują zadania wchodzące w zakres kompetencji szefa Sztabu Generalnego WP. Kolejnymi szczeblami dowodzenia są dowództwa związków taktycznych (dywizja, brygada) oddziałów i pododdziałów. Nowym elementem w dowodzeniu siłami zbrojnymi jest utworzenie Dowództwa Wojsk Lądowych, jako dowództwa rodzajów wojsk. Podporządkowanie Dowództwu Wojsk Lądowych dowództw okręgów wojskowych wraz z podległymi wojskami zmienia ich rolę i miejsce w hierarchii dowodzenia siłami zbrojnymi.

System dowodzenia siłami zbrojnymi Polski jako członka Paktu Północnoatlantyckiego wymaga usprawnienia i dostosowania do standardów tam przyjmowanych. Wiąże się to również z wydzielaniem wojsk operacyjnych do wielonarodowych związków operacyjnych podporządkowanych dowództwu NATO. Wydzielane wojska powinny zatem mieć struktury organizacyjne szczebla taktycznego zbliżone do struktur tego samego szczebla czołowych państw zachodnich, a także zbliżone możliwości bojowe. Trwają intensywne prace nad doskonaleniem systemu dowodzenia siłami zbrojnymi, niektóre propozycje są w trakcie uzgodnień.

Wojewoda (starostowie, burmistrzowie) jako przedstawiciel Rady Ministrów w województwie kieruje realizacją zadań obronnych na obszarze województwa. Do jego obowiązków należy:

- koordynowanie i kontrolowanie działalności administracji rządowej działającej na obszarze województwa w zakresie zgodności z polityką rządu,
- zapewnienie współdziałania jednostek organizacyjnych działających na obszarze województwa w zakresie utrzymania porządku publicznego, a także zapobiegania klęskom żywiołowym oraz usuwania ich skutków.

Wojewodzie, jako szefowi Obrony Cywilnej Województwa bezpośrednio podporządkowany jest Wojewódzki Inspektorat Obrony Cywilnej.

2.2. Źródła i formy zagrożenia elementów systemu obronnego państwa

We współczesnym świecie prawdopodobieństwo wybuchu wojny powszechnej zmniejszyło się znacznie, co nie oznacza całkowitego uwolnienia się od konfliktów. Równie niebezpieczne dla funkcjonowania państwa są zagrożenia spowodowane przez żywioły oraz zachowanie ludzi.

Rozróżnia się następujące zagrożenia dotyczące bezpieczeństwa państwa:[5]

- polityczno-militarne,
- niemilitarne, do których można zaliczyć:

- zagrożenia ustroju konstytucyjnego;
- zagrożenia ładu i porządku publicznego;
- nadzwyczajne zagrożenia środowiska (kryzysy polityczno-cywilizacyjne).

Wśród przyczyn powstawania zagrożeń możemy wyróżnić: ekonomiczne, społeczne, polityczne, psychologiczne, historyczne, etniczne, kulturowe, językowe, terytorialne, wyznaniowe, ekologiczne, wojskowe.

Podstawowe typy zagrożeń, mających wpływ na system obrony państwa, to:

- kryzys polityczno-militarny w otoczeniu Polski;
- zagrożenie ustroju konstytucyjnego;
- kryzys spowodowany zagrożeniem ładu i porządku publicznego, w tym: starcia uliczne, bezpośrednio zagrażające zdrowiu i życiu ludzkiemu; zagrożenia wywołane agresywnym zachowaniem się kibiców lub innych grup społecznych;
- terroryzm na tle: politycznym, religijnym, kryminalnym;
- szpiegostwo i działalność wywiadowcza na szkodę państwa, w tym: obcych grup wywiadowczych; własnych obywateli i funkcjonariuszy aparatu władzy;
- nadzwyczajne zagrożenia spowodowane przez środowisko, np. powódź;
- zagrożenia ekologiczne lub przyrodnicze spowodowane działalnością człowieka (cywilizacyjne).

Rozpatrując potencjalny kryzys polityczno-militarny w otoczeniu Polski[6] pod kątem zagrożenia bezpieczeństwa naszego państwa należy założyć, że może on przybrać formę napięć, sporów a w skrajnych przypadkach nawet konfliktów wojennych. Na przykład spór między Rosją a Ukrainą o Półwysep Krymski lub o podział Floty Czarnomorskiej w skrajnym przypadku mógłby w Polsce spowodować: ograniczenia w dopływie surowców, zakłócenia zbytu towarów, niekontrolowany napływ uciekinierów z obszarów objętych konfliktem zbrojnym, wzrost przestępczości zorganizowanej, przenoszenie epidemii, itp. Dotyczy to także zagrożeń od potencjalnych grup terrorystycznych mających związek z działaniami Polski w ramach NATO na terenie Jugosławii.

Obecnie w rozwiązaniach politycznych przeważa w świecie tendencja rozwiązywania sporów drogą rokowań. Skrajna forma eskalacji kryzysu - konflikt zbrojny w otoczeniu naszego państwa jest zatem mało prawdopodobny, jednakże całkowicie wykluczyć go też nie można.

W klasyfikacji kryzysów niemilitarnych na pierwszym miejscu, jako najgroźniejszy dla bezpieczeństwa państwa, wymieniono zagrożenie ustroju konstytucyjnego. Klasycznym przykładem tego typu zagrożenia może być sytuacja w Iranie, kraju dynamicznie rozwijającym

---

[5] S. Dworecki, *Od konfliktu do wojny*, BUWIK, Warszawa 1996.
[6] Dworecki S. i inni, *Współczesne konflikty zbrojne.Aspekt prognostyczny*, AON RCSS, Warszawa 1988.

się do czasu objęcia władzy (w wyniku zamachu stanu) przez fundamentalistów islamskich. Rządy dostojników islamskich doprowadziły kraj do wojny, w wyniku czego nastąpiło znaczne zubożenie państwa i społeczeństwa. Podobna sytuacja była w Algierii. Zdecydowanie władz algierskich, jak też ostatnie wybory w tym państwie świadczą raczej o zażegnaniu kryzysu.

W warunkach polskich wywołanie kryzysu zagrożenia ustroju konstytucyjnego jest mało prawdopodobne. Nie jesteśmy fanatykami religijnymi, w kraju nie działają partie lub ugrupowania polityczne wyznające skrajne ideologie. Zdecydowana większość naszego społeczeństwa aprobuje obecny ustrój państwowy.

Niebezpieczny dla funkcjonowania państwa jest kryzys spowodowany zagrożeniem ładu i porządku publicznego. Następstwa tego kryzysu odczuwa się w życiu codziennym obywateli jako brak bezpieczeństwa osobistego, a w skrajnych przypadkach może przybrać formę psychozy zagrożenia. Zjawisko to wywoływane jest działalnością różnego rodzaju mafii, gangów, czy też nasilenia innej działalności przestępczej - rozboje, rabunki, kradzieże, itp. Przykładem może być działalność mafii sycylijskiej, gdzie nie tylko zwykli obywatele byli narażeni na utratę życia i mienia, ale także aparat ścigania, wymiaru sprawiedliwości, nie pomijając w tym również osób sprawujących najwyższe urzędy państwowe. Mass media również donoszą o działalności naszych rodzimych "mafii": wołomińskiej, pruszkowskiej i innych działających na wybrzeżu. Mafia bowiem jest zjawiskiem, które oprócz zorganizowanej działalności przestępczej, dąży do wpływu na aparat władzy. Stanowi jedno z rozwijających się bardzo dynamicznie zagrożeń dla bezpieczeństwa państwa. Wynika to z doświadczeń państw zachodnich i obserwacji zjawiska w Rosji. Szczególnie dążenia do ujawnienia korupcji urzędników różnych szczebli administracji państwowej i ich powiązania ze zorganizowanym światem przestępczym, powinny znaleźć odzwierciedlenie w decyzjach organów ustawodawczych i wykonawczych państwa. Ma to niebagatelne znaczenie, jeśli weźmie się pod uwagę wzrost przestępczości w Rosji (o ok. 20%), spowodowany kryzysem finansowym a obejmujący swoim zasięgiem wszystkie poziomy władzy.

Niebezpieczny charakter mają wszelkiego rodzaju starcia uliczne, bezpośrednio zagrażające mieniu oraz zdrowiu i życiu ludzkiemu. Typowym tego przykładem było starcie zwolenników zdelegalizowanej partii faszystowskiej ze zwolennikami partii "zielonych" w jednym z niemieckich miast. Takich zajść nie brakuje i u nas, czego przykładem były majowe demonstracje i kontrdemonstracje, które kończyły się w wielu przypadkach starciami.

Podobny charakter mają zagrożenia wywołane agresywnym zachowaniem się kibiców w czasie meczów i po ich zakończeniu. W trakcie takich starć dochodzi także do niszczenia mienia zarówno prywatnego, jak i publicznego, dewastacji i wandalizmu. Opisane zjawiska, jeżeli mają charakter incydentalny i swoim zasięgiem nie obejmują dużego obszaru, nie są

groźne. Natomiast mogą zagrażać bezpieczeństwu państwa przy nagminnym występowaniu, obejmującym większy obszar kraju oraz wykorzystaniu tego zjawiska przez organizacje wywrotowe czy terrorystyczne.

Kolejnym zagrożeniem jest terroryzm[7], jako zjawisko bezpośrednio godzące w ład i porządek publiczny. Ostatnie lata szczególnie w Polsce ujawniły bezradność organów ścigania w zwalczaniu i zapobieganiu działalności terrorystycznej o charakterze kryminalnym. Należy wziąć pod uwagę niepokojący fakt, że wraz z intensyfikacją procesu integracji Polski ze strukturami NATO może wystąpić najbardziej skrajna forma terroryzmu polityczno-religijnego.

Innego typu kryzysy niemilitarne powodują nadzwyczajne zagrożenia środowiska, wywoływane zarówno przez żywioły, jak też przez działalność ludzką. Geograficznemu położeniu naszego państwa zawdzięczamy, że szereg zagrożeń znamy tylko z mass mediów. Nie występują w Polsce trzęsienia ziemi, erupcje wulkanów, powodzie wywołane falami sztormowymi oceanów, nieczęstym zjawiskiem są huragany o skali i sile niszczenia kilkakrotnie mniejszej niż na innych kontynentach. Zdarzają się w naszym kraju powodzie, pożary, susze, ale są to zjawiska, które nie zagrażały istnieniu naszego państwa, chociaż w zasadniczy sposób mogą wpłynąć na nastroje społeczno-polityczne i mogą być w odpowiedniej sytuacji, wykorzystane przez obce służby specjalne do wzbudzania zagrożenia konstytucyjnego.

Współczesny świat nękają nowe zagrożenia, dotychczas ludzkości nieznane. Przyczyną tych kryzysów są skutki działalności człowieka. W literaturze określa się je zamiennie, jako zagrożenia ekologiczne lub przyrodnicze, względnie cywilizacyjne.[8] Duże znaczenie przywiązuje się głównie do pierwszego etapu reagowania, jakim jest zapobieganie powstawaniu kryzysu, a więc fazie pojawiania się symptomów sytuacji kryzysowych. Jest to niezwykle trudne, wymagające stałego monitoringu i uzyskiwania wiarygodnych informacji. Z punktu widzenia kosztów (społecznych i materialnych) jest to etap najważniejszy. Aby sprostać temu zadaniu należy posiadać odpowiedni system reagowania kryzysowego, zdolny do spełnienia wszystkich uzgodnionych umowami międzynarodowymi warunków służących sprawnej koordynacji działań w sytuacjach kryzysowych.

We współczesnych warunkach szczególne znaczenie ma podsystem kierowania reagowaniem kryzysowym. Zainteresowanie się problematyką kryzysów znalazło odzwierciedlenie w koncepcjach i doktrynach bezpieczeństwa większości państw, w tym Rzeczpospolitej Polskiej. Jego rozbudowa jest jednym z ważniejszych zadań rządowych. Duże znaczenie przywiązuje się głównie pierwszemu etapowi reagowania, jakim jest zapobieganie

---

[7] C. Gearty, *Terroryzm*, Prószyński i S-ka, Warszawa 1998.
[8] M. Krauze, *Wojskowe aspekty współczesnych zagrożeń ekologicznych,* AON, Warszawa 1990.

powstawaniu kryzysu, a więc fazie pojawiania się symptomów sytuacji kryzysowych. Jest to niezwykle trudne, wymagające stałego monitoringu i uzyskiwania wiarygodnych informacji. Z punktu widzenia kosztów (społecznych i materialnych) jest to etap najważniejszy[9]. Aby sprostać temu zadaniu należy posiadać odpowiedni system reagowania kryzysowego, zdolny do wypełniania wszystkich uzgodnionych umowami międzynarodowymi warunków dla sprawnej koordynacji działań w sytuacjach kryzysowych. Problematyka reagowania na kryzysy przewidziana jest w Konstytucji RP, w rozdziale IX, gdzie mówi się o środkach nadzwyczajnych w razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli i porządku publicznego lub w celu zapobieżenia skutkom katastrof naturalnych i technicznych. Wyciąg z Konstytucji RP dotyczący stanów nadzwyczajnych został przytoczony w załączniku nr 2.1. Ustawowo do reagowania na sytuacje kryzysowe zobligowano również wojewodów. Do ich obowiązków należy zapewnienie współdziałania jednostek organizacyjnych działających na obszarze, województwa w zakresie utrzymania porządku publicznego, a także zapobiegania klęskom żywiołowym oraz usuwania ich skutków.

Obecnie w kraju utworzono kilka instytucji reagowania na sytuacje kryzysowe: Komitet Rady Ministrów ds. Zarządzania w Sytuacjach Kryzysowych, Zespół Reagowania Kryzysowego przy MSWiA, a na początku tego roku - Urząd Zarządzania Kryzysowgo. Jednym z jego organów jest Centrum Zarządzania Kryzysowego, którego celem jest integrowanie informacji z systemów monitorowania i wykrywania zagrożeń oraz komunikowanie się z ośrodkami realizującymi stały monitoring nadzwyczajnych zagrożeń środowiska, jak również ciągła współpraca ze środkami reagowania poszczególnych resortów, instytucji i służb.

U podstaw koncepcji funkcjonowania Centrum Zarządzania Kryzysowego przyjęto zasadę prymatu terytorialnego, która mówi że zagrożeniami lokalnymi należy zajmować się na poziomie lokalnym, w gminie powinien zajmować się wójt, ewentualnie starosta a w sytuacjach określonych stanów nadzwyczajnych (wyjątkowych) - wojewoda. Centralne ośrodki władzy i administracji państwa wkraczają tylko w przypadku klęsk żywiołowych. Takie rozwiązania są przyjęte w większości państw demokratycznych. Dlatego też najwyższe organa władzy i administracji państwa np. premier, szefowie resortów, itp. nie muszą dokonywać bezpośredniej wymiany informacji (posiadać kontaktu - łączności), z każdą będącą w strefie zagrożenia gminą. Jednym z najważniejszych i nie rozwiązanych do końca problemów w określonym obszarze np. gminie jest brak wymiany informacji między służbami specjalnymi. Między innymi powodem takiego stanu rzeczy jest uboga infrastruktura techniczna, jak również brak rozwiązań i unormowań legislacyjno - prawnych.

---

[9] Czarniecki A i inni, *Kierowanie obronnością państwa w czasie pokoju, kryzysu i wojny. Materiał studyjny.* AON, Warszawa 1998

Siły i środki do przeciwdziałania skutkom kryzysów niemilitarnych są w większości podporządkowane lub nadzorowane przez Ministra Spraw Wewnętrznych i Administracji (Policja, Państwowa Straż Pożarna, Służba Graniczna, Obrona Cywilna), będą one wykorzystywane m.in. przez szefów operacji do organizacji i prowadzenia działań stosownie do charakteru sytuacji nadzwyczajnej.

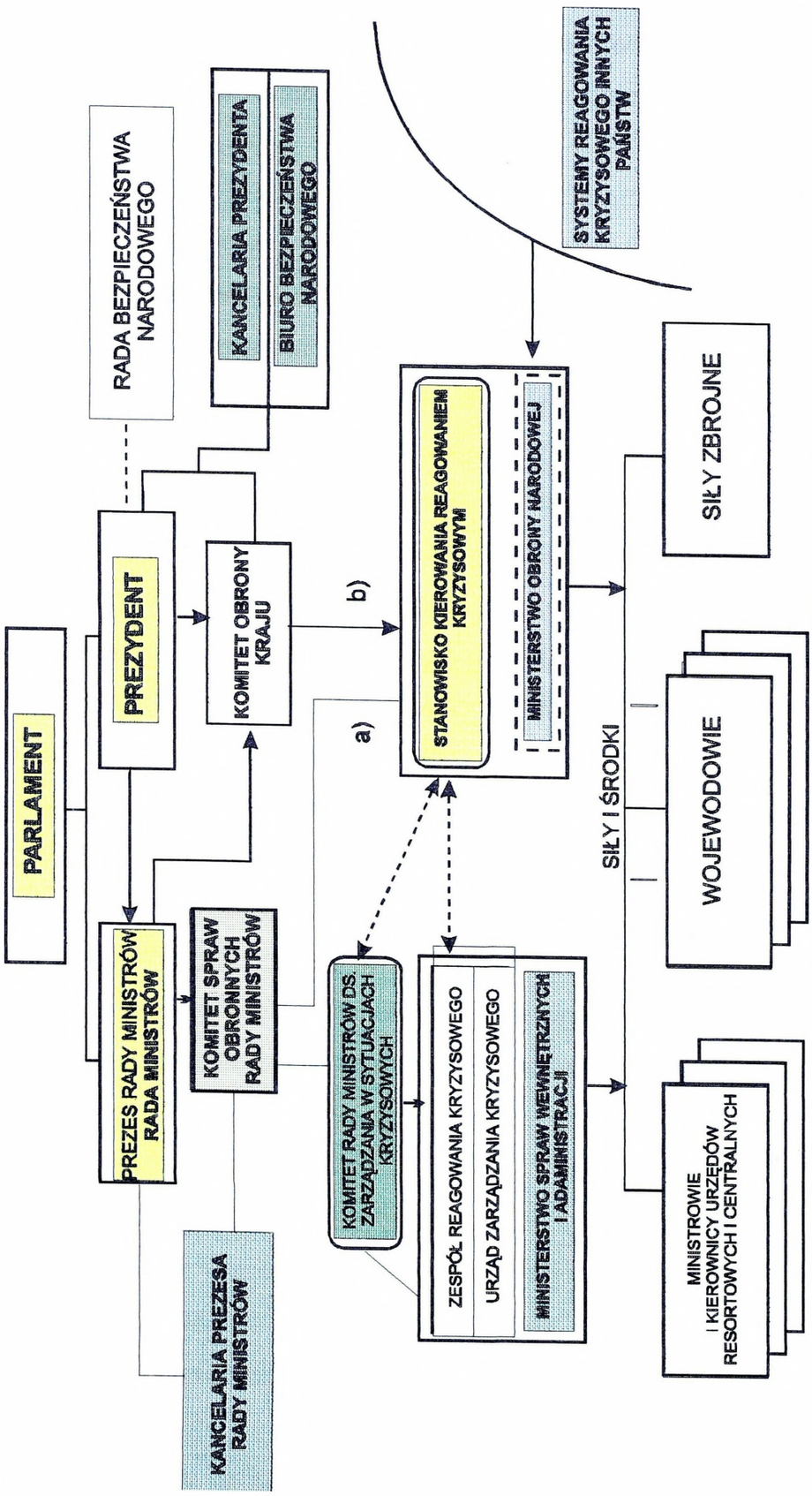
Podstawowym źródłem informacji, o symptomach kryzysu polityczno-militarnego, oprócz oficjalnych komunikatów i kontaktów zagranicznych, są służby dyplomatyczne i służby informacyjne, które nie podlegają bezpośrednio Sejmowi i Prezydentowi RP. Oficjalnym źródłem informacji dla Sejmu i Prezydenta RP będzie Rada Ministrów.

Stąd też zasadnym jest, że Stanowisko Kierowania Reagowaniem Kryzysowym ds. kryzysów polityczno-militarnych usytuowane jest w resorcie podległym ministrowi obrony narodowej, jako naczelnemu organowi administracji państwowej w dziedzinie obronności, bezpośrednio odpowiedzialnemu przed Radą Ministrów za sprawy obronności państwa, w tym za stan i gotowość sił zbrojnych.

Na czas zagrożenia (kryzysu) i wojny podsystem kierowania obronnością rozwija się stopniowo (selektywnie) lub jednocześnie (całościowo) w wojenny system kierowania państwem. Rysunek 2.2.1. przedstawia system kierowania reagowaniem kryzysowym.

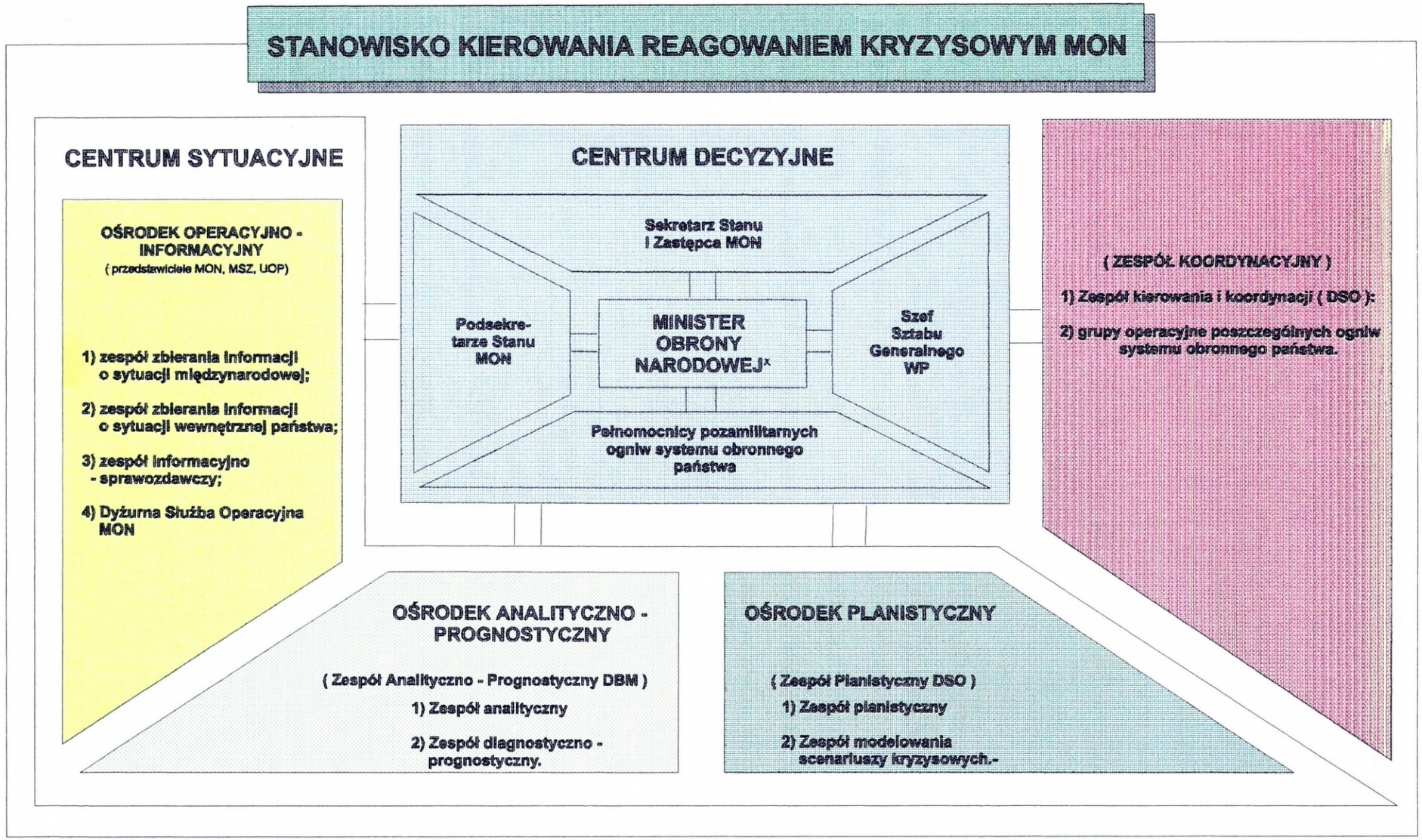
Przyjmuje się, że najwyższym polityczno-strategicznym ośrodkiem decyzyjnym w tym wypadku będzie prezydent. Premier będzie kierował całym układem pozamilitarnym, a siłami zbrojnymi - powołany na czas wojny Naczelny Wódz (Naczelny Dowódca Sił Zbrojnych RP).

Rysunek 2.2.2. prezentuje (jedną z wersji) strukturę i obsadę stanowiska kierowania reagowaniem kryzysowym. Utworzone w MON centrum reagowania na kryzysy polityczno-militarne dostarczałoby naczelnym organom informacji niezbędnych do podejmowania określonych decyzji.



a) wariant, gdy wiodącą rolę w reagowaniu na sytuację kryzysową spełnia Rada Ministrów
b) wariant, gdy wiodącą rolę w reagowaniu na sytuację kryzysową spełnia Komitet Obrony Kraju

Rys. 2.2.1. System kierowania reagowaniem kryzysowym



x w razie potrzeby decydent państwowy (premier, prezydent)

Rys. 2.2.2. STRUKTURA I OBSADA STANOWISKA KIEROWANIA REAGOWANIEM KRYZYSOWYM MON

2.3. Wpływ zagrożeń na funkcjonowanie systemu obronnego państwa

Dla utrudnienia i osłabienia relacji systemu obronnego państwa lub wręcz sparaliżowania jego sprawnego działania wystarczy podjąć kroki powodujące destabilizację struktury poszczególnych elementów składowych systemu obronnego państwa. Na schemacie 2.3.1[10] przedstawiono wpływ zagrożeń na system obronny państwa.

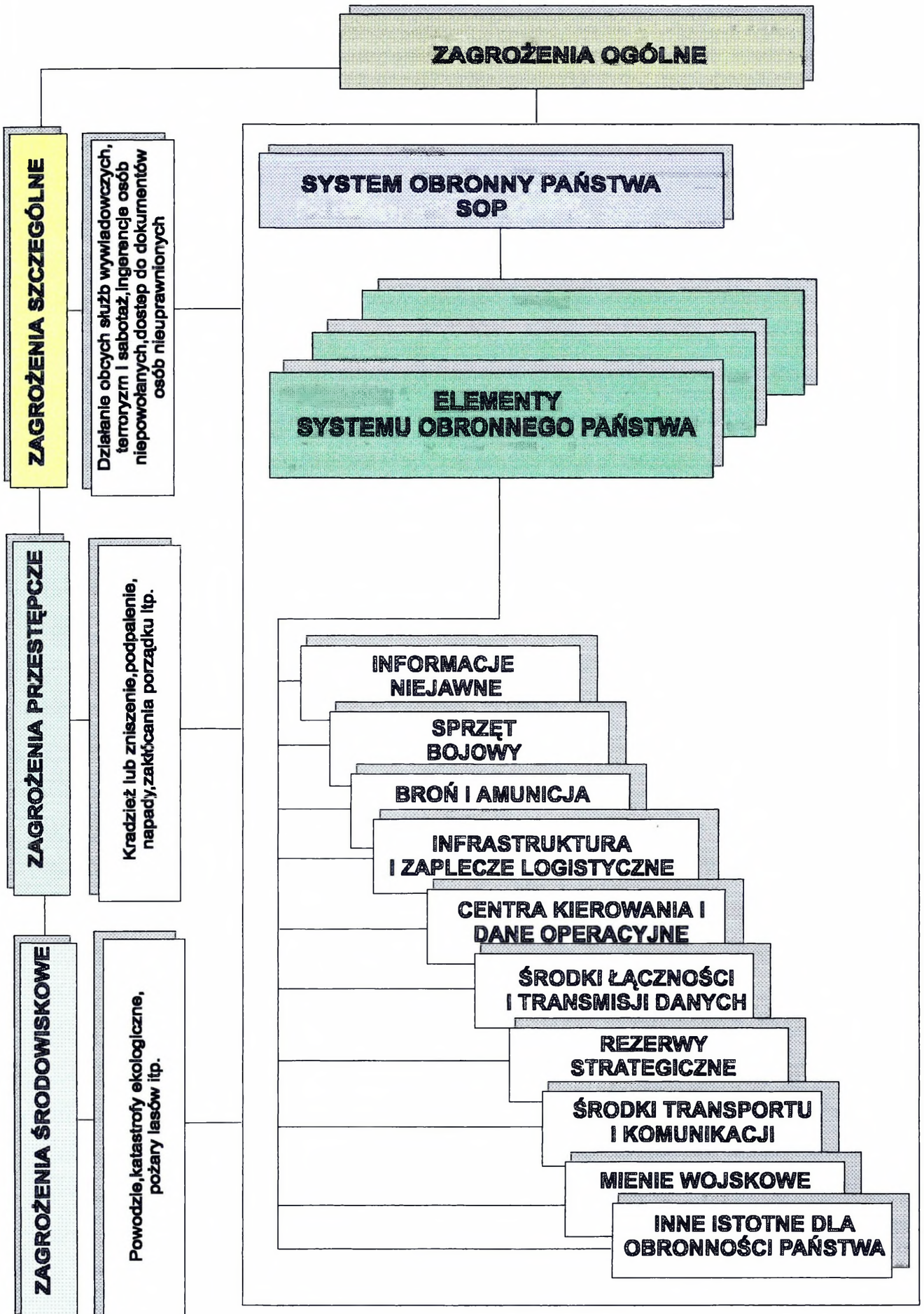
Działania takie mogą być:

- inspirowane z zewnątrz – penetracja przez obce służby wywiadowcze lub grupy terrorystyczne, np. spowodowane zaangażowaniem Polski w akcje i przedsięwzięcia militarne podejmowane w ramach NATO;
- inspirowane wewnątrz – skrajne działania wbrew prawu, np. blokowanie strategicznych węzłów komunikacyjnych, na tle ekonomicznym i socjalnym, spowodowane niezadowoleniem określonych grup społecznych;
- zorganizowane działania przestępcze, np. kradzież broni z jednostki wojskowej dla zasilenia grupy przestępczej;
- spontaniczne, jednostkowe akty przestępcze, np. kradzieże broni, amunicji, sprzętu wojskowego dla celów zarobkowych;
- inne, spowodowane wymuszeniem poprzez:
  - szantaż – np. zagrożenie życia, kompromitację osoby zajmującej wysokie stanowisko polityczne itp.,
  - uzależnienie – alkohol, narkotyki itp.,
- kombinacje wymienionych wyżej zagrożeń.

Należy podkreślić, że zagrożenia te znajdują się we wzajemnych relacjach. Sfera zagrożeń militarnych i niemilitarnych ma wpływ na przestępczość o charakterze ogólnym i szczególnym. Obce służby wywiadowcze mogą wykorzystać objawy zamieszek i niezadowolenia społecznego na tle ekonomicznym czy religijnym, itp. do działań terrorystycznych lub sabotażowych skierowanych przeciwko elementom systemu obronnego państwa. Istnieje duże prawdopodobieństwo, że wrogie Polsce siły mogą zaangażować miejscowy element przestępczy lub osoby powiązane bezpośrednio lub pośrednio z obiektem będącym elementem systemu obronnego państwa dla celów wywiadowczych lub terrorystyczno-sabotażowych, poprzez zakup usługi lub informacji albo szantaż.

---

[10] Opracowanie własne A.Wójcik.



Schemat 2.3.1. Wpływ zagrożeń i ich relacje na funkcjonowanie systemu obronnego państwa

Przestępczość jako zagrożenie bezpieczeństwa

Przez „przestępczość" rozumie się zbiór czynów zabronionych ustawowo pod groźbą kary, a popełnianych na obszarze danej jednostki terytorialnej. Przestępczość jest zjawiskiem społecznym, które charakteryzuje się następującymi cechami[11]:

- stanowi zagrożenie dla obowiązującego porządku prawnego;
- wyraża się we wzroście liczby osób, które popełniły przestępstwa w stosunku do ogółu ludności.

Wśród czynników determinujących przestępczość i jej poziom można wyodrębnić czynniki:

- o charakterze szczególnym, tj. cechy osobiste przestępcy, układy sytuacyjne, zachwianie równowagi psychicznej, frustracje jednostek i grupy społecznej, rozpad więzi nieformalnych, nieprawidłowości w działaniu organizacji formalnych, alkoholizm, rodziny dysfunkcjonalne, wadliwe działania systemu oświatowego i wychowawczego;
- o charakterze ogólnym, tj. nędzę, niesprawiedliwość i konflikty społeczne, nierówny podział bogactw, niski stan zdrowotny społeczeństw, dominację jednej grupy społecznej nad innymi, frustracje wywołaną niespełnieniem podstawowych potrzeb związanych z egzystencją ludzką, masowy wyzysk, nierówność możliwości życiowych i nieszczęścia powodowane przez człowieka;
- o charakterze legislacyjno - prawnym, tj. rygorystyczność kodeksów i przepisów prawnych pozostających w niezgodzie z poglądami społeczeństwa, przestarzałe lub nieprzychylne ludziom ustawodawstwa stosowane w sposób sztywny wobec wielu warstw społeczeństwa, mimo że rzeczywiście nie ma możliwości realizacji tego rodzaju przepisów ze względu na odmienność lub zmienioną obyczajowość, tradycje i wartości, albo z powodu konfliktu z przyjętymi i pielęgnowanymi środkami kontroli społecznej; bezrobocie, migracje ze wsi do miasta, konflikty wewnętrzne w kraju, działania wojenne (zewnętrzne), okupacja wrogiego kraju.

Przestępczość, ze względu na jej wagę, należy rozpatrywać w wymiarze krajowym i międzynarodowym. I tak obawę przed przestępczością jako największym zagrożeniem bezpieczeństwa obywateli wyraża: w Wielkiej Brytanii - 57,5%, w Holandii - 60,5%, w Niemczech - 63%, w Polsce - 64,5% a w Rosji - 74%. Ta kategoria zagrożenia wyprzedziła bezrobocie, obawę przed AIDS, narkotykami czy brakiem pieniędzy.[12]

---

[11] E. Drukheim *Zasady metody socjologicznej*, Warszawa 1968.
[12] Dyrda, wykład, *Psychospołeczne problemy zagrożenia bezpieczeństwa*, AON, Warszawa 1998.

Dane zawarte w przeglądach ONZ za lata siedemdziesiąte i osiemdziesiąte wskazują na tendencje do wzrostu przestępstw zarówno z użyciem przemocy (morderstwo, rabunek, napad), jak i przeciw własności (kradzież, oszustwo). Najwyższy udział w ogólnej przestępczości mają kradzieże (63%), następnie napady (18%), rabunek (6%), przestępstwa "narkotykowe" (6%), oszustwa i defraudacje (4%) oraz inne przestępstwa, tj. zabójstwo, gwałty, korupcja i uprowadzenia (3%).

Nastąpił znaczny wzrost liczby przestępstw związanych z użyciem przemocy (z 20% do 25%) i narkotykami (z 3,1% do 6%).[13] Rośnie liczba przestępstw zaliczanych do tzw. nowych form, jak nielegalny handel bronią i narkotykami.[14] Wzrost przestępczości i jej umiędzynarodowienie zagraża bezpieczeństwu państwa, potęguje strach jednostek i może być przyczyną pogorszenia się stosunków międzynarodowych.

Z analizy danych przedstawionych przez Interpol, Komendę Główną Policji i roczniki statystyczne wynika, że w Polsce w 1995 roku na 100 tys. mieszkańców przypadło ponad 2,5 tys. przestępstw ogółem. Ten sam wskaźnik w 1995 roku wyniósł:
w Finlandii -14823, we Włoszech - 3964, w Hiszpanii - 2317, w Szwajcarii - 4995, w Austrii - 6040, we Francji - 6316, w Niemczech 8138, w Słowacji - 2136.

Wśród podstawowych kategorii przestępstw, które są najbardziej interesujące z punktu widzenia określenia zagrożenia obiektów wojskowych, możemy wyliczyć: zabójstwa, kradzież mienia, kradzież z włamaniem do obiektu, zagarnięcie mienia.

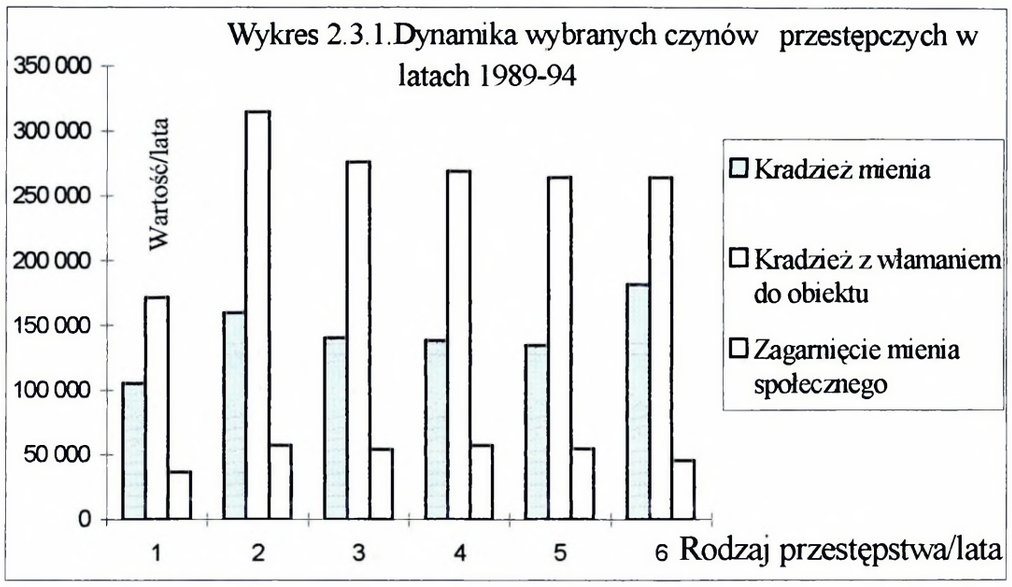
W analizie niniejszej pracy nie ujęto danych dotyczących działań przestępczych typu terroryzm i szpiegostwo.

W tabeli 2.3.1 zaprezentowano dynamikę przestępstw przeciwko mieniu w latach 1989-94.

Tab. 2.3.1. Niektóre rodzaje przestępstw stwierdzonych w latach 1989-1994

Lp	Rodzaj przestępstwa/rok	1 989	1 990	1 991	1 992	1 993	1 994
1	Kradzież mienia	105 129	158 785	139 507	137 510	134 089	180 514
2	Kradzież z włamaniem do obiektu	171 156	313 691	275 308	267 774	263 244	263 244
3	Zagarnięcie mienia społecznego	36 267	56 646	53 872	56 760	54 311	45 018

[13] Op. cit.U. Świętochowska.
[14] B. Hołyst, *Kryminologia*, Warszawa 1994.



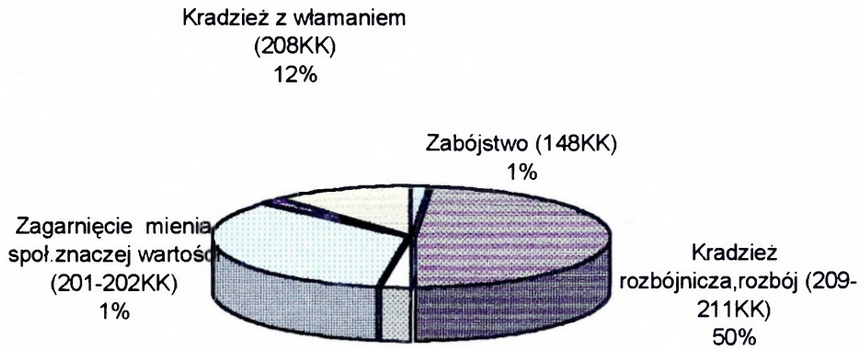
Z tabeli 2.3.1. oraz wykresu nr 2.3.1. wynika, że dynamika przestępstw przeciw mieniu utrzymuje się praktycznie na tym samym poziomie i ulega niewielkim zmianom.

Na podstawie tabeli 2.3.2. można stwierdzić, że kategoria ciężkich przestępstw utrzymuje się na wysokim poziomie, a w wypadku zabójstw - wzrasta.

Tabela 2.3.2. Przestępczość w okresie styczeń 1997/styczeń 1998 – dane ogólnokrajowe z raportu Komendy Głównej Policji, Warszawa luty 1998

Kwalifikacja prawna	1 997	1 998	WD*
Zabójstwo (148KK)	63	75	119,00
Kradzież rozbójnicza, rozbój (209-211KK)	2 040	1 851	90,70
Kradzież z bronią (210&2KK)	97	85	87,60
Kradzież mienia (203, 208KK) powyżej 50tys.	1 446	263	18,20
Kradzież z włamaniem (208KK)	492	55	11,20
Zagarnięcie mienia społ. znacznej wartości (201-202KK)	63	53	84,10

*gdzie WD oznacza wskaźnik dynamiki, który jest procentowym stosunkiem odpowiadających sobie liczb w roku bieżącym i ubiegłym lub w innych okresach porównawczych



Wykres 2.3.2.Udział % wybranych czynów przestępczych w okresie 1997/1998

Z analizy tabeli 2.3.2. i wykresu 2.3.2. wynika, że przestępstwa kradzieży rozbójniczej (50%), kradzieży mienia powyżej 50 tys. zł (34%) i kradzieży z włamaniem (12%) stanowią podstawową kategorię zagrożeń dla obiektów, w tym dla obiektów wojskowych.

Wszystkie działania mające na celu zabezpieczenie techniczno-organizacyjne obiektu wojskowego powinny uwzględniać poziom tych przestępstw, sięgający w tym ujęciu 96% udziału wszystkich rozpatrywanych przestępstw.

Spadek zagrożenia przestępczością w 1996 r. (o blisko 8% zdarzeń) wg przewidywań specjalistów wydaje się mieć charakter przejściowy, będący następstwem ustawowego przesunięcia przestępstw o mniejszych stratach materialnych do kategorii wykroczeń. Poparciem tej tezy jest utrzymywanie się od 1995 r. stałej tendencji realnego zagrożenia przestępczością w Polsce w ilości 700 tys. przestępstw stwierdzonych w ciągu 9 miesięcy 1997 r., tj. o 10,9% więcej niż w analogicznym okresie 1996 r.[15] Obserwowany obecnie rozwój przestępczości wpływa w znacznym stopniu na patologizację życia publicznego w Polsce. Sytuacja staje się tym groźniejsza, że następuje dynamiczny wzrost przestępstw zagrożonych wysokim wyrokiem a jednocześnie obniżył się wiek sprawców popełnianych przestępstw.

Od 1993 roku obserwowane są niekorzystne zjawiska w strukturze przestępstw w szczególności:

- wzrosło zagrożenie przestępstwami przeciwko życiu i zdrowiu oraz mieniu, charakteryzującymi się agresją, przemocą i bezwzględnością wobec ofiar;
- poważny wzrost użycia broni w stosunku do pokrzywdzonych oraz interweniujących policjantów czy innych służb;

[15] B. Hołyst, *Ocena bezpieczeństwa w Polsce*, Konferencja SECUREX'98.

- nasilenie przestępstw o charakterze porachunkowym, tj. zabójstwa, rozboje, pobicia oraz terroryzm kryminalny;
- wzrosła liczba grup przestępczych oraz pogłębił się ich profesjonalizm, czyli obserwuje się więcej przestępstw zaplanowanych i przeprowadzonych w sposób zorganizowany i grupowo;
- coraz częstszy udział w przestępstwach obywateli państw obcych działających w grupach przestępczych na terenie Polski;
- nasilenie przestępstw popełnianych przez nieletnich;
- wpływ tendencji światowych w zakresie przestępczości związanej z obrotem narkotykami.

Nastąpiło rozpowszechnienie się broni palnej jako narzędzia przestępstwa. Świadczy o tym liczba egzemplarzy broni odebranej od nielegalnych posiadaczy: z 876 w 1991 r. do 3106 w 1996 r., tj. ponad 3,5-krotny wzrost. Środowisko przestępcze wykorzystuje nowe źródła zaopatrzenia w broń:

- przemyt z państw ościennych;
- przesyłki pocztowe z USA i Kanady;
- przeróbki broni gazowej na amunicję ostrą;
- nabywanie broni w licencjonowanych punktach sprzedaży na podstawie sfałszowanych dokumentów;
- napady i włamania do magazynów broni.

Do obiektów szczególnie zagrożonych należą: stacje paliw, kantory wymiany walut, wiejskie placówki bankowe oraz inne instytucje finansowe, np. poczty. Do niepokojących zjawisk należy kradzież broni i materiałów, która często jest zorganizowana i zaplanowana w sposób profesjonalny.

Narastającym problemem jest zorganizowana przestępczość cudzoziemców. W 1996 r. jednostki pionu do walki z przestępczością zorganizowaną rozpoznały 377 aktywnych grup przestępczych i zidentyfikowały 4.744 ich członków, w tym 158 grup o składzie międzynarodowym z udziałem 522 osób z 37 państw, głównie z Ukrainy, Rosji, Niemiec oraz Ormian, Wietnamczyków, Albańczyków, Latynosów, Cyganów i Bułgarów.

Główne kierunki działania zorganizowanych grup przestępczych obejmują:

- przestępstwa związane z produkcją, obrotem i przemytem narkotyków - 66 grup;
- wymuszenia rozbójnicze, haracze, okupy, napady i porachunki - 60 grup;
- zorganizowane formy przestępczości gospodarczej - 40 grup;
- fałszerstwa pieniędzy i ich dystrybucja - 28 grup;

- przemyt towarów na wielką skalę - 27 grup;
- pranie brudnych pieniędzy - 20 grup;
- obrót bronią i materiałami wybuchowymi - 14 grup;
- fałszerstwa dokumentów i ich dystrybucja - 9 grup;
- terroryzm bombowy - 5 grup.

Na podstawie badań CBOS można stwierdzić, że w ciągu 6 lat nastąpiło znaczne obniżenie poczucia bezpieczeństwa obywateli. W latach 1987-1993 nastąpiło przewartościowanie przez badanych oceny Polski jako kraju, w którym żyje się bezpiecznie a w ciągu lat 1994-1995 umocniło się przekonanie społeczne, że Polska nie jest bezpiecznym krajem. Obecnie już tylko co czwarty badany zamieszkujący bezpieczną i spokojną miejscowość (zdaniem badanego) uważa Polskę za kraj bezpieczny. W 1993 r. twierdził tak co trzeci ankietowany.

Przestępczość w wojsku na tle zagrożenia bezpieczeństwa w Polsce[16] kształtuje się następująco, w pierwszych 10 miesiącach 1998 roku nastąpił 10% wzrost wszczętych spraw przez prokuratury przeciwko wojskowym sprawcom przestępstw w stosunku do podobnego okresu 1997 roku.[17] Kiedy przyjrzymy się wojsku, zauważymy, że wszelkie naruszenia norm prawnych są podobne do tego, co dzieje się w społeczeństwie. Potwierdza to fakt, że armia nie jest układem odosobnionym. Stanowi skomplikowany system, który jest w relacji z całym układem społeczno - gospodarczym i jego patologicznymi konsekwencjami.

Stąd też znajdujemy wiele alarmujących artykułów w prasie o przestępczości w wojsku.

Z tych relacji wynika, że:[18]

- obiekty wojskowe są niedostatecznie chronione pod względem fizycznym;
- występujący brak odpowiedniego dozoru organizacyjnego nad mieniem wojskowym sprzyja czynom przestępczym;
- niedostateczny poziom wiedzy dotyczący ochrony technicznej praktycznie na wszystkich szczeblach dowodzenia;
- obecny system ochrony techniczno - organizacyjnej obiektów wojskowych umożliwia w dużej mierze penetrację elementów przestępczych, a tym bardziej profesjonalnie przygotowanych grup dywersyjno – terrorystycznych;
- brak systemów alarmowych umożliwiających automatyczną kontrolę i nadzór nad służbami odpowiedzialnymi za ochronę obiektów wojskowych;

---

[16] Zagrożeniach ze strony zorganizowanej przestępczości w wojsku zawiera załącznik nr 2.5.

[17] *Mniejsza armia, więcej przestępstw*, Kurier Polski z 14.12.1998.

[18] *Jednostka wojskowa łatwym łupem?*, Życie Warszawy z 15.12.1998, *Dziurawe ogrodzenie wojskowej jednostki*, Rzeczypospolita 15.12.1998.

- obserwowany jest wzrost kategorii przestępstw związanych z zaborem broni i amunicji.

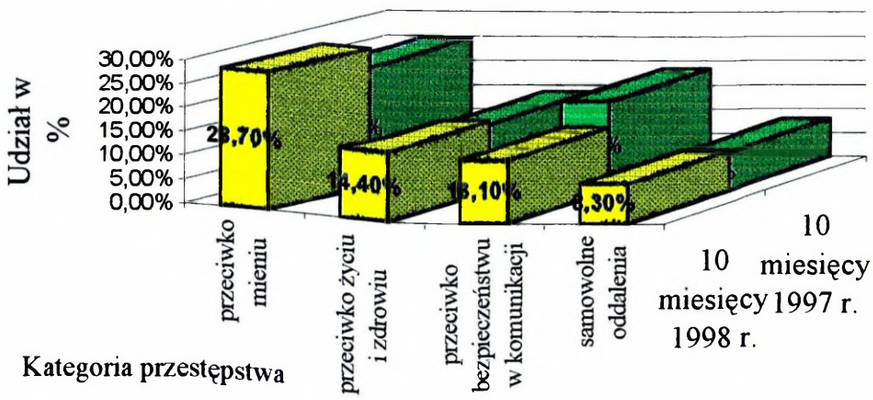
W 1998 roku w wojsku zginęło dwa razy więcej broni i amunicji niż w 1997 r. Z trzydziestu trzech odnotowanych przypadków większość to kradzieże dokonane przez żołnierzy służby zasadniczej[19]. Znaczący wpływ na to, że wzrasta liczba rabunków i przestępstw przeciwko mieniu ma fakt, iż do zasadniczej służby wojskowej przyjmowane są osoby, które w cywilu weszły w konflikt z prawem, co w latach 80-tych nie miało miejsca.[20]

Jednocześnie statystyki potwierdzają, że w porównaniu z rokiem ubiegłym zmniejszyła się znacznie liczba przestępstw, których sprawcami są żołnierze zawodowi.

Tabela 2.3.3. Kategorie wybranych przestępstw w wojsku

Kategoria przestępstwa	10 miesięcy 1998 r.	10 miesięcy 1997 r.
Przeciwko mieniu	28,70%	24,70%
Przeciwko życiu i zdrowiu	14,40%	13,50%
Przeciwko bezpieczeństwu w komunikacji	13,10%	18,40%
Samowolne oddalenia	8,30%	7,90%

Wykres 2.3.3.Przestępczość w wojsku 1997/98



Z dotychczasowych doświadczeń innych państw wynika, że w wojsku mogą wystąpić niekorzystne zjawiska związane ze wzrostem liczby przestępstw związanych z rozprowadzaniem narkotyków wśród żołnierzy, przestępczością zorganizowaną kierowaną przez osoby cywilne, w których uczestniczy kadra zawodowa, a także przestępstwa gospodarcze polegające często na fałszowaniu dokumentów finansowych, defraudacjach, nadużyciach obowiązków i uprawnień,. Duże zagrożenie mogą stanowić przestępstwa związane z wykorzystaniem komputerów, np. do kradzieży środków finansowych z kont, wykradaniu tajemnicy służbowej, itd.

---

[19] *Broń pod nieszczególną kontrolą*, Polska Zbrojna nr 17, kwiecień 1999.
[20] Wg *Mniejsza armia, więcej przestępstw*, odsetek poborowych, który miał konflikt z prawem w cywilu wynosi 5%.

Wnioski

Dotychczasowe rozważania pozwalają wysnuć podstawowy wniosek, że na system obronny państwa mają wpływ sytuacje kryzysowe[21]:

- pośrednie – takie, których źródło powstania ma charakter często zewnętrzny i jego rozwój nie dotyczy bezpośrednio państwa, ale ze względu na powiązania polityczne, gospodarcze i militarne może mieć wpływ na stan bezpieczeństwa kraju, a w szczególności na elementy wchodzące w skład struktury obronnej,
- bezpośrednie – takie których powstanie i rozwój odbywa się na terytorium państwa i przyjmuje różnorodne formy zagrażające bezpieczeństwu państwa, a tym samym obiektom wojskowym.

Sytuacje kryzysowe mogą być przyczyną szeregu różnorodnych potencjalnych źródeł zagrożeń dla systemu obronnego państwa wraz z elementami składowymi, jakimi są obiekty wojskowe. Źródła zagrożeń mogą mieć przyczyny we wszystkich sferach funkcjonowania państwa.

Istniejące rozwiązania w zakresie systemów ochrony obiektów wojskowych oraz ocena stanu krajowych rozwiązań w tym zakresie i istniejące akty prawne, normatywne wymagania i wytyczne potwierdzają konieczność ochrony obiektów wojskowych nowoczesnymi systemami ochrony, które mogą sprostać potencjalnym źródłom zagrożeń, wynikającym z sytuacji kryzysowych dla systemu obronnego państwa.

Z przeprowadzonej analizy wyników badań i literatury przedmiotu wynika ścisły związek przyczynowy pomiędzy stanem i sytuacją w zakresie bezpieczeństwa powszechnego państwa a zagrożeniami systemu obronnego.

Powiązanie to jest ścisłe i wynika z następujących przyczyn powstawania zagrożeń tj. ekonomicznych, społecznych, politycznych, psychologicznych, historycznych, etnicznych, kulturowych, językowych, terytorialnych, wyznaniowych, ekologicznych i wojskowych.

System obronny państwa nie jest układem odosobnionym i podlega takim samym prawom i zasadom funkcjonowania jak inne systemy wchodzące w skład struktury państwa.

System obrony państwa wraz z jego powiązaniami organizacyjno-funkcjonalnymi i elementami składowymi podlega zagrożeniom polityczno-militarnym i niemilitarnym.

W celu neutralizacji zagrożeń niemilitarnych należy zastosować ochronę organizacyjno - funkcjonalną i techniczną ważnych ogniw systemu obronnego państwa.

Szczególne niebezpieczeństwo wynika z zagrożeń o charakterze terrorystycznym, sabotażowym, wywiadowczym, itd.

---

[21] Opracowanie własne A. Wójcik.

Obiekty o znaczeniu strategicznym dla obronności państwa nie są dostatecznie przygotowane do ochrony przed tymi zagrożeniami.

Ochrona elementów systemu obronnego państwa może zostać skutecznie zrealizowana za pomocą systemów ochrony, tj. systemów sygnalizacji zagrożeń i alarmowych.

W dalszych rozważaniach dotyczących zagrożeń i sposobów ich neutralizacji za pomocą systemów ochrony występuje element systemu obronnego państwa pod nazwą „obiekt wojskowy".

Dotychczasowe rozważania oraz przytoczone dane zarówno statystyczne, jak i informacje z mass mediów wskazują, że stan bezpieczeństwa obiektów wojskowych nie stoi na zadowalającym poziomie organizacyjnym i technicznym, a w obiektach należących do podstawowej struktury obronnej państwa, np. jednostkach wojskowych jest wręcz niski. Dlatego też, należy podjąć metodyczne i merytoryczne działania w celu ochrony obiektów wojskowych na poziomie techniczno - organizacyjnym odpowiadającym wzorom zachodnim.

Ochrona fizyczna obiektów wojskowych, wykonywana najczęściej przez żołnierzy służby zasadniczej jest mało skuteczna i nieefektywna, często prowadzona bez odpowiedniego nadzoru i kontroli, a jest często także przyczyną czynów przestępczych lub umożliwia ich dokonywanie.

Staje się konieczna i nieodzowna efektywna ochrona strategicznych obiektów wojskowych, jedynym rozwiązaniem jest zastosowanie automatycznych zintegrowanych systemów sygnalizacji zagrożeń i alarmowych, nadzorowanych przez wykwalifikowane kadry przygotowane do ochrony obiektów wojskowych. Ochrona fizyczna elementów systemu obronnego państwa ma istotne znaczenie podczas uczestniczenia Polski w działaniach w ramach NATO, ponieważ ilość potencjalnych zagrożeń i relacji między nimi szczególnie wzrasta podczas zaangażowania państwa w akcje prowadzone przez NATO.

Może to mieć istotny wpływ na bezpieczeństwo elementów systemu obronnego państwa, a tym samym na cały funkcjonujący system obronny państwa.

3. ANALIZA PORÓWNAWCZA SYSTEMÓW SYGNALIZACJI ZAGROŻEŃ I OCHRONY OBIEKTÓW WOJSKOWYCH WYKORZYSTYWANYCH W POLSCE I WYBRANYCH PAŃSTWACH NATO

3.1. Potrzeby systemu obronnego państwa w zakresie ochrony obiektów wojskowych

Organa władzy i administracji rządowej, podejmując decyzje na różnych szczeblach kierowania politycznego, ekonomicznego, gospodarczego i wojskowego, muszą dziś dobrze znać prawa rządzące systemami, aby zminimalizować prawdopodobieństwo popełnienia błędów.

System obronny państwa, jak każdy złożony obiekt stanowiący całość tworzącą zbiór obiektów elementarnych (elementów) i powiązań (relacji) między nimi, podlega oddziaływaniom zewnętrznym. Wszelkim relacjom podlega także jeden z elementów systemu obronnego państwa, jakim jest podsystem ochrony obiektów. Na stan bezpieczeństwa obiektów wojskowych będą miały niewątpliwie wpływ sytuacje szczególnie trudne, traktowane jako powtarzające się zjawiska indywidualne, które można określić jako krytyczne sytuacje systemowe. Krytyczne sytuacje wywołują zagrożenia bezpieczeństwa obiektu. Do takich sytuacji zaliczamy[1]:

- sytuacje konfliktowe – system znajduje się w polu sił przeciwstawnych (sił fizycznych, sprzecznych interesów, nacisków społecznych lub moralnych, itd.);
- sytuacje zagrożenia – znacznie wzrasta (poza poziom bezpieczeństwa) prawdopodobieństwo niebezpiecznego naruszenia wartości głównych cech systemowych organizacji (np. równowagi, stabilności, spójności, kreatywności, itp.);
- sytuacje kryzysowe – zmiany funkcjonowania i (lub) strukturalne w systemie prowadzą do dezorganizacji jego działania (np. głębokiej nierównowagi, chaosu, regresu, itp.).

Można przyjąć, że w systemowych sytuacjach kryzysowych organa kierownicze (kierownictwo) może popełniać błędy. W systemach mogą być popełniane:

- błędy orientacji – następują w procesach informacyjnych z powodu głębokiej luki informacyjnej albo też nadmiaru informacji zbędnych;
- błędy decyzji – zdarzają się w procesach decyzyjnych z powodu braku umiejętności (lub warunków) dokonywania racjonalnych wyborów celów, sposobów i środków działania;
- błędy realizacji – zdarzają się w procesach roboczych (wykonawczych) z powodu braku umiejętności (lub warunków) wykonywania powziętych decyzji.

---

[1] P. Sienkiewicz *Analiza systemów. Podstawy i zastosowania.* Bellona, Warszawa 1994.

Poza błędami o charakterze incydentalnym większość błędów bierze się z istnienia tzw. barier efektywności. Przez barierę efektywności w organizacji określany jest zespół czynników, względnie stałych (strukturalnych, funkcjonalnych i rozwojowych), ugruntowanych na tradycji, doświadczeniach, nawykach, niekiedy ustaleniach doktrynalnych, które trwale uniemożliwiają efektywne działanie (wzrost efektywności). Można wyróżnić barierę:

- informacyjną;
- decyzyjną;
- realizacji.

Każda z tych barier rodzi swoiste przyczyny i przynosi charakterystyczne skutki. Narzędziem racjonalnej analizy związków przyczynowo-skutkowych, w kontekście owych barier efektywności jest analiza systemowa, która służy przede wszystkim znalezieniu środków pokonania barier lub niedopuszczenia do ich powstania.

Zminimalizowanie lub wręcz eliminację błędów podczas występowania różnych sytuacji oraz barier efektywności w zakresie ochrony obiektów wojskowych możemy uzyskać dzięki automatyzacji i wspomaganiu procesów analizy i decyzji, w którym niezależnie od stopnia zagrożenia i zakłóceń sprawdzona procedura w znacznym stopniu zmniejszy poziom ryzyka popełnienia błędu lub zaniechania realizacji.

We współczesnym świecie wzajemne stosunki podmiotów międzynarodowych można określić przez dwa rodzaje związków i relacji. Pozytywne (konstruktywne), które sprzyjają budowaniu wzajemnego zaufania oraz negatywne (destabilizujące), które rodzą nieufność i podejrzliwość. Wymienione rodzaje stosunków międzynarodowych rodzą potencjalne zagrożenia dla systemu, elementów i relacji systemu obronnego państwa, m.in. dla systemu ochrony obiektów wojskowych.

Zagrożenia militarne stały się we współczesnym świecie najważniejszymi obok zagrożeń gospodarczych czynnikami globalnymi, mającymi wpływ na stabilizację życia w regionach i na świecie. Zagrożenia militarne mogą powstać na podłożu: ekonomicznym, politycznym, etnicznym, społecznym, psychologicznym, religijnym, ekologicznym, wojskowym. W strukturze nowo powstałego systemu międzynarodowego wzrasta znaczenie zagrożeń gospodarczych.

Źródłem konfliktu może się stać narastanie międzynarodowych czy regionalnych dysproporcji rozwojowych, np. między bogatą „Północą" a biednym „Południem".

Do ekonomicznych przyczyn powstawania zagrożeń należą: recesja gospodarcza, restrykcje ekonomiczne, embargo handlowe, ograniczenia kredytowo-finansowe, zadłużenie państwa, status materialny obywateli, nadmierne zróżnicowanie rozwojowe regionów, stan

budżetu państwa, błędy w procesach prywatyzacji i reprywatyzacji, wykup ziemi i obiektów przemysłowych przez obcy kapitał, urynkowienie usług i świadczeń socjalnych.

Poziom rozwoju gospodarczego i sytuacja ekonomiczna państwa ma ścisły związek ze sferą psychiczną, nastrojami społecznymi i poczuciem bezpieczeństwa. Do społecznych przyczyn powstawania zagrożeń militarnych należą: podział etniczny i wyznaniowy, antagonizmy plemienne, stan bezrobocia, stan bezpieczeństwa osobistego obywateli, stan przestrzegania swobód obywatelskich, stan bezpieczeństwa socjalnego, pauperyzacja społeczeństwa, dostępność do oświaty, nauki, kultury i wypoczynku, różnice statusu materialnego.

Do psychologicznych przyczyn powstawania zagrożeń militarnych należą: poczucie zagrożenia praw i swobód obywatelskich, patologiczne zachowanie społeczeństwa, apatia społeczeństwa, aktywność środków propagandy.

Rosnąca współzależność między państwami i globalizacja wpływów może spowodować ekologiczne kryzysy i konflikty, których przyczynami może być: degradacja środowiska naturalnego, próby z bronią nuklearną, katastrofy transportów ze środkami toksycznymi, wwóz do kraju odpadów poprodukcyjnych, awarie elektrowni atomowych, zanieczyszczenia przemysłowe środowiska, stan utylizacji odpadów środków radioaktywnych.

Polityka, uwarunkowana zdobyciem lub utrzymaniem władzy może, być źródłem powstawania lub wykorzystywania sytuacji konfliktowych. Do zagrożeń militarnych powstałych z przyczyn politycznych należą: rozchwianie sceny politycznej, niestabilność państwa, szantaż polityczny, dyskredytowanie władzy, transformacja ustrojowa, izolacja polityczna, terroryzm polityczny.

Do zagrożeń militarnych mających podłoże wojskowe należą: stan produkcji zbrojeniowej, wielkość potencjału obronnego państwa, charakter doktryny wojennej, dyslokacja jednostek wojskowych, struktura organizacyjna sił zbrojnych, stan budżetu ministerstwa obrony, charakter szkolenia wojsk, wydatki zbrojeniowe sąsiadów, wyposażenie techniczne wojsk.

Na stan bezpieczeństwa systemu obronnego państwa, a tym samym poziom zagrożenia obiektów wojskowych, niewątpliwie ma wpływ zjawisko terroryzmu. Terroryzm jest jednym z najpoważniejszych zagrożeń militarno - nacjonalistycznych. Rozumiany jako postać walki prowadzonej przez określone siły, mające na celu zdobycie lub utrzymanie władzy, może przybrać postać:

- terroryzmu powstańczego – społeczno-rewolucyjnego, separatystycznego i niepodległościowego;

- terroryzmu represyjnego – akty gwałtu tajnych organizacji w celu wymuszenia realizacji określonych celów;
- terroryzm reżimowy – represje władzy wobec opozycji politycznej.

Terroryzm stanowi jeden z najbardziej konfliktogennych czynników społeczno-politycznych, sprzyjających wybuchowi konfliktów zbrojnych we współczesnym świecie. Należy mieć na uwadze nowe zjawisko przemocy mającej znamiona terroryzmu, a mianowicie aktywność organizacji o zabarwieniu nacjonalistycznym, neofaszystowskim czy subkultur młodzieżowych np. skinhedów, których motywacją działania jest często rasizm, wrogość do obcokrajowców, etnocentryzm, heterofobia, itd.. Zmienia się oblicze terroryzmu. W ostatnich latach pojawiły się nowe motywacje, nowe uzasadnienia, nowi przeciwnicy, co podważyło wiele podstawowych poglądów na temat terroryzmu i terroru (m.in. pogląd, że Polska jest poza jego zasięgiem działania). Dobrze znane radykalne organizacje lewicowe jak niemiecka Frakcja Czerwonej Armii, włoskie czerwone Brygady i działające od lat nacjonalistyczne i separatystyczne ugrupowania terrorystyczne, jak IRA i OWP zostały obecnie zastąpione przez grupy o mniej zrozumiałych celach ideowych, które stwarzają znacznie większe zagrożenie.

Z omówionych wyżej zagrożeń dla systemu obronnego państwa wynikają potrzeby ochrony obiektów wojskowych. Istnieje potrzeba skutecznego i efektywnego ich rozpoznawania oraz neutralizacji za pomocą systemów ochrony obiektów wojskowych systemu obronnego państwa.

3.2. Istniejące rozwiązania w zakresie ochrony obiektów wojskowych oraz ogólna charakterystyka wybranych systemów ochrony

Do podstawowych aktów prawnych i wymagań dotyczących ochrony obiektów należy zaliczyć:

- ustawy regulujące stan prawny i organizację ochrony obiektów i mienia;
- normy techniczne ;
- wymagania branżowe i szczegółowe;
- inne akty prawne dotyczące pośrednio strony technicznej i organizacyjnej ochrony obiektów.

Do pierwszej grupy można zaliczyć: ustawę o ochronie osób i mienia[2], ustawę o ochronie informacji niejawnych oraz szereg aktów dodatkowych dotyczących wycinkowych zagadnień.

Podstawową normą techniczną dotyczącą ochrony jest Polska Norma PN-93/E-08390 „Systemy alarmowe". Omawiana norma podaje ogólne wymagania co do klasyfikacji systemów

[2]Dz. U. Nr 114, poz.740, Dz.U.Nr 11, poz.95.

i wymagania grupowe dla poszczególnych elementów systemów alarmowych (urządzeń) oraz metody ich kwalifikacji i badań. Wymagania branżowe i szczegółowe zawierają wytyczne na ogół techniczne dotyczące ochrony obiektów podlegających prawnie określonym strukturom organizacyjnym lub podmiotom prawnym. W tym miejscu można wymienić, np.: wymagania techniczne urządzeń zabezpieczających wartości pieniężne, zasady podłączania do jednostek Policji systemów alarmowych z wytypowanych obiektów, tymczasowe normy zabezpieczenia w techniczne urządzenia sygnalizacyjne i alarmowe terenów, obiektów i mienia wojskowego[3].

Ustawa o ochronie informacji niejawnych stanowi podstawowy akt prawny regulujący ochronę informacji niejawnych oraz obejmujący pośrednio zagadnienia dotyczące ochrony obiektów wojskowych.

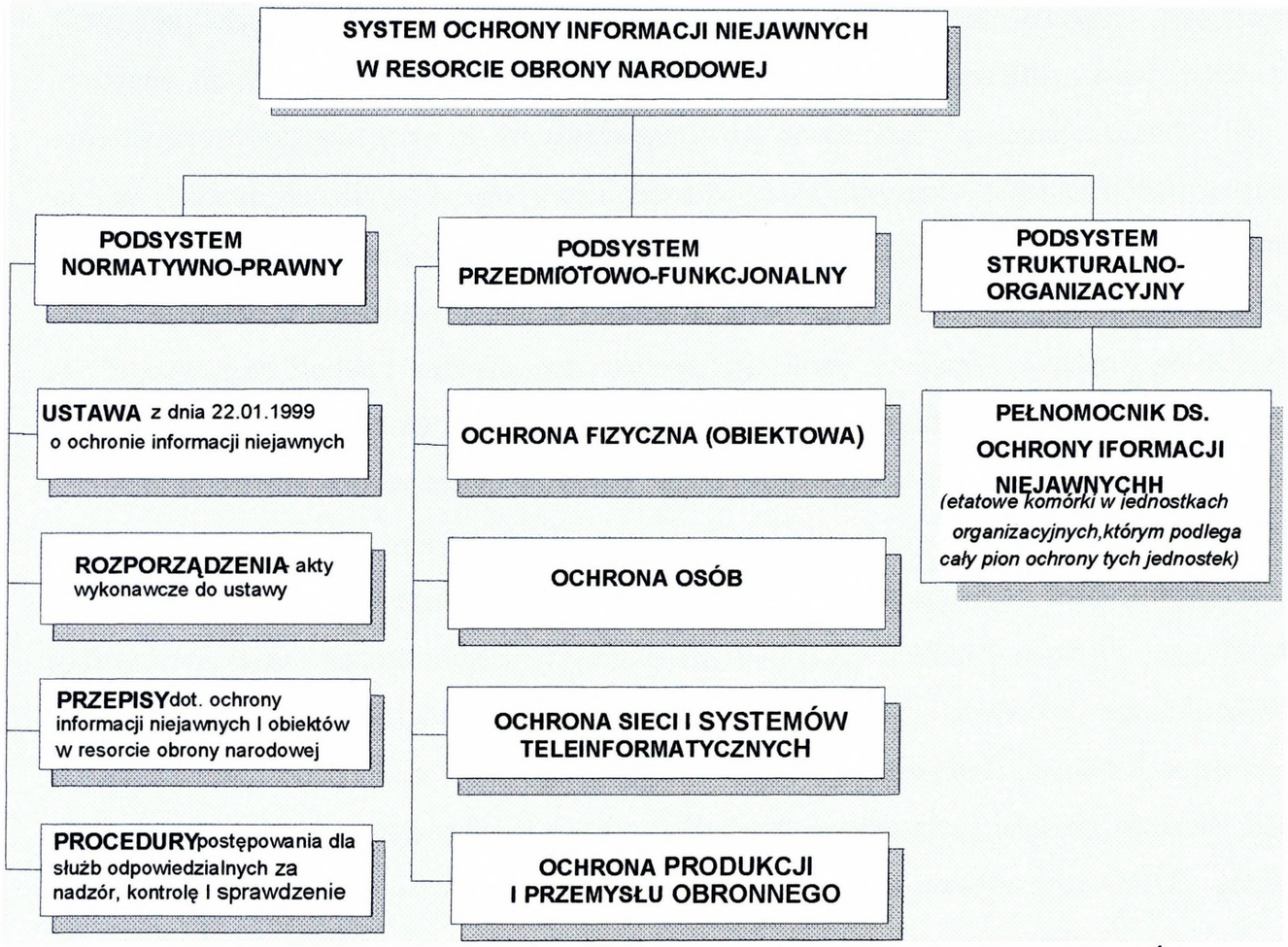
Wymieniona ustawa składa się z 13 rozdziałów oraz 2 załączników, w jej treści jest 12 delegacji do wydania aktów wykonawczych w trybie rozporządzeń. Akty te zostały opublikowane w Dzienniku Ustaw Nr 18, poz. 155-162 i 165-168. Ustawa przewidziała na podstawie art. 53 ust. 2 wydanie przez określonych kierowników resortów wewnętrznych uregulowań, dotyczących „szczegółowych zasad organizacji kancelarii tajnych, stosowania środków ochrony fizycznej oraz obiegu informacji niejawnych".

Ustawa obejmuje następujące rozdziały: przepisy ogólne, organizację ochrony informacji niejawnych, klasyfikację informacji niejawnych, udostępnienie informacji niejawnych, kancelarie tajne, kontrolę obiegu dokumentów; szkolenie w zakresie informacji niejawnych, środki ochrony fizycznej informacji niejawnych, bezpieczeństwo systemów i sieci teleinformatycznych, bezpieczeństwo przemysłowe, zmiany w przepisach obowiązujących, przepisy przejściowe. Przepisy ustawy stanowią podstawę do tworzenia wymagań w zakresie ochrony obiektów wojskowych.

Schemat 3.2.1. przedstawia system ochrony informacji niejawnych w resorcie obrony narodowej w świetle ustawy z dnia 22 stycznia 1999r. Zgodnie z ustawą o środkach ochrony fizycznej informacji niejawnych stosuje się je, w celu uniemożliwienia osobom nieupoważnionym dostępu do takich informacji, a szczególnie ochrony przed: działaniem obcych służb specjalnych, zamachem terrorystycznym lub sabotażem, kradzieżą lub zniszczeniem materiału; próbą wejścia osób nieuprawnionych; nieuprawnionym dostępem pracowników do materiałów oznaczonych wyższą klauzulą tajności. Do realizacji tych zadań służą organizacyjne i techniczne środki tworzące system ochrony obiektu wojskowego.

---

[3]Sztab Generalny WP, Zarząd Obrony Terytorialnej, Warszawa 1999.



Rys. 3.2.1. System ochrony informacji niejawnych w resorcie obrony narodowej[4]

Informacje niejawne muszą być przechowywane w następujących strefach bezpieczeństwa:

- Strefa I klasy jest to obszar, na którym jest przetwarzana lub przechowywana informacja niejawna od klauzuli POUFNE i wyższej w taki sposób, że wejście do tego obszaru praktycznie oznacza dostęp do wszystkich znajdujących się tam informacji niejawnych np. centra operacyjne, rejestry dokumentów, kreślarnie, itp. Strefa ta powinna posiadać jasno wytyczone i strzeżone granice, przez które wszelki wstęp i wyjścia są stale kontrolowane. Wstęp do tej strefy mają osoby odpowiednio sprawdzone i specjalnie upoważnione.
- Strefa II klasy jest to obszar, na którym jest przetwarzana lub przechowywana informacja niejawna od klauzuli POUFNE i wyżej w taki sposób, że może być ona zabezpieczona przed dostępem osób nieuprawnionych przez użycie środków wewnętrznych, np. oddzielne pomieszczenia biurowe. Strefa ta także wymaga jasno wytyczonych i strzeżonych granic, przez które wszelki wstęp i wyjścia są stale

[4] Materiały ze szkolenia w zakresie ochrony informacji niejawnych, WAT Wydział Elektroniki, 8.05.1999.

kontrolowane. Wstęp do tej strefy osób nieuprawnionych jest możliwy tylko z eskortą.

- Strefa administracyjna jest to strefa przylegająca do stref I i II klasy, w której możliwa jest kontrola osób i pojazdów. W strefie tej nie wolno przetwarzać i przechowywać informacji niejawnych.

Z powyższych wymagań wynika, że strefy bezpieczeństwa w obiektach wojskowych należy chronić systemami ochrony technicznej. Dlatego też dokonano charakterystyki podstawowych systemów technicznego zabezpieczenia obiektów wojskowych. Wszystkie informacje techniczne oraz rozszerzenia tematu dotyczące normatywnych i użytkowych stawianych tym systemom omówiono szeroko w załącznikach do niniejszej rozprawy (od nr 3.1. do nr 3.9.). Informacje zawarte w tym rozdziale umożliwiają poznanie przeznaczenia i zasad działania systemów ochrony, zakresu i wymagań techniczno - eksploatacyjnych oraz powiązań systemów (podsystemów) i ich elementów.

Obiekt chroniony to budynek lub zespół budynków (zgrupowanych lub rozrzuconych na określonej powierzchni), ogrodzony trwale lub tymczasowo lub bez widocznych fizycznych ograniczeń wstępu, posiadający zarówno architekturę naziemną, jak i (lub) podziemną.

Obiekt systemu obronnego państwa to obiekt lub grupa obiektów, które z racji przeznaczenia i funkcji pełnionych w strukturze organizacyjnej państwa należy do rzeczowych zasobów potencjału obronnego państwa.

Najczęściej omawianym chronionym obiektem należącym do systemu obronnego państwa jest jednostka wojskowa.

Ochrona obiektu to zespół przedsięwzięć i środków organizacyjno-technicznych uniemożliwiających (przynajmniej w znacznym stopniu utrudniających) przeniknięcie na teren obiektu intruza lub intruzów (osób niepowołanych lub nieuprawnionych) i dokonania czynów kryminalnych, w szczególności włamania, napadu lub aktów sabotażu, terrorystycznych, szpiegowskich, które w istotny sposób mogą osłabić, utrudnić lub sparaliżować działalność funkcjonalno-organizacyjną obiektu i struktur z nim związanych poprzez związki przyczynowo-skutkowe.[5] Dla wyjaśnienia definicji można wskazać przykład obiektu należącego do systemu obronnego państwa, w którym nastąpiło włamanie i skradziono plany mające wpływ na struktury obronne państwa.

System ochrony obiektu to zespół środków organizacyjno-technicznych w postaci służb ochrony fizycznej (załoga ochronna, agenci ochrony) i specjalistycznych środków technicznej

[5] Opracowanie własne A. Wójcik.

ochrony (systemów sygnalizacji zagrożeń i alarmowania) zorganizowanych według określonych zasad taktycznych i normatywnych wymogów ochrony danego obiektu.

System alarmowy to zespół środków i zasad taktycznych, mających na celu zapewnienie stanu bezpieczeństwa obiektu (człowieka lub mienia) w przestrzeni i czasie w celu zachowania jego podstawowej substancji funkcjonalnej. System alarmowy zgodnie z PN-93/E-08390-11 jest to instalacja elektryczna przeznaczona do wykrywania i sygnalizacji nienormalnych warunków, wskazujących na istnienie niebezpieczeństwa. W projekcie PN-EN-50131 system alarmowy nazywany jest instalacją elektryczną, która reaguje na ręczne lub automatyczne wykrycie istniejącego niebezpieczeństwa. Wg autora należy rozszerzyć definicję systemu alarmowego „o wczesne wykrywanie niebezpieczeństw i wezwanie do działań prewencyjnych w systemie alarmowym." W takim ujęciu definicja przyjmie następującą postać: „system sygnalizacji zagrożeń i alarmowania jest to instalacja elektryczna powiązana w system organizacyjny, wykorzystujący wszelkie środki techniczne, w postaci urządzeń i ich oprogramowania, przeznaczona do wczesnego wykrywania i przekazywania sygnałów o grożących niebezpieczeństwach obsłudze – wezwanie do działania - aby mogła ona uruchomić procedury interwencyjne w celu prewencyjnego odstraszania potencjalnych intruzów (przeciwników), a tym samym ochrony zasobów funkcjonalnych (ludzi lub mienia) chronionego obiektu."

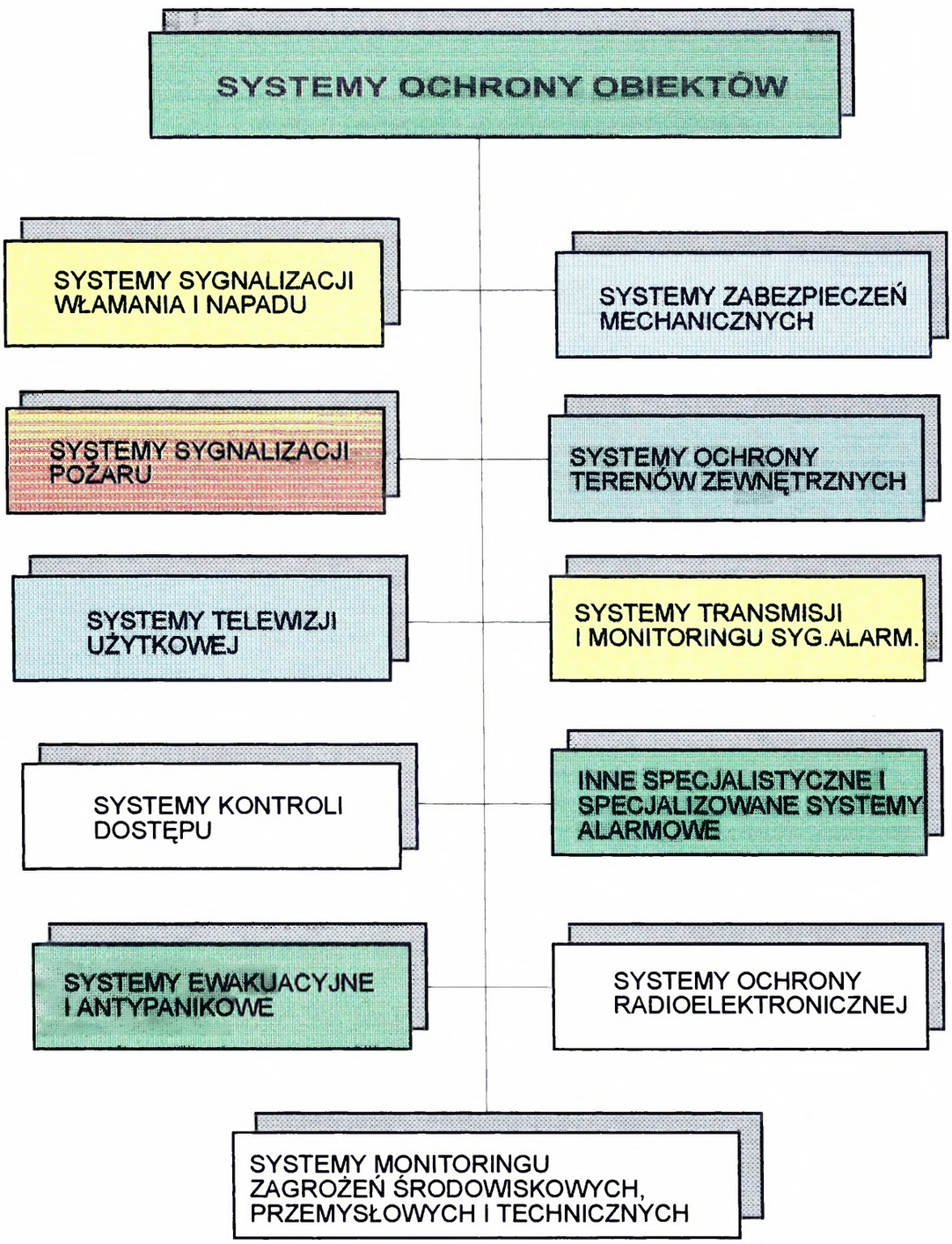
Klasyfikacja systemów sygnalizacji zagrożeń i alarmowania

Systemy ochrony technicznej w zasadzie dzieli są na:

- budowlane systemy ochrony;
- systemy ochrony mechanicznej;
- systemy ochrony elektronicznej. W ostatnim czasie dołączono, w ramach integracji systemów alarmowych, inne systemy sygnalizacji zagrożeń, wynikających z rozwoju cywilizacyjnego, infrastruktury architektoniczno- budowlanej, np. ewakuacyjne i antypanikowe oraz wykrywania gazów trujących;
- techniczne systemy działań prewencyjnych lub wczesnego likwidowania zagrożeń. Chodzi tu przede wszystkim o systemy neutralizujące niebezpieczeństwa za pomocą tzw. automatyki zagrożeń, np. systemy oddymiania i wentylacyjne, gaszenia, blokowania mechanicznego wejść, regulacji parametrów technicznych obiektu (temperatury i oświetlenia, wykrywania CO_2);
- systemy transmisji i monitoringu. Systemy te w sensie organizacyjnym, szczególnie dla firm zajmujących się zawodowo ochroną mienia są wyodrębniane w klasyfikacji, natomiast w sensie technicznym zaliczają się do systemów elektronicznych.

Ostatnie lata wyodrębniły nie tylko technicznie, ale także organizacyjnie systemy przekazujące informacje o stanie bezpieczeństwa obiektu do lokalnych (miejscowych) lub oddalonych punktów dozoru mienia, których zadaniem jest reakcja fizyczna (ludzka) na zagrożenia zasygnalizowane za pomocą środków technicznych.

Wariant klasyfikacji systemów ochrony obiektów przedstawiono na rys. 3.2.2.

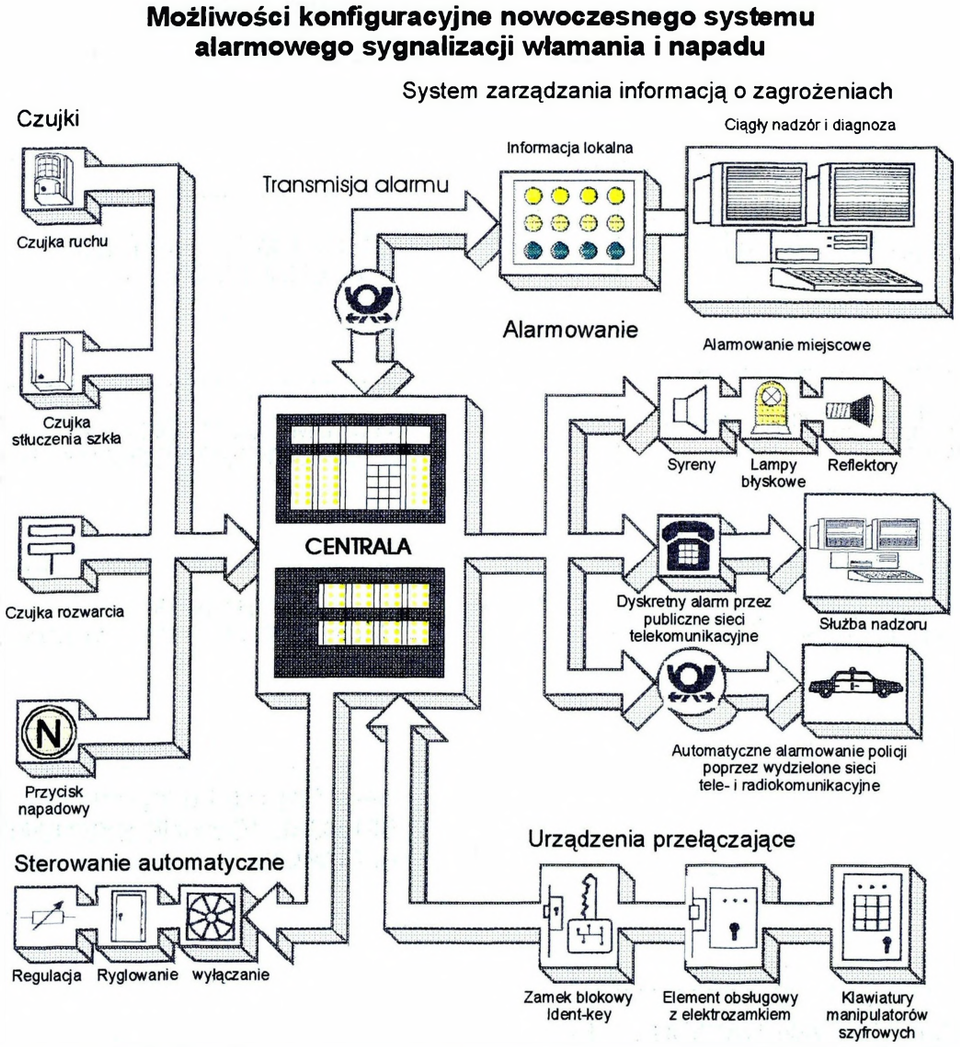


Rys. 3.2.2. Rodzaje systemów ochrony obiektów (wariant)[6]

[6] Opracowanie własne

Systemy alarmowe włamania i napadu

System alarmowy włamania i napadu stanowi podstawowy system zabezpieczenia przed działaniami przestępczymi. Charakterystyka systemu sygnalizacji włamania i napadu oraz elementów wchodzących w jego skład, ogólne wymagania, zasady stosowania są zawarte w arkuszach Polskiej Normy PN-93/E-08390-14[7].



Rys. 3.2.3. Struktura organizacyjna systemu alarmu włamania i napadu

Wymagania wobec nowoczesnego systemu alarmu włamania i napadu wykraczają bardzo często poza wymagania normatywne, szczególnie w opcji sterowań automatyki, transmisji, obsługi, oprogramowania wspomagającego i narzędziowego oraz diagnostycznego.

Elementem decydującym o jakości technicznej systemu sygnalizacji zagrożeń jest centrala alarmowa, której konstrukcja, wyposażenie techniczne i sposób programowania, transmisji danych oraz możliwość rozbudowy i współpracy nie tylko z urządzeniami, ale także

[7] Bliższe informacje zawarto w załącznik nr 3.1.

pracy w sieci zintegrowanej, decydują o nowoczesności i jej możliwościach techniczno - organizacyjnych. Zakres normy obejmuje wymagania i badania central alarmowych (CA) włamania i napadu przeznaczonych do instalowania w budynkach jako element wyposażenia instalacji w nowych budynkach, jak i centrale instalowane później w budynkach już istniejących. Omawiana norma dotyczy CA przeznaczonych do wykrywania i sygnalizowania - alarmowania wtargnięcia osoby nieuprawnionej na obszar objęty ochroną lub sygnalizowania - alarmowania napadu.

Zgodnie z przyjętą normą centrala alarmowa to część systemu alarmowego (SA) jest to urządzenie przyjmujące i przetwarzające żądania włączania, wyłączania działające według określonego algorytmu, umożliwiające wytworzenie stanu alarmowania. Należy jednak pamiętać, że alarm to ostrzeżenie o istnieniu niebezpieczeństwa dla życia, mienia i środowiska. Natomiast system alarmowy jako instalacja elektryczna do wykrywania i sygnalizowania nienormalnych warunków, wskazujących na istnienie niebezpieczeństwa, dozoruje obiekt stanowiący część budynku lub (i) obszaru, w którym system alarmowy może wykryć niebezpieczeństwo. W systemie alarmowym występuje zespół środków technicznych (przesyłowych i końcowych) umożliwiających wymianę informacji, który nazywamy liniami. Linie dozorowe fizycznie podłączone są do centrali alarmowej.

Centrala alarmowa (CA), tak jak cały system alarmowy, posiada ochronę przeciwsabotażową, która jest zespołem środków elektrycznych i mechanicznych zapobiegających celowemu zakłóceniu działania CA i części składowych określonego systemu alarmowego. W tych systemach są wykorzystywane podstawowe typy czujek:

- czujki aktywne podczerwieni - urządzenie wykrywające, przeznaczone do wytwarzania stanu alarmowania, gdy zostanie przerwana wiązka promieniowania między nadajnikiem a odbiornikiem;
- czujki wykrywające ruch (detektory ruchu), które mogą być: ultradźwiękowe lub mikrofalowe Dopplera, pasywnej podczerwieni, czujki zespolone, tj. urządzenia posiadające właściwości dwóch czujek ruchu, np. ultradźwiękowej i pasywnej podczerwieni. Stosowane są przede wszystkim w miejscach, gdzie mogą wystąpić różne zakłócenia w pracy czujki jednego typu;
- czujki wstrząsowe i sejsmiczne, tj.: wibracyjne (inercyjne) urządzenia wywołujące stan alarmowania w odpowiedzi na wykrycie różnego typu drgań lub wibracji materiału, konstrukcji chronionego obiektu; sejsmiczne - stosowane do ochrony specjalnych urządzeń budowlanych typu skarbiec, budynek specjalny lub kasy pancerne;

- czujki stłuczenia szkła to urządzenie wywołujące stan alarmowania w odpowiedzi na wykrycie drgań charakterystycznych pękającego (tłuczonego) szkła za pomocą przetworników piezoelektrycznych;
- czujki magnetyczne i rozwarciowe to mechaniczne i elektromechaniczne urządzenia rozwarciowe lub kontaktronowe, wywołujące stan alarmowania w odpowiedzi na wykrycie przerwania obwodu dozorowego występującego np. przy wyważenie okna, drzwi itd.;
- przyciski i listwy napadowe to urządzenia alarmowe reagujące w sposób natychmiastowy (bez opóźnienia czasowego) w przypadku zagrożenia bezpośredniego, szczególnie napadem lub aktem terrorystycznym;
- czujka nadzoru dokumentów jest to czujka optoelektroniczna nadzorująca dokumenty i banknoty. Znajduje zastosowanie w przypadku zagrożenia kradzieżą banknotów lub dokumentów, np. w kasach lub jako zabezpieczenie miejscowe we wnętrzu kas pancernych;
- czujki specjalne, inne czujki specjalistyczne i urządzenia wywołujące stan alarmowania w odpowiedzi na wykrycie różnych zjawisk fizykochemicznych, np. zmiany ciśnienia w obiekcie, zmiany parametrów pola elektrostatycznego itd.;
- czujki ochrony bram roletowych i zwijanych służą do ochrony ciężkich bram zwijanych. Rozwarcie dwóch części powoduje przerwanie obwodu i wprowadzenie CA w stan alarmowania.

Elementy manipulacyjne są to dodatkowe urządzenia sterujące np. przełącznik, przycisk, klawiatura, urządzenie albo część CA, stosowany do włączania /wyłączania, zmiany stanu, programowania CA albo jego części.

Obrazowanie polega na przedstawieniu informacji o stanie CA lub innego urządzenia systemu alarmowego, najczęściej za pomocą stanu wskaźników optycznych, monitorów, tablic synoptycznych, komunikatów alfanumerycznych, akustycznych, tekstowych, graficznych lub ich kombinacji.

Przed nowoczesnymi systemami alarmowymi (centralami alarmowymi) coraz częściej stawiane jest zadanie współpracy z urządzeniami elektromechanicznymi, których zadaniem jest zwiększenie czasu przełamania aktywnego oporu systemu technicznej ochrony.

Sygnalizacja akustyczna lub (i) optyczna jest realizowana przez sygnalizatory, które są urządzeniami wskazującymi stan alarmowania w dozorowanym obszarze. Sygnalizator jest urządzeniem wytwarzającym dźwiękowy albo dźwiękowo-świetlny sygnał alarmu.

Systemy alarmowe sygnalizacji pożaru

Urządzenia wchodzące w skład systemu powinny posiadać odpowiednie dopuszczenia w zakresie stosowania w ochronie ppoż. na terenie Polski, wydane przez Centrum Naukowo - Badawcze Ochrony Przeciwpożarowej. Należy podkreślić, że omawiane wymagania wobec central, zasilaczy itp. systemów włamania oraz klasyfikacja tych systemów i urządzeń odnosi się także do systemów pożarowych.[8] Rodzaje stosowanych czujek i innego wyposażenia stosowanego w systemach pożarowych:

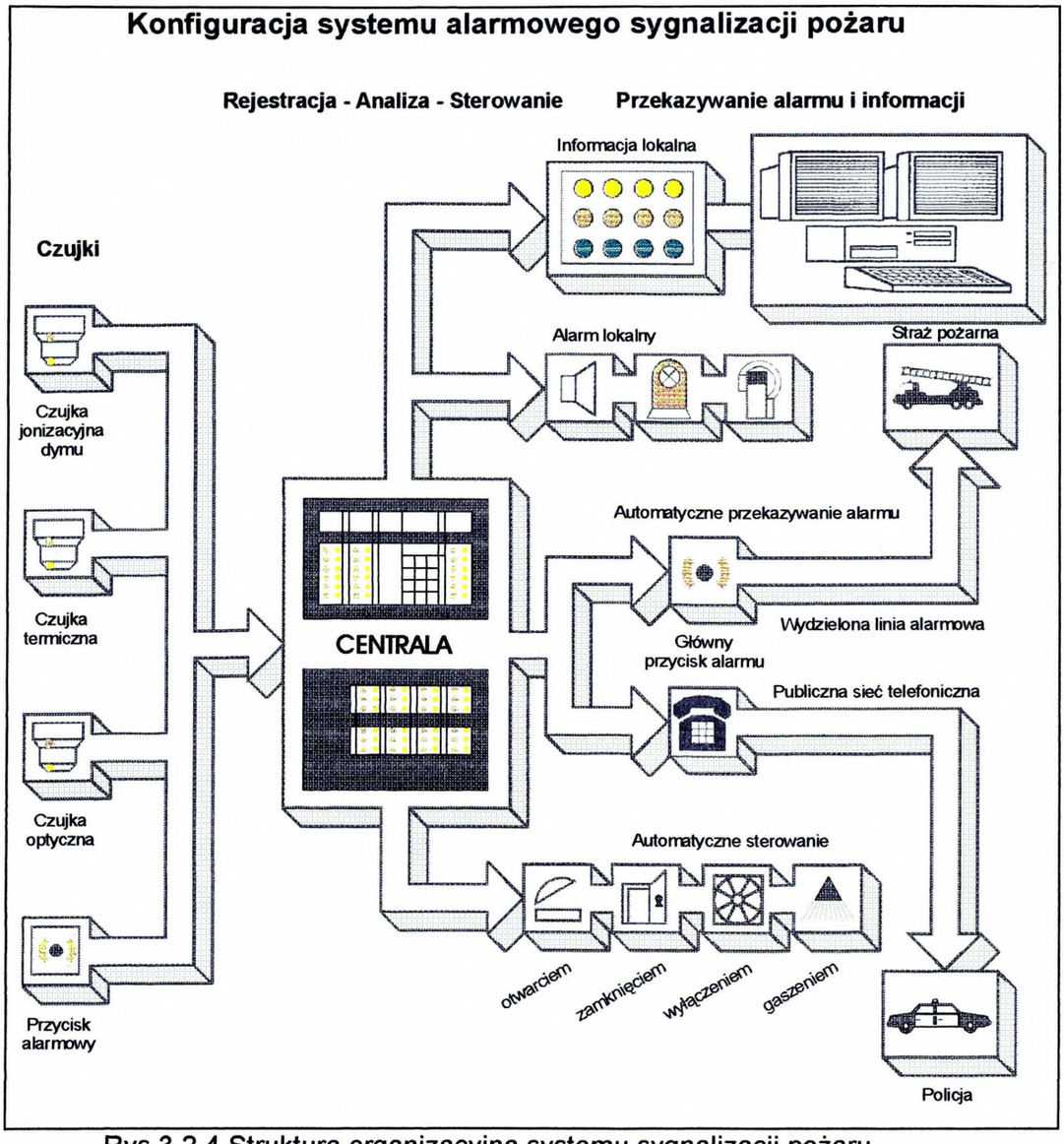
- czujki temperatury - czujki, których zadziałanie następuje w wyniku wzrostu temperatury otoczenia; liniowe czujki temperatury;
- czujki dymu.- czujki dymu reagują na produkty spalania i (lub) rozkładu termicznego, tj.: czujki dymu jonizacyjne; czujki dymu optyczne; czujki z rurkami ssącymi;
- czujki płomieni - czujki płomienia reagują na promieniowanie elektromagnetyczne towarzyszące procesowi spalania płomieniowego;
- czujki iskier;
- czujki manualne (pożarowe przyciski alarmowe) - służą do bezpośredniego uruchomienia instalacji alarmu pożaru przez manualne wywołanie lokalnego optyczno-akustycznego sygnału alarmu i (lub) powiadomienie straży pożarnej;
- gniazdo czujki - urządzenie podłączone bezpośrednio do magistrali przewodowej instalacji pożarowej, które umożliwia mechaniczne zamocowanie czujki pożarowej i jej komunikację z centralą.
- urządzenia dodatkowe systemu alarmu pożaru - najczęściej stosowane urządzenia dodatkowe w systemach pożarowych to: optyczne wskaźniki zadziałania czujki; obudowy kanałowe czujek; moduły adresowe, moduły sterujące, izolatory zwarć.

Systemy pożarowe sterują automatyką zagrożeń np. klapami dymowymi wentylacją i klimatyzacją oraz często są stosowane do wyzwalania systemów ewakuacyjnych.[9]

Rysunek 3.2.4 przedstawia strukturę systemu sygnalizacji pożaru.[10]

---

[8]Informacje techniczne i wymagania zawarte są w załączniku nr 3.2.
[9]Więcej informacji o systemach ewakuacyjnych zawarto w załączniku nr 3.10.
[10]Opracowanie własne - A. Wójcik.



Rys.3.2.4.Struktura organizacyjna systemu sygnalizacji pożaru

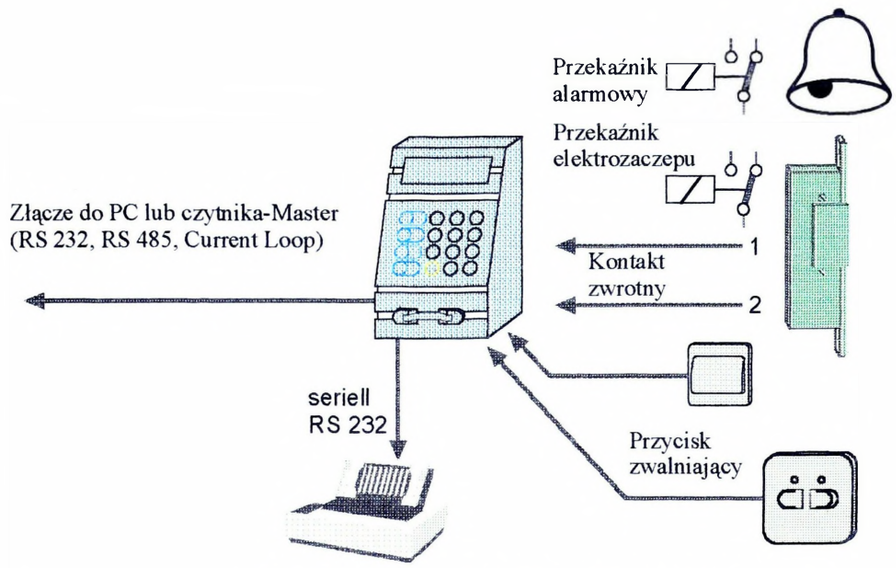
Systemy kontroli dostępu

Systemy kontroli dostępu (access control z ang., Zutrittskontrolle z niem.) skrót SKD, nazywane również systemami kontroli przejść lub sterowania dostępem, ze względu na swoje funkcje ochrony podczas funkcjonowania obiektu, bez konieczności angażowania systemu alarmowego lub innych technik zabezpieczeń elektronicznych, zdobywają coraz większe uznanie wśród użytkowników i ekspertów zabezpieczeń[11]. Przez dostęp w ujęciu bezpieczeństwa rozumie się czynność wejścia do lub wyjścia z obszaru chronionego.

System kontroli dostępu (SKD) jest to system zawierający komplet elementów organizacyjnych i interpretacyjnych oraz komplet elementów wyposażenia technicznego, niezbędnego do sterowania dostępem.

[11]Szczegółowe informacje techniczne zawarte są w załączniku nr 3.3.

Podstawowymi elementami tworzącymi system kontroli dostępu pod względem funkcjonalnym, organizacyjnym i technicznym są: sterownik dostępu; czytnik nośnika identyfikacyjnego; mechaniczne urządzenie blokujące; oprogramowanie systemu.



Rys.3.2.5.Elementy systemu kontroli dostępu

Systemy telewizji użytkowej

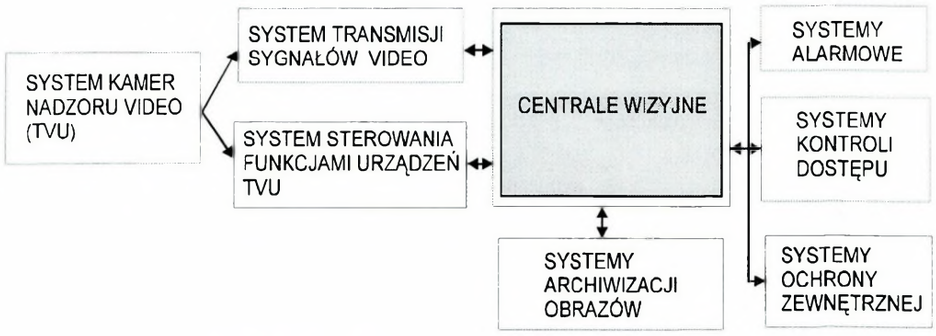
System telewizji użytkowej (TVU) lub system telewizji przemysłowej (TVP) albo system CCTV - z ang. - closed circuit television jest to system złożony z takich elementów, jak: zestaw kamerowy, urządzenia kontrolne oraz urządzenia do przesłania i sterowania, które są niezbędne do optycznego (wizyjnego) dozorowania określonej strefy bezpieczeństwa[12]. Instalacja telewizji dozorowej zawiera sprzętowe i programowe elementy systemu TVU, w pełni zmontowane i działające, a przeznaczone do określonej strefy bezpieczeństwa.

Współczesne systemy obserwacji wizyjnej w sposób zasadniczy różnią się od dawniej stosowanych systemów TVU, które możemy teraz uznać za proste rozwiązania konwencjonalne, w których głównym elementem był zespół kamera-monitor. Zasadnicza różnica polega na wydzieleniu się w nowoczesnym systemie wizyjnym specjalizowanych podsystemów funkcjonalnych systemu obserwacji TVU.

W systemie telewizji użytkowej można wyróżnić: podsystem obserwacji wizyjnej, tj. kamery, obiektywy, obudowy ochronne, uchwyty mocujące, głowice obrotowe, reflektory podczerwieni itd.; podsystem odbioru wizji, tj. monitory, ekrany wizyjne itd.; podsystem transmisji wizji, tj. nadajniki, odbiorniki, wzmacniacze sygnałów wizyjnych, modemy itd.;

[12]Informacje techniczne i wymagania zawarte są w załączniku nr 3.4.

podsystem sterowania, tj. pulpity sterujące funkcjami specjalnymi np. głowicami, ogniskową i przysłoną kamery itd.; podsystem archiwizowania i rejestracji obrazu, np. magnetowidy, wideodrukarki itd.; podsystem przekształcania, rozdzielania, multipleksowania obrazu, tj. przełączniki wizji, multipleksery, centrale wizyjne.



Rys.3.2.6.Główne elementy systemu telewizji użytkowej

Systemy ochrony zewnętrznej

Przez systemy zewnętrzne rozumiane są wszystkie środki techniczno-organizacyjne służące do ochrony obiektów na otwartej przestrzeni, przy czym przestrzeń ta może być ograniczona obwodem wokół strzeżonego obiektu lub w pewnej od niego odległości.[13]

Ochrona zewnętrzna obejmuje przede wszystkim następujące strefy ochrony:

- wysuniętą (zewnętrzną) obwodową, najdalej wysuniętą linię ochrony wynikającą z ograniczeń topograficznych lub architektonicznych;
- peryferyjną, strefę pomiędzy strefą obwodową zewnętrzną a obiektem chronionym;
- obwodową wewnętrzną, obejmująca architektonicznie zewnętrzną część obiektu;
- miejscową, czyli wytypowane obiekty ochrony indywidualnej.

Systemy ochrony zewnętrznej w sposób zdecydowany zwiększają zakres strefowy i czas prewencyjnego działania systemu ochrony technicznej obiektu. Można wyróżnić dwie podstawowe grupy systemów przeznaczonych do wykrywania poruszających się obiektów (człowiek, pojazd, zwierzę):

- systemy aktywne, wielkości fizyczne, które są podstawą działania urządzenia alarmowego, ulegają zmianie w wyniku pojawienia się obiektu niepożądanego w strefie ochrony,

[13] Bliższe informacje zawarte są w załączniku nr 3.5.

- systemy pasywne, które mierzą określone wielkości fizyczne wytwarzane lub wydzielane podczas wkraczania obiektu w strefę ochrony np. poprzez zmiany ciśnienia, pola magnetycznego, wibracji i drgań mechanicznych.

Podstawowe grupy systemów zewnętrznych można podzielić na: systemy elektromagnetyczne; systemy optyczne; systemy oparte o czujniki wibracyjne i siły.

Systemy budowlane, mechaniczne i elektromechaniczne

Ogólnie systemy zabezpieczenia budowlanego możemy podzielić na[14]:

- architektoniczno – budowlane;
- budowlano-mechaniczne;
- mechaniczne;
- elektromechaniczne.

Podstawowymi czynnikami decydującymi o bezpieczeństwie budynku z punktu widzenia architektonicznego - budowlanego jest: obecność miejsc ogólnie dostępnych obok chronionego obiektu, mieszanie budynków mieszkalnych z biurowymi, niewłaściwe zagospodarowanie działki wokół obiektu, niewłaściwe zaplanowanie zieleni, rozwiązania architektoniczne zawierające wnęki, podcienie, gzymsy, długie balkony, gzymsy itd., obecność przylegających do chronionego budynku przybudówek, budynków pomocniczych, zastosowanie nieprawidłowego ogrodzenia w stosunku do poziomu zagrożenia chronionego obiektu, istnienie kilku wejść do chronionego obiektu, istnienie słabych konstrukcyjnie ścian działowych, nieodpowiedni konstrukcyjnie dach i strop, niewłaściwy i jednakowy układ pomieszczeń na piętrach budynku, możliwość niekontrolowanego wejścia na dach dzięki drabinom i schodom ewakuacyjnym umożliwiającym wspinanie się po nich na wyższe kondygnacje.

Typowymi urządzeniami budowlanymi, specjalnie przeznaczonymi do ochrony są: pomieszczenia skarbcowe, śluzy, furty i bramy otwierane i sterowane ręcznie, ogrodzenia i mury, zapory, bariery i blokady drogowe i wjazdowe oraz parkingowe, okna, świetliki, drzwi antywłamaniowe i skarbcowe, inne elementy architektury specjalnej.

Systemy ochrony budowlano-mechaniczne

Na system ochrony budowlano-mechanicznej składa się zarówno architektura obiektu tj. konstrukcja ścian, podłóg, powierzchnie przeszklonych, jak i zaprojektowane i naturalne otwory architektoniczne typu: otwory drzwiowe, okna, włazy, świetliki, tarasy, balkony, a także urządzenia zaporowe, takie jak ogrodzenia, fosy, zapory mechaniczne i blokady przejazdu, bramy, kraty, drzwi, kłódki, zasuwy, zamki mechaniczne, elektrozamki, elektrozaczepy, trzymacze elektromagnetyczne, kołowroty, bariery ruchome, itd. Wymienione urządzenia mają

[14] Bliższe informacje zawarte są w załączniku nr 3.6.

za zadanie nie tylko utrudnić wejście nieupoważnionym osobom, ale przede wszystkim utrudnić lub uniemożliwić wniknięcie potencjalnego intruza do stref chronionych obiektu.

Nie należy zapominać o najstarszej grupie zabezpieczeń mechanicznych takich jak budowle typu: skarbce, kasy pancerne, szafy pancerne i metalowe, skrytki itd., które zawsze współpracują z systemami alarmowymi.

Systemy elektromechaniczne

Pozwoliły rozszerzyć funkcjonalnie system alarmowy na aktywny, stawiający określony opór czasowy działaniom włamaniowym intruza lub (i) podejmujący automatycznie proceduralne działania neutralizujące.

Systemy elektromechaniczne można zasadniczo podzielić na następujące grupy: czujki elektromechaniczne stykowe; elektrozaczepy; zamki elektromechaniczne blokujące; trzymacze elektromagnetyczne; inne blokady elektromechaniczne.

Systemy monitoringu sygnalizacji zagrożeń i alarmowania

W pojęciu omawianych norm system transmisji alarmu stanowią urządzenia i sieć użyte do przekazania informacji o stanie jednego lub więcej systemów alarmowych do jednego lub więcej alarmowych centrów odbioru.[15]

Alarmowym centrum odbioru jest miejsce oddalone od obszaru dozorowanego, miejsce z ciągłą obsługą, do którego przekazywana jest informacja o stanie jednego albo więcej systemów alarmowych, w celu sygnalizacji (alarmowe centrum odbioru) lub do retransmisji (stacja pośrednicząca lub punkt zbiorczy).

Rozpowszechnione są następujące grupy urządzeń monitorujących obiekty (podział ze względu na rodzaj drogi wykorzystanej do przesyłania informacji):

- monitoring dialerowy - wykorzystujący komutowaną sieć telefoniczną;
- monitoring z wykorzystaniem tzw. „łączy sztywnych”;
- monitoring radiowy;
- monitoring wielotorowy.

Systemy mieszane monitoringu, np.: system telefoniczny komutowany i radiowy stosowane są do poprawy parametrów systemu ogólnego.

Zintegrowane systemy sygnalizacji zagrożeń i alarmowania oraz automatycznego nadzorowania obiektu

Od początku lat osiemdziesiątych obserwowany jest dynamiczny rozwój techniczny wspomagania decyzji i zarządzania systemami bezpieczeństwa i automatyki obiektu.

---

[15] Bliższe informacje zawarte są w załączniku nr 3.7.

Zasadniczo można te systemy podzielić na dwie, mogące niezależnie od siebie pracować i (lub) współpracować, grupy:

- zintegrowane systemy alarmowania i sygnalizacji zagrożeń[16],
- zintegrowane systemy zarządzania automatyką budynków.

Wymienione wyżej systemy są syntezą naszych dotychczasowych rozważań dotyczących wymagań, funkcji i budowy systemów alarmowania i sygnalizacji zagrożeń.

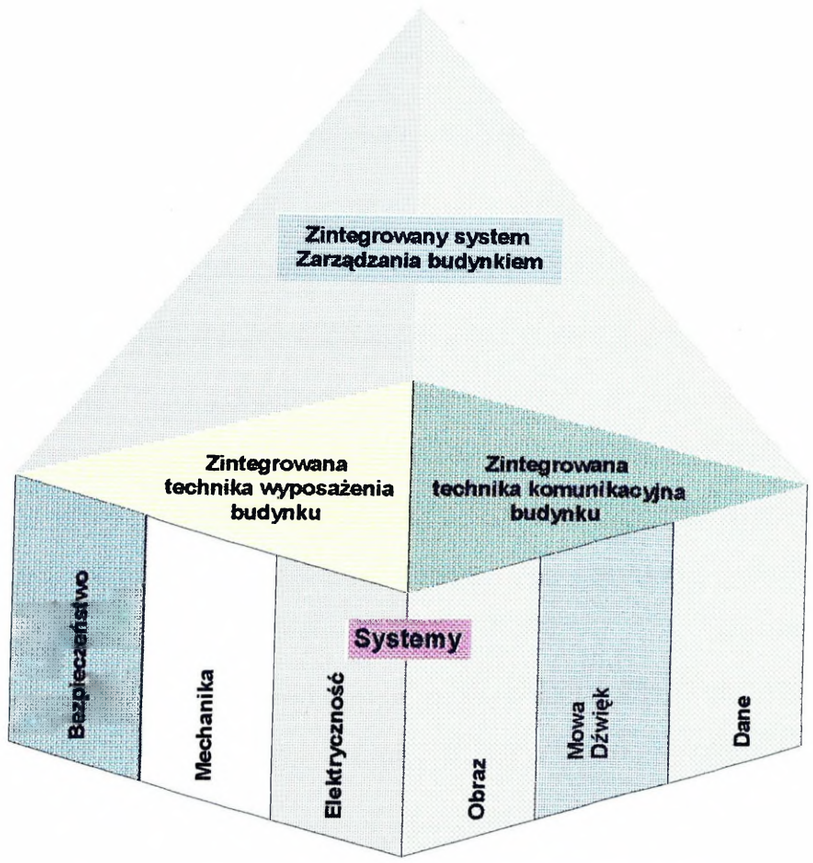
Zastosowana w rozwiązaniach tych systemów technologia oraz organizacja sprowadza je do poziomu doradczego w formie "sztucznej inteligencji". Systemy te są podstawą do modelowania systemów alarmowania i sygnalizacji zagrożeń na potrzeby obronne państwa.

Integracja systemów alarmowych umożliwia:

- prawidłową kontrolę nad pracą autonomicznych systemów, często różnych producentów;
- elastyczne określenie zakresu skali integracji;
- podział i efektywny nadzór nad strefami bezpieczeństwa;
- podniesienie efektywności i poziomu bezpieczeństwa ludzi i mienia chronionego;
- obniżenie kosztów eksploatacji systemów;
- skrócenie czasu efektywnej interwencji neutralizującej skutki działań przestępczych i środowiskowych.

W latach osiemdziesiątych, w wyniku szybkiego postępu technologicznego w dziedzinie techniki mikroprocesorowej, zaczęły się pojawiać nowe zastosowania elektroniki, informatyki i telekomunikacji, szczególnie w automatyce i sterowaniu systemami w budynkach. Powstało określenie „inteligentny budynek". „Inteligentny budynek" jako system posiada określoną strukturę organizacyjno-techniczną, której zadaniem jest maksymalizacja wydajności procesu eksploatacji budynku i efektywne zarządzanie jego zasobami. Rysunek 3.2.7. przedstawia zintegrowane zarządzanie obiektem poprzez zintegrowaną technikę wyposażenia i komunikacji.[17]Użytkowane systemy umożliwiają wykrywanie zakłóceń, diagnozują błędy i uszkodzenia, planują i kontrolują przeglądy i konserwację urządzeń oraz informują o niebezpieczeństwie wymuszając automatycznie określone procedury interwencyjne.

[16] Bliższe informacje zawarte są w załączniku nr 3.8, 3,9.
[17] W. Harke, P. Waneck, *Gebäude Management Systeme.*



Rys.3.2.7.Prezentacja modelu upraszczającego zarządzanie i procesy automatyzacji obiektu

3.2.1.Ocena stanu krajowych rozwiązań ochrony obiektów wojskowych

System alarmowy (SA) można podzielić na następujące części[18]:

1) centrala (urządzenie sterujące) - 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 wytwarza 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;

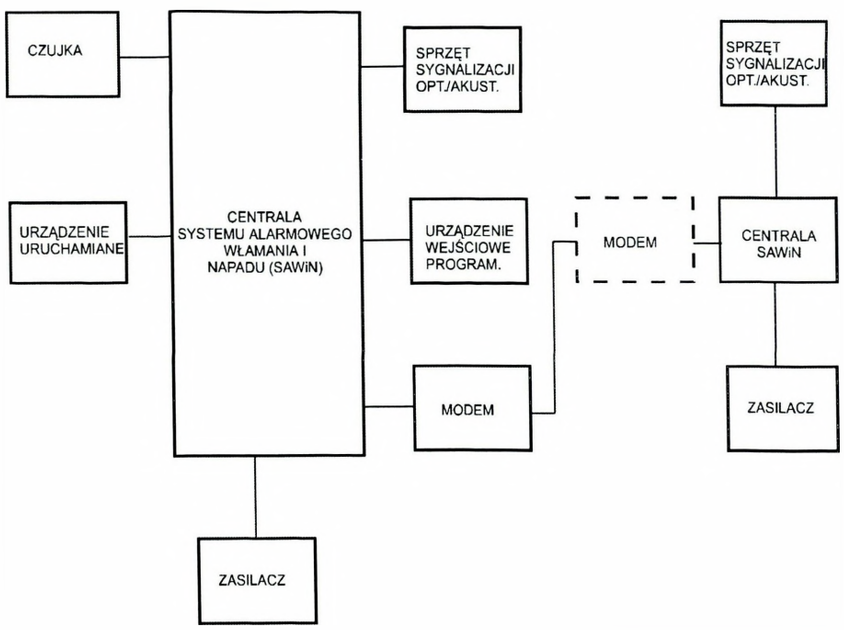
4) sprzęt sygnalizacji optycznej i (lub) akustycznej - urządzenia, których zadaniem jest poprzez sygnały optyczne i (lub) akustyczne poinformować służby ochrony lub innych użytkowników o grożącym niebezpieczeństwie;

[18] Polska Norma PN-93/E-08390-14, *Systemy alarmowe*.1993.

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 przekazywanie sygnałów z centrali do alarmowego centrum odbiorczego (oddalonego) poprzez wykorzystanie różnych systemów transmisji. Części składowe systemu alarmowego włamania i napadu (SAWiN) przedstawiono na rysunku 3.2.1.1.



Rys.3.2.1.1.CZĘŚCI SKŁADOWE SYSTEMU SAWiN

Wytyczne stosowania norm zabezpieczenia w techniczne urządzenia sygnalizacyjne i alarmowe instalowane w ochronie obiektów wojskowych zalecane przez Sztab Generalny (Zarząd Obrony Terytorialnej) został opracowany projekt dokumentu, który stanowi podstawę do planowania inwestycji, budowy systemów ochrony, modernizacji istniejących systemów oraz określający ilość i rodzaj urządzeń instalowanych w poszczególnych strefach chronionego obiektu wojskowego[19].

W dokumencie określono strefy ochrony jako:

- peryferyjne (na zewnątrz obiektu poza jego ogrodzeniem);
- zewnętrzne (obwodowa i bezpośrednie);

[19] *Tymczasowe normy zabezpieczenia w techniczne urządzenia sygnalizacyjne i alarmowe terenów, obiektów i mienia wojskowego*, SG WP, Zarząd Obrony Terytorialnej, Warszawa 1999.

- wewnętrzne (przestrzeń wewnątrz budynków).

W dalszej części opracowania zdefiniowane są techniczne urządzenia sygnalizacyjne (TUS) stosowane do ochrony obiektów wojskowych oraz urządzenia alarmowe (UA). Określone są podstawowe warunki, jakie muszą spełniać TUS i UA, tzn. optymalne wykorzystanie, nieutrudnienie pracy personelu w obiekcie, uwzględnienie już istniejących innych systemów sygnalizacji zagrożeń oraz uzupełnianie innych środków zabezpieczających.

Wymienione wymagania dotyczą parametrów funkcjonalnych systemów ochrony oraz poszczególnych urządzeń, takich jak np. czujki, kamery, szyfratory, itd. Przedstawiono wymagania techniczno-użytkowe stawiane systemom ochrony technicznej w zależności od rodzaju chronionego mienia, dzieląc je na: magazyny broni, amunicji, granatów, materiałów wybuchowych, pomieszczenia kancelarii tajnych, mobilizacyjnych, kas oraz miejsc przechowywania narkotyków i innych środków toksycznych; magazyny sprzętu bojowego; pozostałe magazyny.

Wszystkie urządzenia i instalacje wchodzące w skład systemów alarmowych muszą spełniać odpowiednie normy w zakresie przepisów ppoż., w tym także przeciwwybuchowości, iskrobezpieczności oraz w zakresie kwalifikacji do odpowiedniej klasy systemów i urządzeń alarmowych.[20]

W normie (projekcie) ujęto wymagania co do zabezpieczenia poszczególnych stref, podkreślając, że strefa peryferyjna jest zabezpieczana w czasie „W", przestawiono także sposób montażu czujników i informacje o dopuszczalnej długości sektora lub strefy zabezpieczanej przez poszczególne urządzenia. Jednocześnie podane są ilości czujek stosowanych do ochrony pomieszczeń w zależności od ważności (kategorii zagrożenia), kształtu i wielkości powierzchni. Podano także zasadę kolejności ochrony stref obiektu, a mianowicie priorytet posiada strefa ochrony wewnętrznej, następnie rozszerzenie ochrony obiektu obejmuje strefę zewnętrzną – bezpośrednią i obwodową.

Jeżeli tak to mawiany dokument, mimo że nie spełnienia wszystkich wymagań Dyrektywy Bezpieczeństwa ACE z ang. Allied Command Europe (Zjednoczone Dowództwo Europejskie) i innych norm oraz zasad ochrony obiektów, to jednak stanowi duży krok w ujednoliceniu wymagań wobec systemów ochrony obiektów wojskowych na potrzeby obronności państwa.

Istniejące krajowe rozwiązania systemów ochrony obiektów wojskowych w ostatnich latach w zdecydowany sposób zostały ukierunkowane na nowoczesne kompleksowe organizacyjno-techniczne systemy sygnalizacji zagrożeń i alarmowania. Osiągnięto to dzięki

[20] Polska Norma PN-83/E-08110, PN-84/E-08107 i PN-93/E-08390.

napływowi nowoczesnej technologii oraz zwiększeniu nakładów przeznaczanych na ten cel przez resort obrony. Jednak nadal istnieje problem optymalnego wyboru najlepszych rozwiązań technicznych dla ochrony konkretnych obiektów wojskowych, adekwatnych do kategorii zagrożenia.

Brak doświadczenia, znormalizowanych i sprawdzonych wytycznych i procedur, dostatecznej wiedzy w zakresie ochrony organizacyjno-technicznej oraz bariery finansowe mogą być przyczyną nieprawidłowych rozwiązań ochrony obiektów wojskowych.

3.2.2. Rozwiązania w zakresie ochrony obiektów wojskowych stosowane w niektórych państwach NATO

Systemy chroniące obiekty wojskowe państw NATO wyróżnia szczególnie silnie położony nacisk na ochronę zewnętrzną i peryferyjną obiektu wraz z jego wyposażeniem oraz zgromadzonym sprzętem wojskowym. Zdecydowanie w tym zakresie przewodzą rozwiązania amerykańskie, ale także nie ustępują im niemieckie i angielskie, czy też izraelskie.

Należy podkreślić, że wobec systemów ochrony zewnętrznej stawiane są najwyższe wymagania techniczno-użytkowe w zakresie wykrywania zagrożeń (szczególnie w aspekcie zagrożeń ze strony aktów terrorystycznych), prób wtargnięcia intruza w strefę chronioną - przy jednoczesnej eliminacji fałszywych alarmów. Wymienione systemy są kosztowne w instalowaniu i w późniejszej eksploatacji. Dlatego ochrona zewnętrzna obiektów wojskowych według standardów NATO wymaga wysokich nakładów inwestycyjnych.

Wszystkie stosowane i spotykane rozwiązania są omówione w dalszej części pracy. Ze względu na aspekt techniczny przestawiono jedynie przykładowe aplikacje systemów ochrony zewnętrznej stosowane do ochrony obiektów wojskowych.

Rysunek 3.2.2.1. prezentuje system alarmowy tworzący barierę fizyczną i elektroniczną w postaci ogrodzenia wokół chronionej strefy (obiektu)[21]. W razie forsowania ogrodzenia, na drutach czujnikowych generują się impulsy elektryczne, które przekazywane są do centrali alarmowej, która umożliwia wizualizację stanu ochrony obiektu za pomocą tablicy synoptycznej lub kamery telewizji przemysłowej. W systemie może być wykorzystany dowolny drut stalowy z powłoką antykorozyjną.

Ogrodzeniowy system wibracyjny z układem wykrywania ruchu i śledzenia przedstawia rysunek 3.2.2.2. Aplikacja może być stosowana w większości rodzajów płotów i ogrodzeń metalowych.

---

[21] Systemy: DTR-2000, Barricade 500 firmy MAGAL Security Systems Ltd, Izrael.

Często stosowanym rozwiązaniem w określonych sytuacjach ochrony obiektu lub sprzętu wojskowego, np. samolotu, są bariery mikrofalowe przedstawione na rysunku 3.2.2.3 i 3.2.2.4.[22] Wejście intruza w pole dozoru bariery wywołuje alarm. Bariery mikrofalowe stanowią skuteczny system ochrony małych obiektów i niewielkich stref ochrony do 100-150 m długości.

Na rysunkach 3.2.2.5. i 3.2.2.6. przedstawiona jest aplikacja systemu ochrony zewnętrznej ogrodzeniowego akustycznego (np. czujki FS-2-2 na siatce).

Systemy ochrony obiektów wojskowych NATO charakteryzują się połączeniem elementów fizycznej zapory (np. ogrodzenia zakończone drutami kolczastymi, skośne wysięgniki uniemożliwiające wejście itd.) z bardzo wczesnym elektronicznym rozpoznawaniem zagrożenia. Rozwiązania w tym zakresie zaprezentowano na rysunkach 3.2.2.7 i 3.2.2.8.

Rysunek 3.2.2.9. prezentuje jeden ze sposobów ochrony przedmiotów, sprzętu, kas i wyposażenia wojskowego za pomocą systemu alarmowego reagującego na zbliżenie (np. próba wejścia w strefę, sięgnięcia, otworzenia, uruchomienia, itd.).

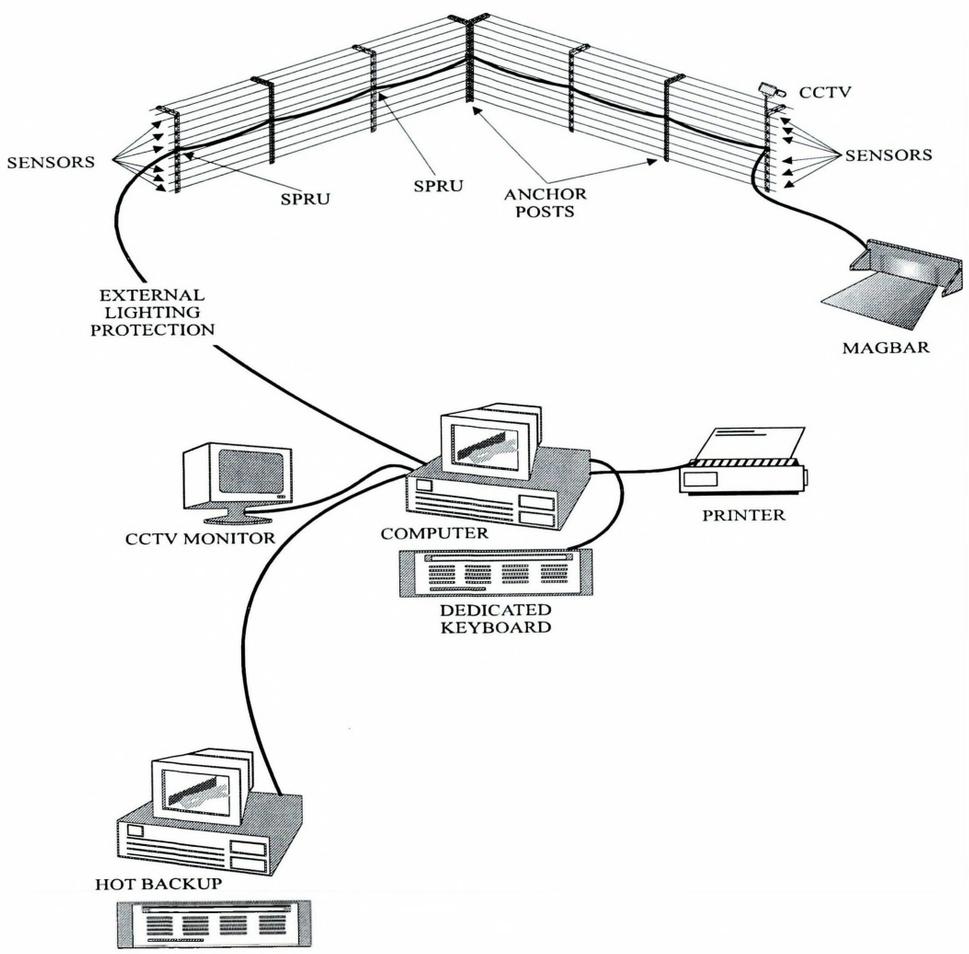
Powszechnie są stosowane zaawansowane systemy wykrywania ruchu i śledzenia intruza, zbudowane w oparciu o cyfrową analizę przetwarzania obrazów uzyskanych z kamer nadzoru wizyjnego przedstawia rysunek 3.2.2.10. W omawianym przypadku największe problemy, ze względu na zakłócenia środowiskowe i przemysłowe, sprawiają aplikacje ochrony zaprojektowane specjalnie do zastosowań zewnętrznych.

W systemach wizyjnych z detekcją ruchu każda próba nieupoważnionego wejścia w kontrolowany przez kamerę obszar jest prezentowana na monitorze wraz z graficznym śledzeniem intruza lub kilku intruzów jednocześnie.

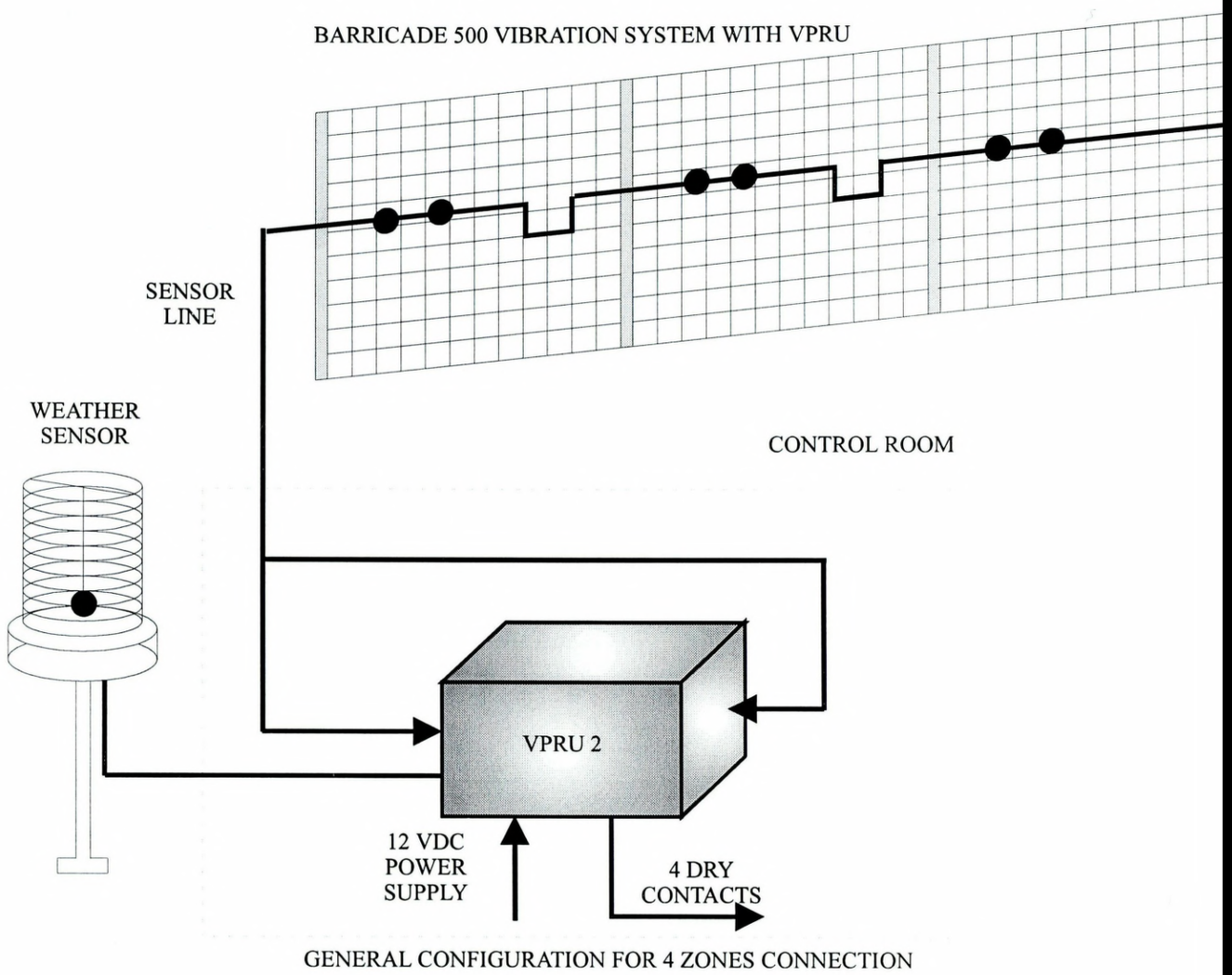
Poniżej przedstawione zostały omawiane aplikacje systemów ochrony obiektów wojskowych stosowane w wybranych państwach zachodnich.

---

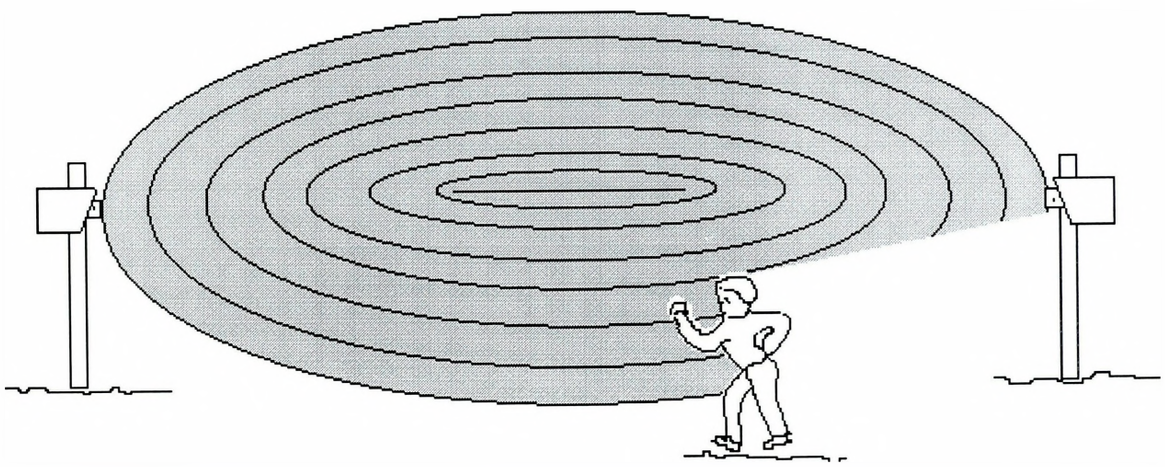
[22]Systemy: MPS-4100, Comgard MX-1000 firmy PERIMETER PRODUCTS, INC., USA.



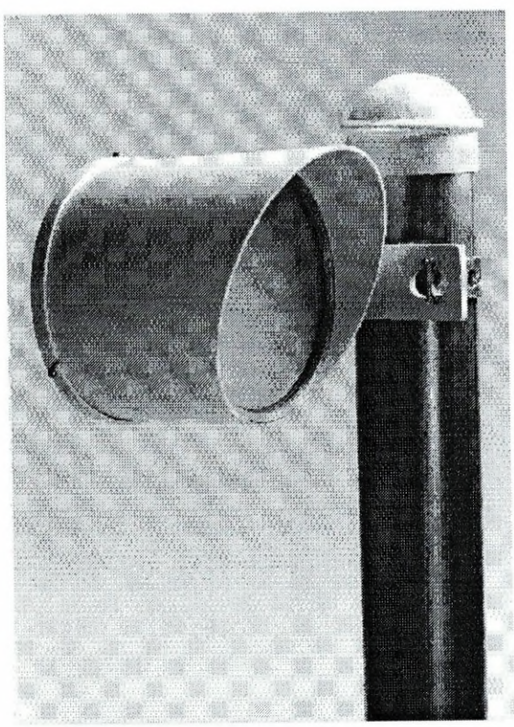
Rys. 3.2.2.1. System ochrony zewnętrznej ogrodzeniowy – elektromechaniczny naciągowy



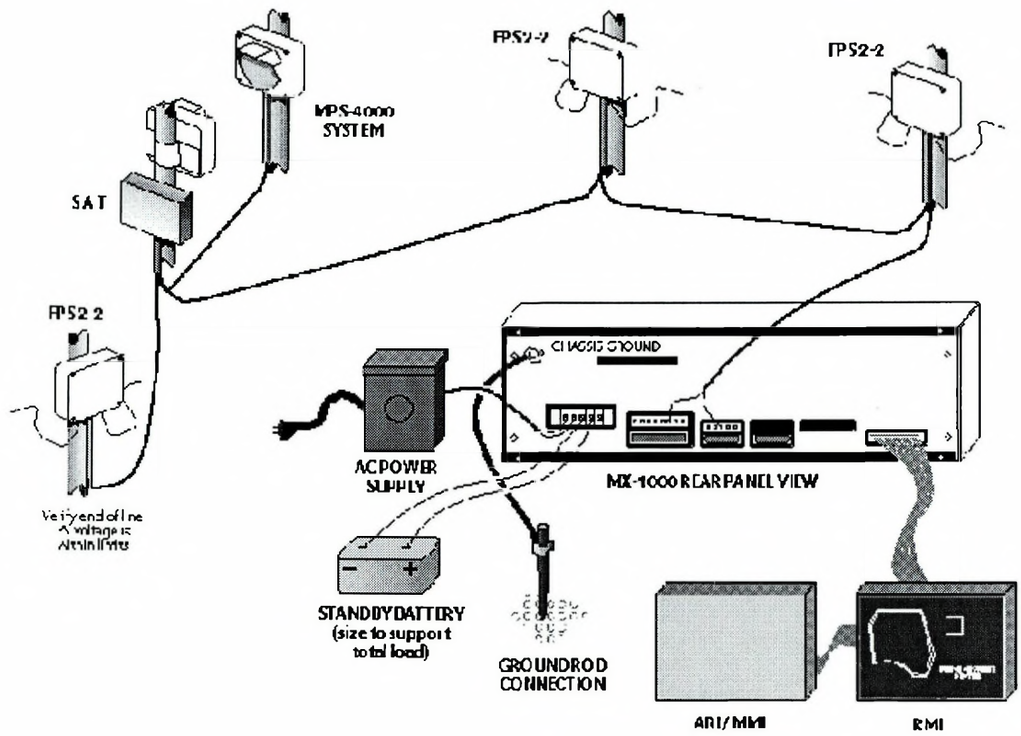
Rys. 3.2.2.2. System ochrony zewnętrznej ogrodzeniowy - wstrząsowy



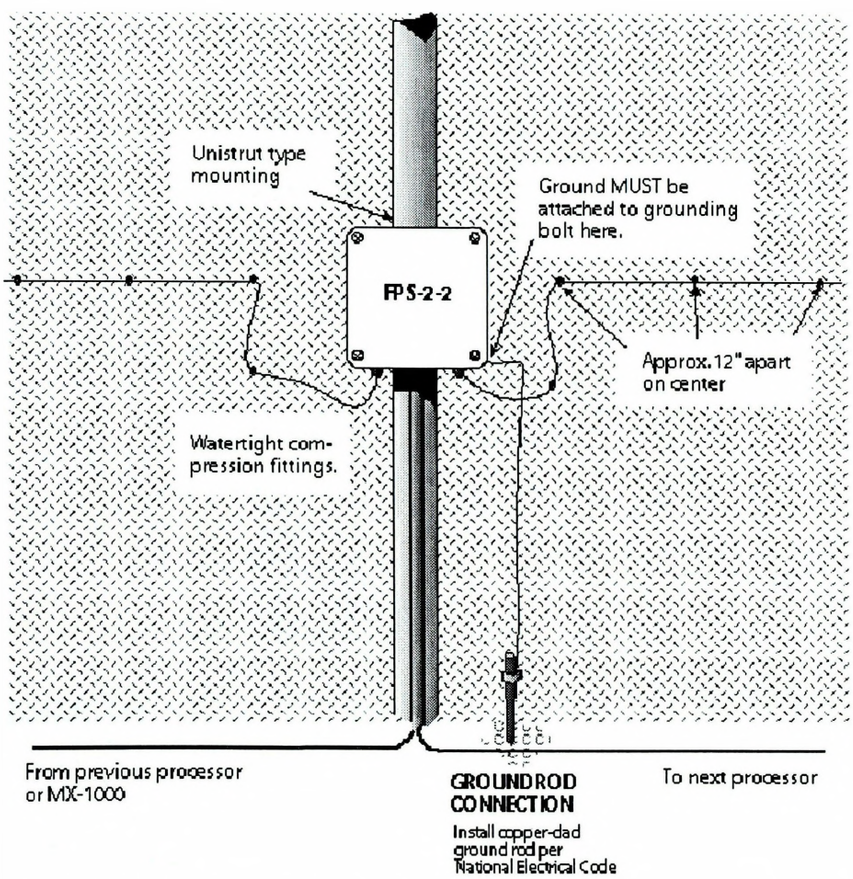
Rys. 3.2.2.3. Zasada działania bariery mikrofalowej



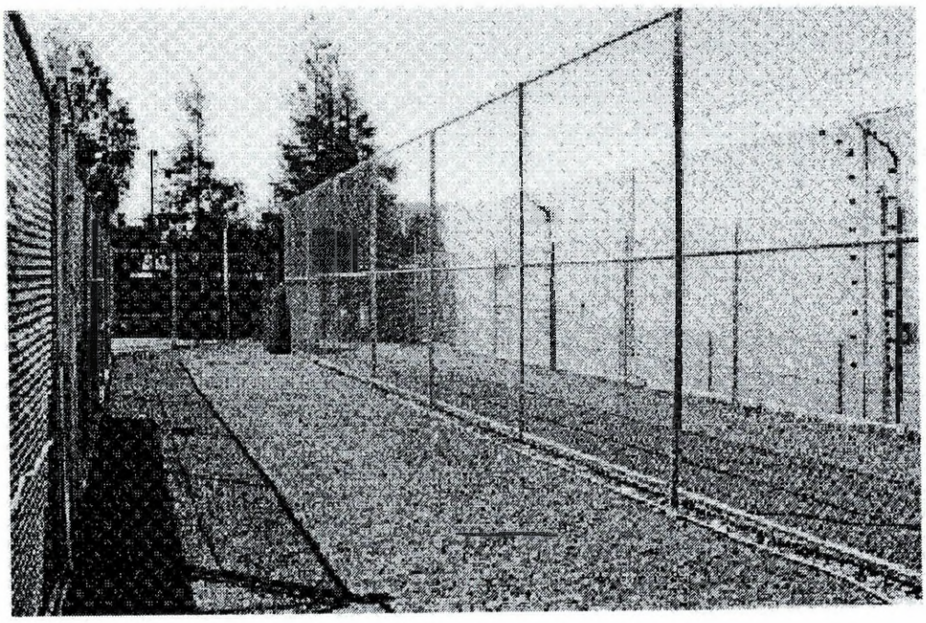
Rys. 3.2.2.4. Nadajnik mikrofalowy systemu ochrony zewnętrznej obwodowej



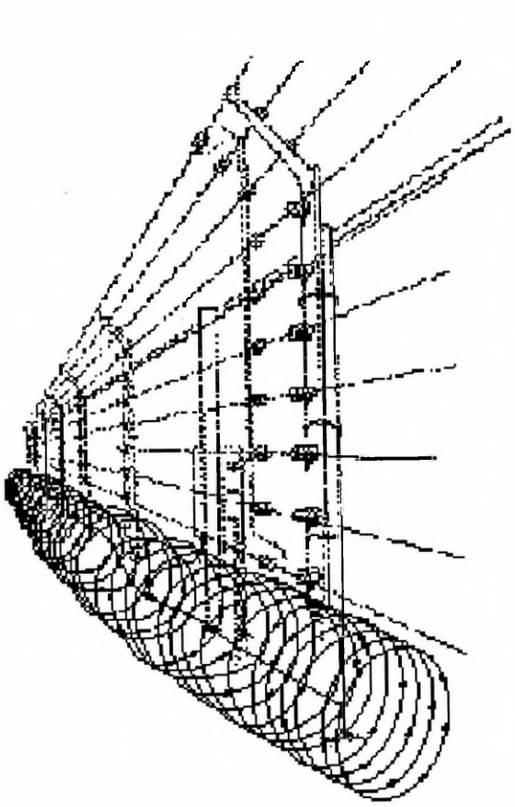
Rys. 3.2.2.5. Kompletny system ochrony ogrodzenia reagujący na zbliżenie intruza



Rys. 3.2.2.6. Montaż czujnika akustycznego na metalowej siatce

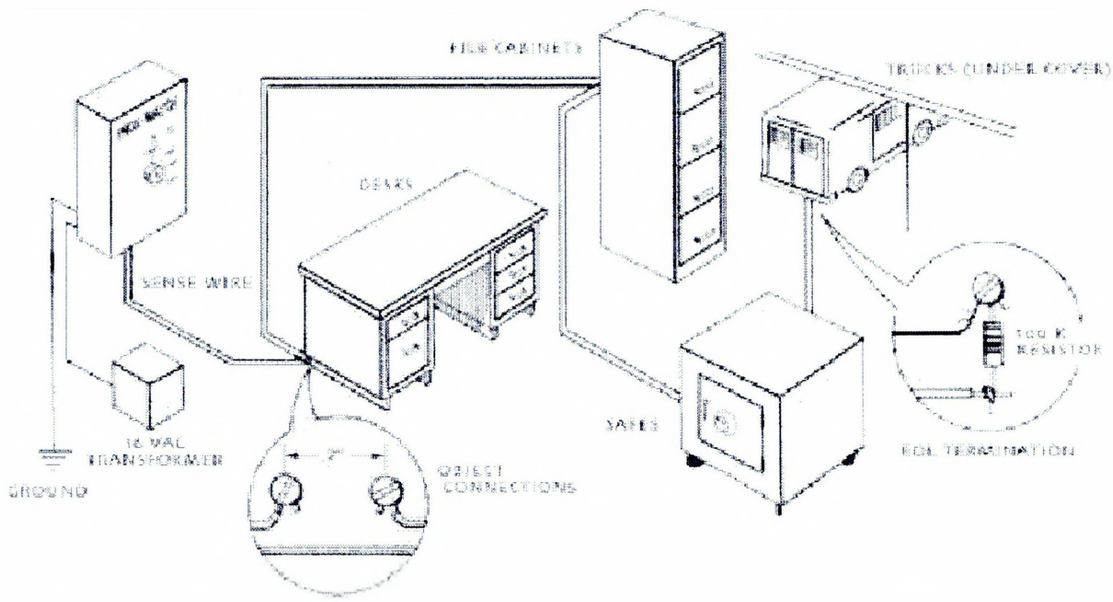


Rys. 3.2.2.7. Potrójna strefa ochrony zewnętrznej oddzielona ogrodzeniami z nadzorem systemu alarmowego

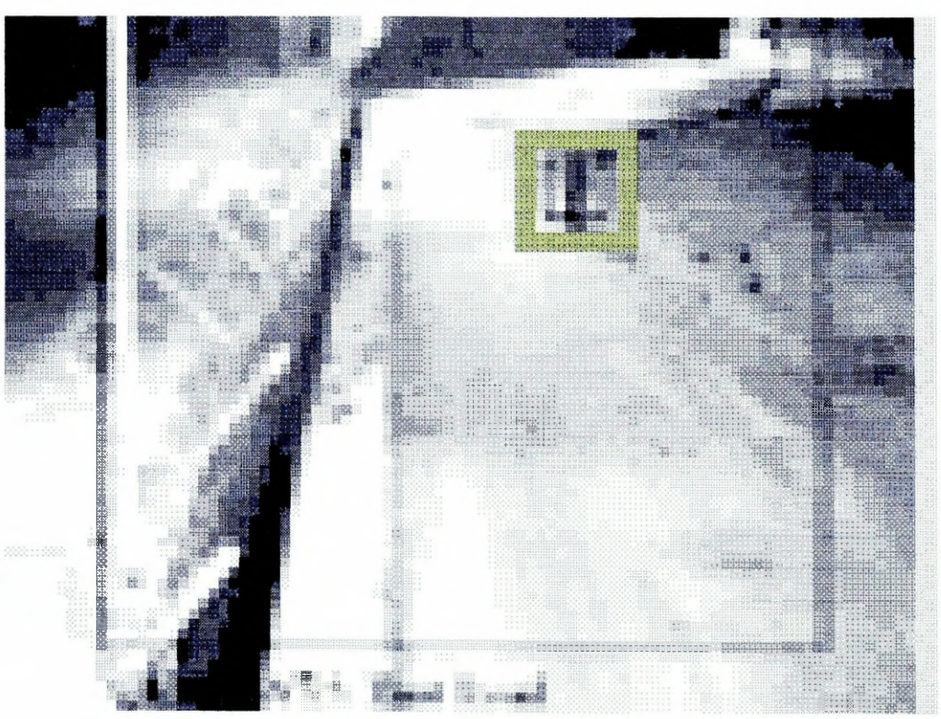




Rys. 3.2.2.8. Ochrona strefy zewnętrznej za pomocą systemu ogrodzeniowego i specjalnych drutów kolczastych uniemożliwiających podejście do ogrodzenia



Rys. 3.2.2.9. Plan instalacyjny systemu zbliżeniowgo (elektromagnetycznego)ochrony kas, sprzętu, wyposażenia biura, pojazdów, itp.



Rys. 3.2.2.10. System wizyjny wykorzystujący analizę ruchu (obraz „nocny" na monitorze)

3.3. Wymagania stawiane systemom ochrony obiektów wojskowych w kontekście członkostwa Polski w NATO

Najważniejsze zasady funkcjonowania NATO stanowią konstrukcję organizacyjną sojuszu i podstaw procedur jego działania i obejmują[23]:

- całkowitą suwerenność państw członkowskich;
- consensus w podejmowaniu decyzji politycznych;
- oddzielenie struktury politycznej od zintegrowanej struktury dowodzenia.

Zasada całkowitej suwerenności państw członkowskich jest realizowana w sferze organizacyjnej i decyzyjnej. W Traktacie Waszyngtońskim podkreślona jest rola równości stron państw członkowskich. Jedynym najwyższym organem decyzyjnym NATO, upoważnionym do podejmowania decyzji w imieniu Sojuszu jest Rada Północnoatlantycka (NAC - z ang. - North Atlantic Council) lub odpowiednie komitety złożone z reprezentantów państw członkowskich, które są upoważnione do podejmowania decyzji dotyczących wspólnego potencjału militarnego, poziomu wydatków wojskowych, programów inwestycyjnych Sojuszu. Przy czym NAC nie ma prawa do wymuszenia na państwie członkowskim obowiązku ścisłego przestrzegania wspólnych decyzji.

Państwa członkowskie samodzielnie decydują o liczebności i składzie wydzielonych kontyngentów do zintegrowanej struktury obronnej. Ostateczne decyzje konsultowane są na forum Komitetu Planowania Obronnego (DPC – z ang. - Defence Planning Committee) i Komitetu Wojskowego, jednakże żaden organ Sojuszu nie może zmusić państwa członkowskiego do wysłania wojsk w rejon konfliktu.

Podstawą zasady consensusu jest pełna jednomyślność wszystkich decyzji podejmowanych przez NAC, DPC, NPG (NPG – z ang. - Nuclear Planning Group), Komitet Wojskowy (MC - z ang. - Military Committe) inne organa kolektywne Paktu. Głos sprzeciwu ze strony jednego z państw może zablokować każdą decyzję NATO.

Zasada rozdziału struktury politycznej NATO od zintegrowanej struktury dowodzenia została przeniesiona z tradycji państw anglosaskich, gdzie sprawnie funkcjonują mechanizmy cywilnej i demokratycznej kontroli nad wojskiem. Ta zasada sprowadza się do systemowego oddzielenia struktur odpowiedzialnych za przygotowanie i podejmowanie decyzji politycznych i wojskowych od organów odpowiedzialnych za ich wykonanie.

Pion polityczny NATO stanowi NAC wspierany przez komitety NATO i Komitet Wojskowy (wraz z IMS - z ang.- International Military Staff) jako podstawowy organ doradczy w sprawach militarnych. Na bazie analiz i programów NAC podejmuje decyzje w sprawach

---

[23]B. Balcerowicz, *Wybrane problemy obronności Państwa*, AON, Warszawa 1997.

funkcjonowania NATO. Za wykonanie tych decyzji odpowiada zintegrowana struktura militarna.

Planowanie obronne w NATO

Ramy planowania obronnego NATO są tworzone jako zasady będące dokumentem zbiorowego bezpieczeństwa.[24]. Kraje członkowskie posiadają suwerenność w procesie planowania obronnego. Posługują się przy tym procedurami służącymi do:

- określenia sił potrzebnych do realizacji polityki sojuszu;
- koordynowania narodowych planów obronnych;
- ustalania celów planowania i działania sił zbrojnych sojuszu jako całości.

Obowiązuje doroczna wymiana informacji pomiędzy międzynarodowymi cywilnymi i wojskowymi sztabami, władzami NATO i rządami państw członkowskich NATO. Ta wymiana umożliwia porównanie własnych intencji narodowych z ogólnymi potrzebami NATO oraz ewentualne ich ponowną analizę w aspekcie politycznych wytycznych, weryfikacji potrzeb, zmiany ról i zadań w zakresie odpowiedzialności i sił zbrojnych.

Analiza wymienionych zagadnień odbywa się ciągle, a jej wyniki są uwzględniane w każdym etapie cyklu planowania obronnego. Uzgodniona koncepcja planowania obronnego jest początkiem procesu planowania obronnego. Koncepcja określa w ogólnym zarysie cele sojuszu oraz środki do ich osiągnięcia. Ministrowie obrony opracowują co dwa lata szczegółowe wytyczne.

Specyficzne planistyczne cele i zadania dla sił zbrojnych państw członkowskich są opracowywane na bazie tych wytycznych. Okres planowania obejmuje sześć lat, a w niektórych wypadkach - dłuższy okres.

Plany są uaktualniane co dwa lata. Dodatkowo ministrowie obrony dokonują corocznych przeglądów planowania obronnego i wydają wytyczne, w których uwzględniane są oceny wkładu krajów członkowskich do wspólnej obrony w odniesieniu do ich możliwości i problemów. Wynikiem corocznych przeglądów planów obronnych jest Plan Sił NATO, który stanowi podstawę planowania w NATO na kolejne 5 lat.

Planowanie obronne odbywa się według ustalonej procedury planowania. Głównym organem koordynującym jest Komitet Planowania Obronnego, który zbiera propozycje, uzgadnia je z branżowymi komitetami i konferencjami oraz przedstawicielstwami narodowymi.

Proces planowania obejmuje następujące fazy:

- Wytyczne ministerialne – efekt politycznego, technologicznego i militarnego ukierunkowania planowania przez Komitet Planowania Obronnego, zatwierdzany podczas wiosennej sesji ministrów.

---

[24]M. Bednarz, Z. Robekowski, *Rozwój systemu obronnego (Prognozowanie i planowanie obronne)*, AON, Warszawa 1998.

- Określenie zadań sił zbrojnych – dla wszystkich szczebli dowodzenia i krajów, na każdy rok, z określeniem udziału każdego państwa. Głównymi zamierzeniami są inwestycje, zmiany organizacyjne, dyslokacja sił, poziom zdolności i gotowości bojowej. Komitet wojskowy uzgadnia propozycje zadań z każdym krajem członkowskim. W razie braku zgodności stron zagadnienia sporne przekazywane są do rozpatrzenia w wyższych organach (komitetach). Wszystkie plany są uzgadniane z określonymi instytucjami i sztabami międzynarodowymi. Następnie plany przekazywane są Komitetowi Obronno- Weryfikującemu, który ocenia plany pod kątem celów polityczno- militarnych oraz sporządza raport i przekazuje go do Komitetu Planowania Obronnego. Plany są zatwierdzane przez sesję ministerialną i przekazywane krajom członkowskim do realizacji. Po tym fakcie każdy kraj planuje nakłady finansowe na realizację zamierzeń na okres pięcioletni.
- Coroczny przegląd (ocena obrony) – realizacja planów jest sprawdzana i nadzorowana przez specjalistów wojskowych NATO i Sztab Międzynarodowy. Ustala się, czy stan sił zbrojnych kraju odpowiada postawionym do realizacji celom. Wyniki przeglądu zestawiane są w karcie kraju i wyjaśniane w raporcie.

Dyrektywa bezpieczeństwa ACE

Jednym ze szczegółowych dokumentów dotyczących wymagań stawianych ochronie obiektów wojskowych oraz obiegu informacji i utrzymania tajemnicy państw członkowskich NATO jest Dyrektywa Bezpieczeństwa ACE (ACE – z ang. - Allied Command Europe)[25]. Dyrektywa Bezpieczeństwa ACE ustanawia podstawowe zasady i minimalne wymagania bezpieczeństwa, które są stosowane na obszarze Zjednoczonych Sił Europejskich (ACE). Zasady i wymagania zostały uzgodnione przez kraje członkowskie tak, aby każdy kraj członkowski sojuszu obowiązywały wspólne zasady zabezpieczenia dla dowództwa, agencji czy formacji.

Środki bezpieczeństwa stosowane w każdej formacji ACE obejmują m.in. takie zagadnienia, jak: organizacja bezpieczeństwa, bezpieczeństwo fizyczne, dokumentów, systemu ADP, tj. sieci automatycznej obróbki danych, jak również bezpieczeństwo techniczne i komunikacji, ze szczególnym uwzględnieniem bezpieczeństwa materiałów kryptograficznych. Środki stosowane w każdej formacji ACE obejmują wszystkie osoby mające dostęp do informacji niejawnych i wszystkie pomieszczenia mieszczące takie informacje lub inne istotne elementy operacyjne. Wszystkie działania skoordynowane są w taki sposób, aby zostały spełnione minimalne wymagania operacyjne i warunki lokalne.

Dyrektywa Bezpieczeństwa ACE zawiera następujące części:

---

[25] *Dyrektywa Bezpieczeństwa ACE (Zjednoczonego Dowództwa Europejskiego) Numer 70-1*, NATO jawne, 1997.

- Część I: informacje ogólne;
- Część II:zabezpieczenia prewencyjne;
- Część III:zabezpieczenia dokumentów;
- Część IV:bezpieczeństwo osobowe;
- Część V:INFOSEC;
- Część VI:procedury bezpieczeństwa.

Część II jest najbardziej interesująca z punktu widzenia wymagań stawianych systemom ochrony obiektów wojskowych w kontekście członkostwa Polski w NATO. W rozdziale 1 części I zaprezentowane są informacje dotyczące podstawowych zasad i wymagań minimalnych w tym: organizacji bezpieczeństwa, bezpieczeństwa ochronnego, dokumentów, personelu, INFOSEC - z ang. Info Security – ochrona informacji, a w rozdziale 2 omówiona jest organizacja bezpieczeństwa, obowiązki i planowanie w tym: rola Komitetu Wojskowego, władze bezpieczeństwa, delegowanie uprawnień w zakresie bezpieczeństwa, odpowiedzialność dowództwa, stanowiska aparatu bezpieczeństwa, odpowiedzialność indywidualna, wewnętrzne kontrole bezpieczeństwa, odstępstwa i wsparcie w zakresie kontrwywiadu.

W części II przedstawione są wymagania w zakresie zabezpieczenia prewencyjnego. W tym rozdziale omówione są z nazwy sposoby i środki neutralizacji zagrożeń. Rozdział dotyczący bezpieczeństwa fizycznego zawiera m.in.: omówienie stref bezpieczeństwa (klasy I i II), koncepcji stref bezpieczeństwa, kontroli dostępu, w tym automatycznych systemów kontroli dostępu, kontroli wyrywkowej, zasad wydawania przepustek, organizacji straży, patroli i strażniczych oddziałów reagujących, sposobów przechowywania niejawnych informacji NATO.

Przedstawiono wymagania co do fizycznego zabezpieczenia, za pomocą kontenerów, przechowywanych informacji NATO (klasy A, B i C), sejfów i pomieszczeń wzmocnionych, zamków mechanicznych, zamków szyfrowych, użytkowania kluczy. Zaprezentowano potrzeby w zakresie ochrony biur, pokojów konferencyjnych i stref przed aktywnym i pasywnym podsłuchem audio i wideo, zasady tworzenia obszarów technicznie bezpiecznych.

Określone są zasady dotyczące bezpieczeństwa przekaźników komunikacyjnych, terminali i materiałów krypto, nadzoru nad nimi oraz kontrwywiadowczego programu bezpieczeństwa technicznego, wykorzystującego techniczne środki przeciwpodsłuchowe.

W aneksie A do rozdziału 1 części II przedstawiono szerzej zadania i wymagania co do barier fizycznych, elektronicznych systemów ochrony dostępu i włamania. Natomiast aneks B zawiera informacje co do urządzeń do przechowywania niejawnych materiałów NATO. Aneks C określa wymagania minimalne dla obszarów technicznie bezpiecznych (TSA – z ang. - Technically Secure Area) w stosunku do: telefonów, urządzeń komunikacji wewnętrznej,

podwójnych sufitów, ścian i podłóg, kanałów ogrzewczych i klimatyzacyjnych, rur, okablowania oraz izolacji akustycznej pomieszczeń, a także wielkość i sposoby zabezpieczania otworów i drzwi. Omówione są wymagania bezpieczeństwa w warunkach polowych i bojowych, zasady tymczasowego przemieszczania urządzeń stałych, obszary TSA w bunkrach.

Rozdział 2 części II dyrektywy ACE zawiera omówienie zabezpieczenia instalacji ACE przed sabotażem i terroryzmem. Ze względu na trudne do przewidzenia okoliczności sabotażu, każda formacja ACE tworzy własne procedury bezpieczeństwa wewnętrznego. Natomiast zagrożenie terrorystyczne może być skierowane przeciw organizacjom ACE i ich personelowi.

Zagrożenia terrorystyczne mogą obejmować:

- ataki bombowe – bomby umieszczone również w samochodach, przenośnych walizkach i urządzenia zapalające, w poczcie;
- morderstwa, porwania i próby zastraszania członków personelu ACE lub ich rodzin;
- demonstracje wywoływane dla rozruchów lub powodowania konfrontacji;
- bezpośrednie ataki na pomieszczenia ACE lub ich okupacja;
- fałszywe alarmy (szczególnie bombowe) z zamiarem szykanowania.

Przedstawiony jest podział obowiązków i odpowiedzialności kraju goszczącego i macierzystego w zakresie zabezpieczenia. Zaprezentowano planowanie bezpieczeństwa wewnętrznego, prowadzenie szkoleń i kontroli. Przedstawiono procedury przyjmowania informacji i ostrzeżeń o działalności terrorystycznej, finansowania zabezpieczeń fizycznych i innych materiałów zabezpieczających. Ważnym elementem zabezpieczenia jest koordynacja i nadzór sekcji antyterrorystycznych i antysabotażowych.

Do drugiego rozdziału części II dołączono następujące aneksy:

- aneks A – uwagi na temat planowania zabezpieczeń przeciw atakom.
- aneks B – stany alarmowe i podejmowanie środki zabezpieczenia.

Część III, omawiająca zabezpieczenie dokumentów, zawiera następujące rozdziały tematyczne: system rejestracji dokumentów z klauzulami „Cosmic" i „Atomal", klauzule i oznaczenia dokumentów, przygotowanie, przesyłanie, niszczenie i nadzór nad dokumentami niejawnymi, ujawnienie informacji NATO.

W części IV, ujmującej bezpieczeństwo osobowe, zawarte są następujące rozdziały: dostęp do niejawnych materiałów NATO, szkolenie i instrukcje bezpieczeństwa.

W części V, dotyczącej bezpieczeństwa ADP/INFOSEC (Automatic Data Processing – z ang. - bezpieczeństwo danych i ich procesu obróbki), zaprezentowane są: zasady i wymagania ACE/INFOSEC; organizacja i odpowiedzialność; zabezpieczenie informacji NATO gromadzonej, transmitowanej w systemach i sieciach ADP; bezpieczeństwo nośników

informacji; wolno stojące systemy ADP; bezpieczeństwo komunikacji; przenośne systemy ADP; oprogramowanie złośliwe i wirusy.

Część VI, omawiająca procedury bezpieczeństwa, zawiera: naruszenie reguł bezpieczeństwa; inspekcje bezpieczeństwa; bezpieczeństwo techniczne.

Omówiony dokument jest podstawą dla krajów członkowskich NATO do opracowania szczegółów organizacyjnych i technicznych ochrony obiektów wojskowych należących do struktury wojskowej Sojuszu. Wskazuje kierunki i wymagania co do obrony pozostałych obiektów wchodzących w skład systemu obronnego państwa.

Wnioski

Stan ochrony obiektów wojskowych, pomimo podjęcia szeregu inicjatyw prawnych, organizacyjnych i technicznych, jest nadal niezadowalający i musi ulec zasadniczej poprawie w związku z obecnością Polski w strukturach NATO.

Istniejące rozwiązania systemów ochrony obiektów wojskowych ukierunkowano na nowoczesne systemy ochrony technicznej. Osiągnięto to dzięki możliwości stosowania najlepszych światowych rozwiązań oraz zwiększeniu nakładów przeznaczanych na ochronę obiektów wojskowych. Jednak nadal istnieje pilny do rozwiązania problem optymalnego wyboru najlepszych rozwiązań technicznych stosowanych w ochronie obiektów wojskowych, adekwatnie do kategorii zagrożenia.

Brak odpowiedniego doświadczenia, znormalizowanych, sprawdzonych wytycznych i procedur, dostatecznej wiedzy w zakresie ochrony obiektów oraz bariery finansowe są przyczyną często nieprawidłowych rozwiązań w zakresie ochrony obiektów.

Wprowadzone w życie akty normatywne, szczególnie zaś ustawa o ochronie informacji niejawnych, wymusza konieczność fizycznej ochrony obiektów wojskowych. Fizyczna ochrona informacji niejawnych w obiektach wojskowych powinna obejmować ochronę przed:

- działaniem obcych służb specjalnych;
- zamachem terrorystycznym lub sabotażem;
- kradzieżą lub zniszczeniem materiału;
- próbą wejścia osób nieuprawnionych;
- nieuprawnionym dostępem pracowników do materiałów oznaczonych klauzulą tajności.

Szczególnym zagrożeniem dla struktur obronnych państwa jest rozwijający się w zmodernizowanej formie terroryzm. Wszystkie wymienione zagrożenia mogą zostać zneutralizowane przez systemy alarmowe, posiadające cechy organizacyjne i techniczne

umożliwiające bardzo wczesne wykrywanie potencjalnych zagrożeń, ich analizę, diagnozę i uruchamianie procedur interwencyjnych i zapobiegawczych lub minimalizujących skutki wtargnięcia intruza.

W celu zapewnienia praktycznej efektywności stosowania systemów ochrony w obiektach wojskowych należy stworzyć model systemu ochrony wykorzystujący systemy sygnalizacji zagrożeń i alarmowe na potrzeby obronności państwa.

Omawiany model powinien wzorcowo prezentować sposób zabezpieczenia oraz spełniać wszystkie wymagania stawiane przez ochraniany obiekt należący do struktury obronnej państwa. Budowa takiego modelu jest możliwa po opracowaniu metodologii tworzenia modelu.

Metodologia projektowania i budowy modelu systemu ochrony obiektu wojskowego, jak również ich symulacja działania wraz z procedurami weryfikacyjnymi jest istotnym elementem dostosowania krajowych systemów ochrony obiektów wojskowych do standardów obowiązujących w państwach NATO.

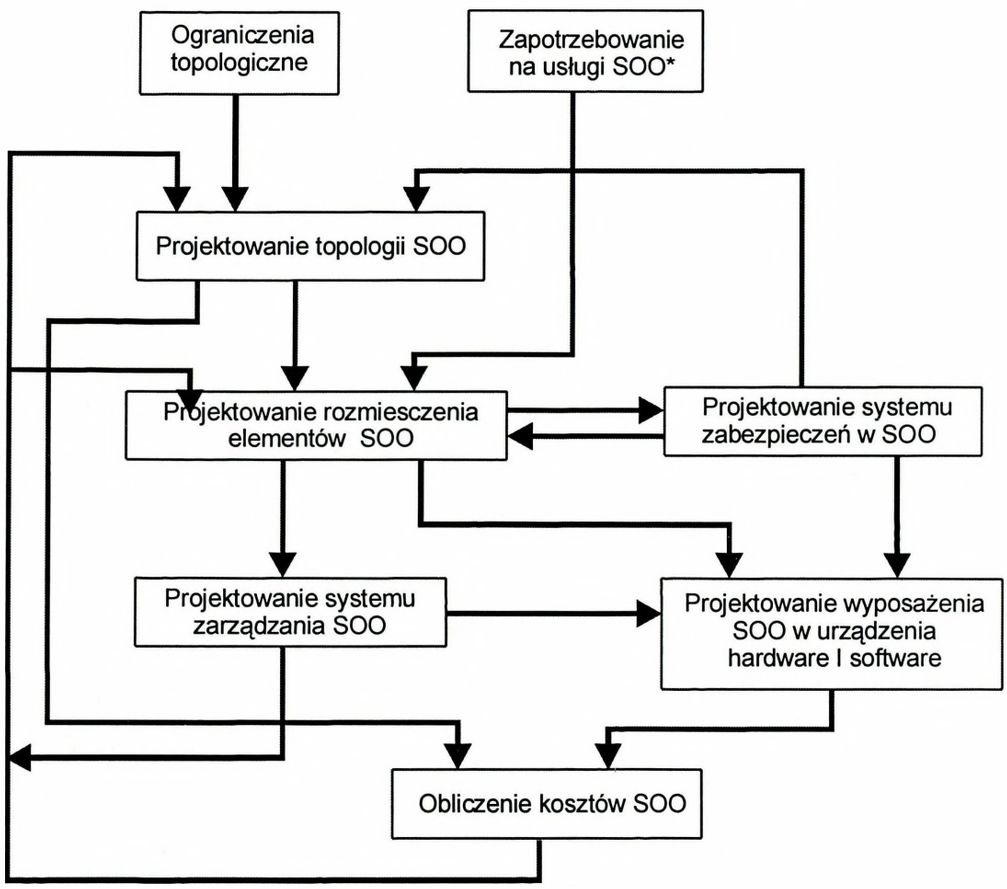
Należy podjąć działania podnoszące standard bezpieczeństwa obiektów wojskowych w kontekście członkostwa Polski w NATO i wymagań stawianych ochronie obiektów wojskowych przez dyrektywy bezpieczeństwa ACE obowiązujące w państwach Sojuszu.

4. MODEL SYSTEMU OCHRONY OBIEKTÓW WOJSKOWYCH

4.1. Projektowanie systemu ochrony obiektu

Projektowanie systemu ochrony obiektów jest procesem bardzo złożonym i trudnym z uwagi na rozmiar i skomplikowanie projektowanych systemów oraz mnogość i różnorodność czynników, które powinny być uwzględnione w trakcie tego procesu. Podstawowym zadaniem jest doprowadzenie do rozwiązania, które minimalizowałoby koszt zaprojektowanego systemu ochrony przy spełnieniu narzuconych przez niego wymagań technicznych, eksploatacyjnych, niezawodnościowych, itp. przy uwzględnieniu różnorodnych ograniczeń na możliwe do zaakceptowania rozwiązania.

W zasadzie nie istnieją algorytmy, które pozwoliłyby na bezpośrednie uzyskanie rozwiązania w ten sposób sformułowanego problemu. W procesie projektowania systemu ochrony obiektów dochodzi z reguły do jego dekomponowania na mniejsze elementy, w obrębie których poszukuje się (niezależnie od pozostałych) optymalnego bądź tylko zadowalającego rozwiązania.



*SOO - system ochrony obiektów

Schemat 4.1.1.Ogólny schemat blokowy procesu projektowania systemu ochrony obiektów

Ogólny układ blokowy procesu projektowania systemu ochrony obiektu przedstawiono na schemacie 4.1.1. Ilustruje on zasadniczą cechę tego procesu, opierającą się na daleko idącej współzależności nieomal jego wszystkich elementów. Powiązane są one bowiem ze sobą wzajemnymi sprzężeniami zwrotnymi powodującymi, że projektowanie systemu ochrony obiektu jest procesem o charakterze iteracyjnym, doprowadzającym do ostatecznego rozwiązania w wyniku szeregu przybliżeń modyfikacji poszczególnych jego elementów.

Do głównych elementów procesu projektowego, jakie można wyróżnić przy odpowiednio wysokim poziomie jego ogólności, należy zaliczyć:

- projektowanie topologii systemu ochrony obiektu – określenie jego struktury topologicznej, obejmujące:
  - położenie centrali alarmowej i urządzeń alarmowych;
  - ich wzajemne powiązanie;
  - sieć kablową;
  - uwzględnienie czynników ograniczeń nałożonych na tę strukturę, wymagań stosowanego systemu zabezpieczeń i zarządzania;
- wyznaczenie w obrębie przyjętej struktury systemu ochrony – dróg komunikacyjnych we wszystkich możliwych relacjach połączeń międzywęzłowych (tzw. routing), drogi muszą być dla poszczególnych relacji pojedyncze lub wielokrotne;
- alokacja zapotrzebowań na systemy ochrony oparta na macierzy zainteresowań:
  - rozdział tych zapotrzebowań przy wykorzystaniu analizy i diagnostyki,
  - określenie potrzeb dla określenia stopnia zabezpieczenia i zarządzania,
  - wyznaczenie niezbędnych parametrów organizacyjno-technicznych pracy systemu ochrony;
- projektowanie systemu zarządzania systemem ochrony;
- zaprojektowanie wyposażenia systemu ochrony w odpowiednie urządzenia w szerokim rozumieniu tego słowa, tzn. zarówno hardware, jak i software;
- obliczenie całkowitego kosztu projektowanego systemu ochrony.

Opisane wyżej rozważania prowadzą do wniosku, że możliwe jest ogólne sformułowanie problemu projektowania systemu ochrony obiektu, a także określenie podstawowych składników

algorytmicznych procesu projektowania.[1] Praktyczna realizacja procesu projektowania systemu ochrony obiektu natrafia na poważne trudności. Można wskazać dwa zasadnicze źródła tych trudności:

- złożoność obliczeniowa,
- brak jednoznacznych kryteriów optymalizacji.

Złożoność obliczeniowa związana jest nie tylko z wielkością „rzeczywistych" systemów ochrony, lecz także z wymogiem projektowania równocześnie wielu ze sobą powiązanych konfiguracji systemu i bogactwem możliwych metod wykorzystania środków służących do tego celu. Ponadto pojawia się problem złożoności sprzętu instalowanego w tych systemach.

Trudności z określeniem analitycznych kryteriów ukierunkowujących proces projektowania (optymalizacji) wynikają głównie ze wzrostu znaczenia „poza ilościowego" przesłanek oceny jakości systemu ochrony obiektu. Szczególnie trudno wyrazić ilościowo pożądane właściwości systemu ochrony w kontekście problemów związanych z jego zarządzaniem i eksploatacją:
Jak uwzględnić w globalnym koszcie systemu ochrony obiektu korzyści wynikające z elastyczności strukturalnej jego zasobów?

1. Jak wyrazić ilościowo względne korzyści z zastosowania różnych metod oceny (określenia) zasobów zważywszy, że różnią się one zarówno złożonością realizacji, jak i własnościami eksploatacyjnymi (np. czasem reakcji na zmiany stanu systemu ochrony)?

Wobec powyższego, nie można liczyć na stworzenie w pełni algorytmicznej metody projektowania systemu ochrony obiektów – „automatu do projektowania". Przedstawiony tu zarys metodologii pozwala jedynie na stworzenie ram procesu projektowania i narzędzi wspomagających ten wielokryterialny proces. Ponieważ nie wszystkie aspekty projektu dadzą się wyrazić ilościowo, więc wiedza i doświadczenie projektanta muszą, jak zwykle, stanowić ostateczny punkt odniesienia.

W procesie projektowania systemów ochrony wykorzystuje się dzisiaj powszechnie technikę komputerową. Używane programy i systemy projektowania korzystają z różnych technik, mają bardzo zróżnicowane właściwości i możliwości wykorzystania, lecz wszystkie mają dwie wspólne cechy:

- proces projektowania jest ściśle związany z optymalizacją;
- w procesie projektowania wykorzystuje się różnego rodzaju modele.

---

[1] P. Sienkiewicz –red. nauk., *Wystarczalność obronna*, Bellona, Warszawa 1996.

Komputerowe programy użytkowe, bazujące na matematycznych modelach systemów, wykorzystują różne techniki umożliwiające symulację zachowań badanych systemów ochrony. Wszystkie te systemy, mając bardzo zróżnicowane właściwości i możliwości aplikacyjne, a projektanci próbują udzielić odpowiedzi na dwa pytania:

1. Jaki model w sposób najwierniejszy oddaje cechy badanego systemu?
2. Jak zoptymalizować modelowaną rzeczywistość?

W wypadku projektowania systemu ochrony na potrzeby obronności przeprowadzenie obserwacji jego funkcjonowania i określenie jego parametrów, w warunkach rzeczywistego stanu zagrożeń jest zadaniem kosztownym, długotrwałym i trudnym do wykonania ze względu na złożoność i niepowtarzalność sytuacji. Fragmentaryczne wyniki przeprowadzonych obserwacji są niepełne i nie odzwierciedlają faktycznego stanu rzeczy. Dlatego najwłaściwszą metodą jest prowadzenie badań modeli systemów ochrony obiektów.

W odniesieniu do systemów ochrony obiektów wojskowych, ze względu na złożoność procesu i warunki w jakich funkcjonują, poszukiwanie analogii między systemem rzeczywistym a zbudowanym modelem sprawia pewne trudności. Opracowanie każdego modelu wymaga przyjęcia szeregu kryteriów i ograniczeń będących w swym założeniu warunkami brzegowymi.

Przez model rozumie się taki układ, który można poddać się analizie lub materialnie zrealizować, który odzwierciedlając przedmiot badania, zdolny jest zastępować go tak, że jego badanie dostarcza nam nowej informacji o tym przedmiocie[2]. Ogólnie można stwierdzić, że model jest odwzorowaniem rzeczy i zjawisk czy procesów, które zamierzamy stworzyć lub określić[3]. Innymi słowy: model powinien przedstawiać elementy systemu, wzajemne ich powiązanie i oddziaływanie. Otaczającą nas rzeczywistość można odzwierciedlić za pomocą wielu form, jak również można spotkać wiele rodzajów modeli i sposobów ich klasyfikacji. Podział modeli na rodzaje, klasy czy grupy przeprowadza się na podstawie kryteriów przyjętych zależnie od konkretnych potrzeb wynikających z celu, któremu klasyfikacja ma służyć.

Za jedno z najprostszych, ale niezbyt ścisłych, kryteriów podziału modeli można przyjąć charakter „materiału" (myśl, pismo, rysunek, materia, energia itp.), z którego powstają:

- modele doznaniowe;
- modele opisowe;
- modele fizyczne.

---

[2] Praca zbiorowa, *Wybrane metody optymalizacji decyzji*, Wydawnictwo Ministerstwa Obrony Narodowej 1969.
[3] Praca zbiorowa, *Teoria systemów*, Politechnika Wrocławska 1980

Można je również podzielić według formy odzwierciedlenia badanej rzeczywistości następująco:[4]

- poglądowe;
- słowne;
- analogowe;
- matematyczne.

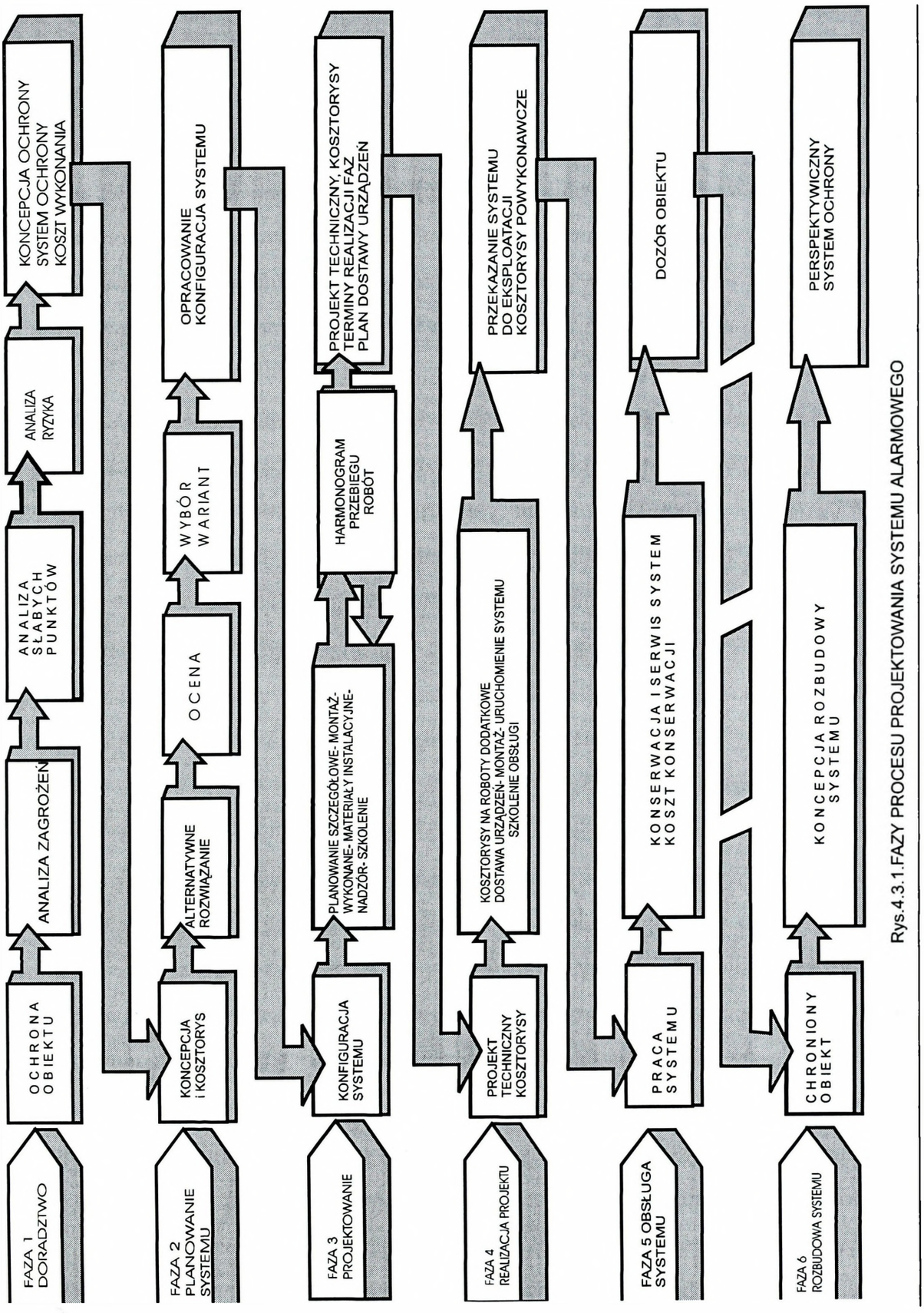
Budowa modelu, jego badanie oraz poszukiwanie analogii pomiędzy zbudowanym modelem a rzeczywistym systemem charakteryzują badania modelowe. Zbudowane modele systemu stanowią przedmiot modelowania. Modelowanie jest metodą badania procesów technicznych, fizycznych, chemicznych, biologicznych i innych, polegającą na dokonywaniu prób i pomiarów na modelach jako układach dogodnych ze względu na dużą różnorodność dostępnych technik pomiarowych, większe bezpieczeństwo operatora, mniejsze koszty badań.

Na etapie opracowywania modelu przyjęto szereg założeń, zarówno w postaci wymagań, jak i niezbędnych uproszczeń. System ochrony obiektu, z uwagi na swą specyfikę, wymuszał systemowe podejście do badań, których podstawą było świadome posługiwanie się modelem systemu na określonym poziomie uszczegółowienia – adekwatnym do aspektu analizowanych procesów.

Przebieg tworzenia koncepcji, projektu i realizacji systemu ochrony technicznej przedstawiono na rysunku 4.1.1. W zasadzie w każdym podejściu do problemu projektowania możemy wyróżnić sześć podstawowych faz:[5]

- faza 1 jest to pierwsza wstępna część tworzenia koncepcji ochrony obiektu, odgrywa w niej pierwszorzędną rolę wiedza i elastyczność podejścia projektanta, który występuje w tej fazie jako doradca techniczny i organizacyjny przyszłego inwestora lub użytkownika. Na podstawie posiadanych informacji, wizji lokalnych, danych uzyskanych od klienta projektant dokonuje analizy zagrożeń, analizy słabych punktów i ryzyka dla danego obiektu, dokonuje kwalifikacji obiektu pod względem klasy zagrożeń i klasy systemu. Ta analiza jest niezbędna do opracowania koncepcji ochrony obiektu pod względem zabezpieczenia technicznego, jak i organizacyjnego. Projektant odrzuca wszystkie rozwiązania nie spełniające obowiązujących przepisów i wymagań.

[4] J. Stoner, Ch. Wankel, *Kierowanie*, PWN, Warszawa 1994.
[5] O informacji o metodyce projektowania znajduje się w opracowaniu A. Wójcik *Przebieg procesu projektowania*.



Rys.4.3.1.FAZY PROCESU PROJEKTOWANIA SYSTEMU ALARMOWEGO

Chodzi tu głównie o urządzenia, ich zastosowanie w odpowiednich systemach. I tak w systemach o wysokim stopniu ryzyka, np. w jednostce wojskowej, zostaną zastosowane adekwatne urządzenia zalecane do stosowania w tych klasach systemów, które jednocześnie posiadają odpowiednie świadectwa dopuszczenia i atestacji zarówno polskie, ale często i zagraniczne, które są zgodne z wymaganiami norm europejskich;

- faza 2 - prowadzi do opracowania konfiguracji systemu możliwego dla inwestora do realizacji pod względem technicznym i ekonomicznym. Opracowanie konkretnego systemu poprzedza wariantowe opracowanie rozwiązań, które po wnikliwej ocenie krytycznej i optymalizacji kosztów, pozwala dokonać optymalnego wyboru rozwiązania problemu technicznej ochrony;
- faza 3 - jest etapem szczegółowego przedstawienia opracowanej koncepcji, dotyczy to planowania szczegółów wykonania instalacji przewodowej, montażu, oceny zapotrzebowania materiałów instalacyjnych, przeszkolenia i informacji dla wykonawców, są to prace związane z tworzeniem projektu technicznego, który jest podstawą do opracowania terminarza robót i dostawy urządzeń;
- faza 4 - jest etapem nadzoru projektanta nad przebiegiem prac instalacyjnych i montażowych, korekty i modernizacji bieżących zmian. Projektant powinien być obecny także przy odbiorze systemu alarmowego, potwierdzić czy realizacja systemu alarmowego jest zgodna z projektem;
- faza 5 - obejmuje bieżącą eksploatację obiektu, szczególnie w okresie gwarancyjnym. Rola projektanta jest tu istotna z punktu widzenia ewentualnego wprowadzenia zmian i korekty projektu lub doprowadzenia do założonych rozwiązań w projekcie w celu poprawy zdolności ochronnych systemu;
- faza 6 - wymusza ujęcie w projekcie rozwiązania, które jest na tyle elastyczne, aby w przyszłości można było dokonać modernizacji systemu. Jak wynika z powyższych rozważań rola projektanta w procesie tworzenia i wdrażania systemu techniczno - organizacyjnej ochrony obiektu jest istotna dla wszystkich uczestników tego procesu, zarówno dla inwestora, wykonawcy, jak i dla bezpośredniego użytkownika systemu ochrony.

Tworzenie koncepcji ochrony jest procesem złożonym, obejmującym szereg istotnych elementów z różnych dziedzin nauki i branż. Projektant musi ująć szereg problemów w różnych płaszczyznach analizy. Podstawowymi czynnikami, które kształtują koncepcję zabezpieczenia są

rzeczywiste możliwe do przewidzenia na tym etapie wiedzy i możliwości oraz niemożliwe do przewidzenia w chwili zagrożenia. Oczywiście wszystkie rodzaje ingerencji obcej, tj. napad, włamanie, sabotaż, terroryzm, szpiegostwo, itd. stawiane są przy analizie ryzyka na pierwszym miejscu. Nie należy zapominać podczas procesu tworzenia koncepcji o pozostałych czynnikach zagrożenia takich, jak: wypadki przy pracy, które wymuszają tworzenie stref ochronnych przed zagrożeniami przemysłowymi, pożarami, eksplozjami, mającymi także przyczyny naturalne.

Eksploatacja urządzeń podczas procesów technologicznych może także stanowić zagrożenie dla życia i mienia. Urządzenia będące na wyposażeniu obiektu, np. schody ewakuacyjne mogą być z powodzeniem wykorzystane do przełamania systemu ochrony.

Czynniki kształtujące koncepcję ochrony wynikają z obowiązujących przepisów i zakresu ochrony, ale także innych, np. zasady ewakuacji ludzi w przypadku paniki, które zasadniczo są w sprzeczności z wymaganiami systemu alarmowego. Konieczna jest analiza realizacji założonych celów, a także funkcji w ujęciu strategicznym, jakiemu powinno służyć zabezpieczenie, tj. czy skutki złego zabezpieczenia będą miały konsekwencje w wymiarze mikro- czy też makroskali dla systemu obronnego państwa. Środki organizacyjne i techniczne, wynikające z możliwych do poniesienia nakładów finansowych na ochronę, stanowią ważny element w ocenie koncepcji pod względem możliwości i efektywności zastosowanej ochrony.[6]

Na przykładzie instalacji systemu alarmowego włamania i napadu autor przedstawił zasadnicze czynności występujące w procesie projektowania systemu ochrony obiektu w ujęciu praktycznym, pozwalający opracować procedury projektowania i kontroli realizacji systemu ochrony obiektu.[7] (rys. 4.1.2.). Procesem wymagającym analitycznego podejścia jest określenie:

- kategorii zagrożenia obiektu;
- poziomu ryzyka;
- określenie typu obiektu pod względem konstrukcyjno-budowlanym, a tym samym określenie słabych punktów pod względem zabezpieczenia mechanicznego, tj. ilość i typy otworów okiennych, drzwiowych, świetlików, balkonów, zejść, korytarzy, rodzaj dachu, kąt pochylenia, itd.;
- funkcjonowania i organizacji pracy w obiekcie, priorytetów dostępu i ochrony, postępowania w warunkach zagrożeń, odpowiedzialności personalnej i materialnej, itd.;

---

[6] Wójcik A., *Metodyka kosztorysowania prac projektowych i wykonawstwa elektronicznych systemów alarmowych*, ZTOM TECHOM 1999 – opracowanie własne.

[7] Opracowanie własne

- otoczenia obiektu, tj. zabudowy, wzajemnych relacji i zależności z obcymi lub obiektami np. wspólne węzły komunikacyjne;
- innych trudnych do określenia lub niemożliwych zagrożeń i warunków funkcjonowania obiektu np. zmiany architektoniczne zewnętrzne.

Po przeprowadzeniu analizy i opracowaniu danych projektant przystępuje do określania środków neutralizacji zagrożeń tj. środków technicznych i organizacyjnych ochrony obiektu.

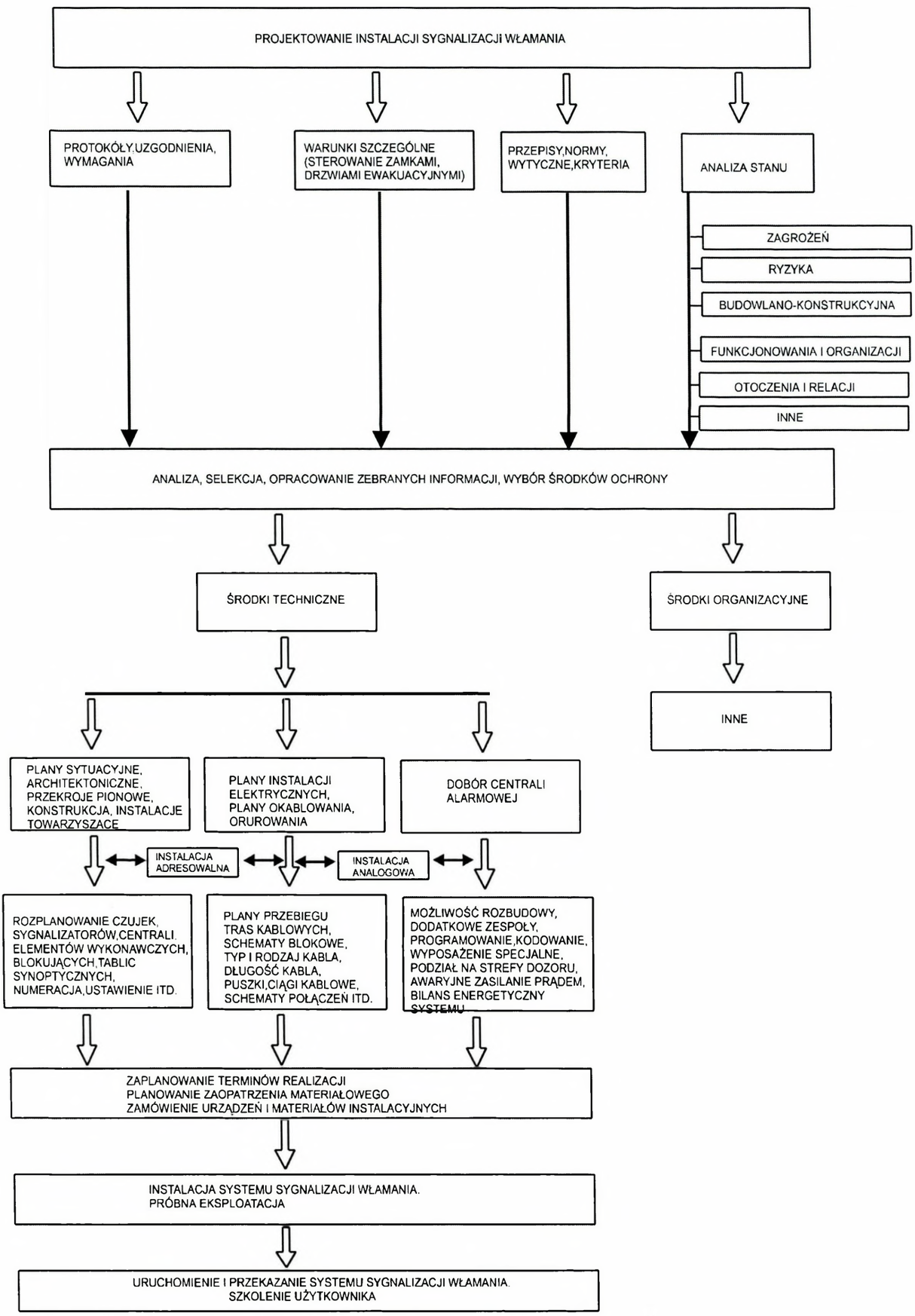
Na podstawie planów architektonicznych, konstrukcyjnych, instalacji towarzyszących, tj. elektrycznych, klimatyzacji, grzewczych, energetycznych, sieci telekomunikacyjnych i komputerowych, następuje rozplanowanie czujek, elementów wykonawczych np. dobór typu zamka szyfrowego, tablicy synoptycznej. Ustalane jest miejsce montażu elementów sterujących, tj. centrali alarmowej. Dokonywana jest numeracja i przyporządkowanie urządzeń. Przed przystąpieniem do zaplanowania tras kablowych podejmowana jest decyzja co do wyboru techniki transmisji sygnałów sterujących i alarmowych. Jej konsekwencją jest wybór typu i rodzaj okablowania (przewodów) stosowanego w systemie ochrony.

Wymienione czynności i przedsięwzięcia kończą proces organizacyjno - technicznego projektowania systemu ochrony obiektu. Ukończony projekt jest podstawą do planowania przebiegu prac instalacyjnych i montażowych, zaopatrzenia materiałowego, itd. Dalszą konsekwencją realizacji projektu jest wdrożenie systemu do eksploatacji. Po uruchomieniu systemu i przekazaniu go do użytkowania, powinno nastąpić przeszkolenie bezpośrednich użytkowników.

Przebieg procesu projektowania powinien wyglądać następująco:

a. Analiza zagrożeń.
b. Ocena poziomu ryzyka.
c. Klasyfikacja obiektu do klasy systemu alarmowania.
d. Dobór urządzeń alarmowych do klasy systemu.
e. Organizacja funkcjonowania systemu- podział na strefy dozoru.
f. Planowanie rozmieszczenia urządzeń.
g. Planowanie przebiegu tras kablowych.
h. Dokonanie bilansu energetycznego i dobór systemu zasilania awaryjnego.
i. Analiza zagrożeń.
j. Ocena poziomu ryzyka.
k. Klasyfikacja obiektu do klasy systemu alarmowania.

Rys.4.1.2.Przebieg procesu projektowania systemu ochrony obiektu w ujęciu praktycznym



l. Dobór urządzeń alarmowych do klasy systemu.

m. Organizacja funkcjonowania systemu- podział na strefy dozoru.

n. Planowanie rozmieszczenia urządzeń.

o. Planowanie przebiegu tras kablowych.

p. Dokonanie bilansu energetycznego i dobór systemu zasilania awaryjnego.

q. Określenie współzależności systemu alarmowego w stosunku do innych instalacji alarmowych w obiekcie w tym automatyki budynku.

r. Organizacja stanowiska nadzoru wewnętrznego nad systemem, tj. wymagania architektoniczne, wyposażenie, ergonomiczne rozmieszczenie urządzeń sterujących i sygnalizujących.

s. Opracowanie współdziałania systemu z monitorowaniem zewnętrznym.

t. Opracowanie zintegrowanego systemu sygnalizacji zagrożeń (ochrony obiektu).

Projektant na etapie opracowywania koncepcji na podstawie przeprowadzonej analizy zagrożeń po określeniu kategorii zagrożonej wartości (zgodnie z Polską Normą może być określona: od Z1-niska do Z4-najwyższa klasy zagrożenia) i po jej zoptymalizowaniu musi dokonać wyboru klasy systemów i adekwatnie do tego przyjąć klasę urządzeń alarmowych. Dokonuje tego opierając się na ustalonej kategorii zagrożenia i analizie (ekspertyzie) zagrożenia np. włamaniowego z określeniem dróg i metod prawdopodobnego wniknięcia intruza (przeciwnika).

Niewątpliwie wybór przez projektanta technologii, w jakiej zostanie wykonany system alarmowy, determinuje skuteczność ochrony obiektu oraz efekt użytkowy i funkcjonalny, a w konsekwencji - koszty realizacji.[8]

Wykonanie systemu alarmowego możemy podzielić na następujące fazy:

- wykonanie instalacji przewodowej systemu;
- montaż urządzeń systemu;
- oprogramowanie systemu;
- uruchomienie systemu;
- praca próbna systemu;
- szkolenie obsługi;
- odbiór systemu.

[8] A. Wójcik., *Zasady opracowywania kosztorysów sygnalizacji alarmowej*, TECHOM, Warszawa 1996.

Nowoczesne systemy alarmowe umożliwiają projektowanie instalacji na bazie: techniki konwencjonalnej i techniki adresowej.[9]

e. technika konwencjonalna (wieloprzewodowa) - w technice konwencjonalnej poważnym ograniczeniem jest ilość elementów (np. czujek), które można przyporządkować (podłączyć) na jednej linii dozorowej. Zbyt duża ilość elementów utrudnia identyfikację uszkodzonego lub będącego w stanie alarmu elementu.

Taki sposób projektowania i wykonania jest wysokonakładowy ze względu na:

- zwiększoną komplikację i ograniczenia występujące przy projektowaniu, dotyczy to szczególnie ilości i mieszania różnych typów na linii dozorowej;
- brak możliwości precyzyjnego wskazania urządzenia;
- konieczność stosowania różnych typów kabli i materiałów instalacyjnych;
- ograniczenia funkcjonalne, użytkowe i programowe tak zbudowanego systemu;
- zwiększenie czasu przeznaczonego na wykonanie instalacji;
- dużą podatność instalacji na zakłócenia, co ma konsekwencje w zwiększonych kosztach napraw;
- konieczność zaplanowania większej ilości czasu na konserwację i serwis.

Systemy alarmowe wykonywane w technice konwencjonalnej znajdują zastosowanie w przypadku instalacji nieskomplikowanych, małych i niewymagających pod względem funkcjonalnym i użytkowym. Ze względu na wymienione wyżej i inne ograniczenia systemy konwencjonalne są wypierane przez nowoczesne instalacje oparte na magistralach adresowych.

b. technika adresowa (magistralowa) - jest to bardzo istotny element, o którym często zapomina się przy projektowaniu nowoczesnych systemów alarmowych, to inteligentna technologia przepływu danych. Przejrzysta technologia magistrali danych ma wiele zalet dla użytkownika i instalatora systemów alarmowych. Nie tylko pozwala na dokładną i indywidualną kontrolę całego systemu, ale jest także innowacyjna pod względem możliwości selektywnego komunikowania się z elementami systemu alarmowego.

Podstawowe zalety technologii magistralowej to obniżenie kosztów ze względu na:

- praktycznie brak zasadniczych ograniczeń projektowych i programowych;
- możliwość podłączenia dużej liczby urządzeń na magistrali oraz mieszania różnych typów urządzeń;

---

[9] A. Wójcik, *Niezawodność systemów sygnalizacji pożaru firmy effeff gwarancją bezpieczeństwa*, artykuł Instalator Polski, czerwiec 1998.

- skrócenie czasu projektowania przez ujednolicenie okablowania;
- skrócenie czasu wykonania i wynikające z tego tytułu oszczędności w nakładach na materiały instalacyjne;
- przejrzystość, elastyczność i prostotę serwisu instalacji;
- niezawodność instalacji;
- wysokie walory użytkowe i funkcjonalne;
- dużą odporność na zakłócenia i ujemny wpływ środowiska pracy;
- niskie koszty konserwacji i serwisu.

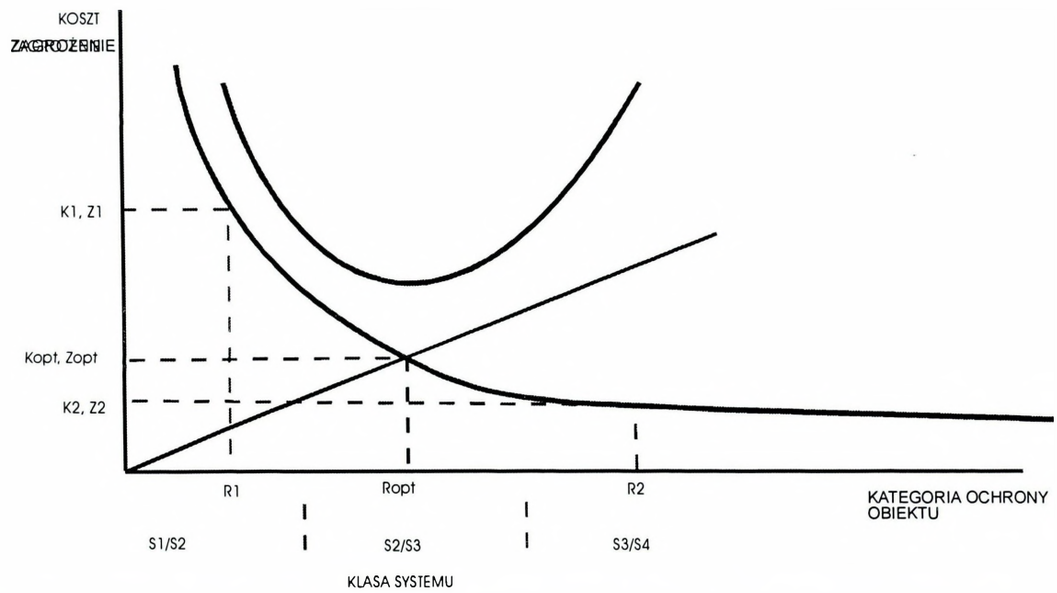
Instalacja magistralowa wymaga szczególnej staranności planistycznej i dokładności przy jej wykonywaniu.

Sporządzenie analizy kosztów jest jedną z poważniejszych czynności w procesie organizowania i przebiegu wszelkich przedsięwzięć gospodarczych, dotyczy to także instalacji systemów alarmowania i sygnalizacji zagrożeń[10]. Rachunek ekonomiczny nie powinien ograniczać, lecz wymuszać racjonalne działanie, w celu optymalizacji kosztów, uwzględniający nakłady na:

- wykonanie systemu sygnalizacji zagrożeń i alarmowania, w tym: dokumentację techniczno - kosztorysową systemu; instalacje teletechniczne systemu; oprogramowanie i uruchomienie systemu;
- szkolenie obsługi na różnych poziomach dostępu;
- eksploatację systemu uwzględniającą warunki techniczno – ekonomiczne, tzn.:
  - bieżące koszty obsługi użytkownika tj.: zużycie energii niezbędnej do prawidłowego funkcjonowania systemu; podlegające zużyciu materiały eksploatacyjne, np. karty magnetyczne itd.; ilość i kwalifikacje obsługi, tj. płace; poziom zapasów materiałowo –technicznych, koniecznych do utrzymania sprawności technicznej systemu;
  - serwis gwarancyjny i serwis pogwarancyjny oraz konserwację systemu; modernizację systemu, w zakresie kosztów: rozbudowy systemu o elementy podnoszące stan bezpieczeństwa obiektu; unowocześnienia systemu, uwzględniające starzenie techniczne i moralne elementów systemu.

[10] A. Wójcik, *Metodyka kosztorysowania prac projektowych i wykonawstwa elektronicznych systemów alarmowych*, skrypt ZTOM TECHOM 1999.

Przykad modelu optymalizacji kosztów na system ochrony technicznej przy jednoczesnym zmniejszeniu stopnia ryzyka przedstawia rysunek 4.1.4.[11] Optymalizacja kosztów znajduje szczególne zastosowanie w systemach wysokiej kategorii zagroenia, które wyst puje w obiektach wojskowych. Koszt jest elementem determinujcym poziom techniczny i jako wykonania systemu alarmowego, poniewa koszt zastosowanych w rozwizaniu technicznym systemu urzdze ma wpyw na technologi wykonania, która bezporednio oddziauje na koszt robocizny bezporedniej, np. sposób okablowania systemu i zwizane z tym nakady, a z kolei okablowanie systemu zwizane jest z moliwociami technicznymi systemu takim jak: moliwoci oprogramowania systemu; obsugi i eksploatacji; rozbudowy; konserwacji; elastycznoci itd..

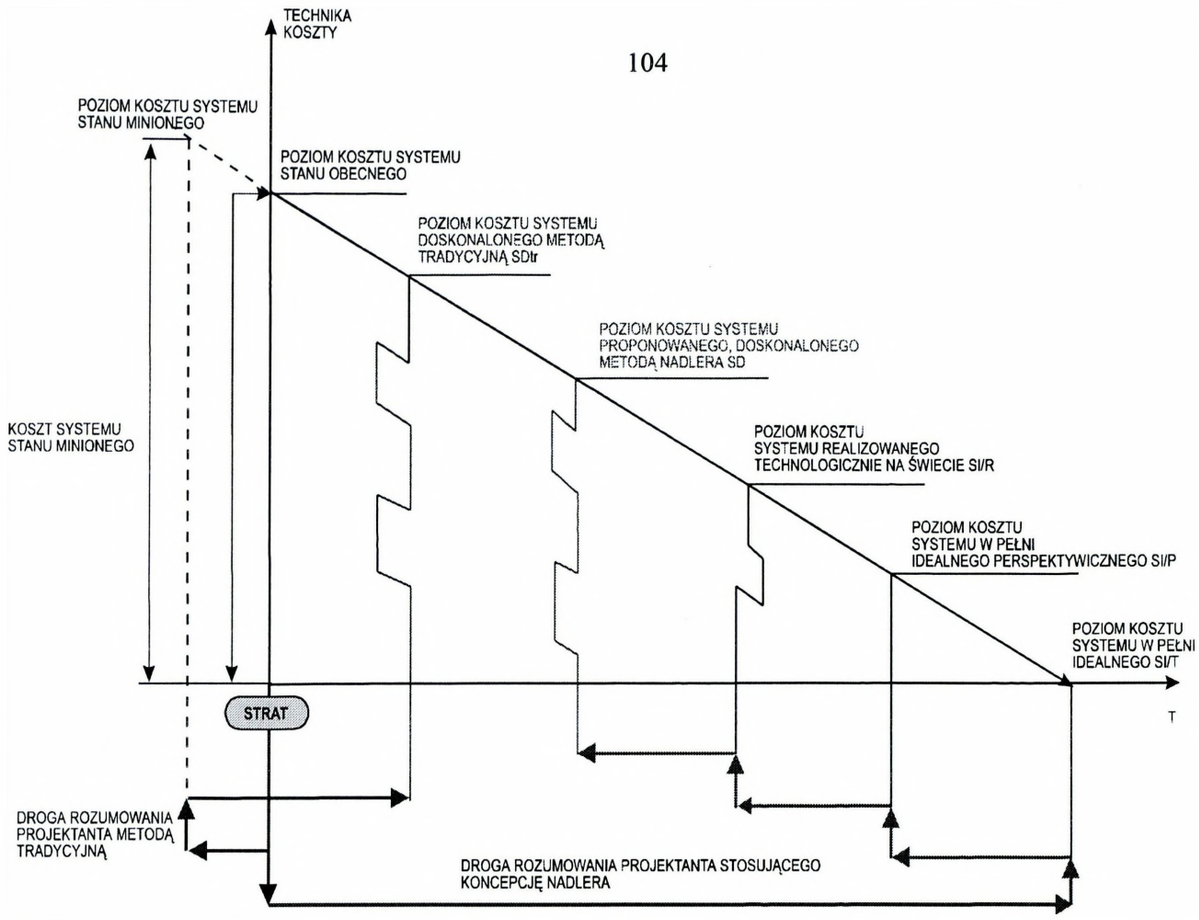


RYS.4.1.4.MODEL OPTYMALIZACJI KOSZTÓW PRZY PROJEKTOWANIU SYSTEMU OCHRONY OBIEKTU

Wybór technologii, w jakiej zostanie wykonany system alarmowy, determinuje skuteczno ochrony obiektu oraz efekt uytkowy i funkcjonalny a w konsekwencji - koszty realizacji.

Rysunek 4.1.5. przedstawia przebieg projektowania systemu alarmowego z wykorzystaniem modelu idealnego Nadlera.

[11] A. Wójcik, *Kosztorysowanie w ofercie, prac projektowych i wykonawczych oraz powykonawczych sygnalizacji alarmowej*, Przewodnik Rzeczoznawcy, Zeszyt Nr 4. Warszawa 1994.



Rys.4.1.5. ZALEŻNOŚĆ WYBORU DROGI ROZUMOWANIA PROJEKTANTA STOSUJĄCEGO KONCEPCJĘ TRADYCYJNĄ I NADLERA A KOSZTAMI ZASTOSOWANEJ TECHNIKI ZABEZPIECZEŃ.

Rysunek 4.1.5. prezentuje sposób doskonalenia modelu poprzez kolejne kroki przybliżające do oczekiwanego rozwiązania pod względem technicznym i kosztowym. Punktem wyjścia w metodzie Nadlera jest system (model) idealny. Ta metoda budowy modelu w stosunku do tradycyjnego opracowywania modelu pozwala wybrać najbardziej optymalne rozwiązanie organizacyjno – techniczne i kosztowe.

Stwierdzono, że zastosowany typ ochrony obiektu jest właściwy i wykorzystujący wszystkie jego możliwości oraz zasady wzajemnej asekuracji stref ochrony. Zasadniczo każdy obiekt zakwalifikowany do wyższej kategorii zagrożeń i klasy systemu powinien zawierać co najmniej dwie strefy ochrony.

Należy sprawdzić prawidłowość rozmieszczenia urządzeń wykonawczych, np. czujek, szyfratorów lub innych urządzeń wykonawczych, czy są rozmieszczone zgodnie ze wskazówkami producenta i wymaganiami normatywnymi. Plan rozmieszczenia urządzeń jest podstawą do opracowania instalacji przewodowej systemu wg obowiązujących zasad i przepisów, tj. wydzielenie i ochrona instalacji przewodowej, sposoby jej prowadzenia, tj. w rurkach pod tynkiem,

w wydzielonych zamkniętych korytkach itd., podanie typów przewodów, sposobów ich łączenia, uwzględnienie przepustów dla zbiorczej instalacji, określenie sposobów prowadzenia instalacji w pionach, w strefach nie chronionych, zasad zasilania urządzeń w energię elektryczną i sposobu oraz punktu zasilania nią urządzeń.

Niezbędne minimum projektowe zawiera także sprawdzenie systemu pod względem energetycznym, tj. czy system wytrzyma pracę w trybie awaryjnym w czasie określonym przez przepisy dla klasy systemu i stopnia zagrożenia obiektu. Dobór i zaprojektowanie odpowiedniego zasilania awaryjnego jest istotnym elementem w dokumentacji technicznej systemu. Wskazówki dotyczące zasad podłączania systemu alarmowego do głównej tablicy zasilającej, tj. wydzielony obwód zasilający nie podłączony do innych odbiorników, są ważnymi elementami ogólnych wymagań.

Część technologiczna dokumentacji obejmuje wykaz zastosowanych urządzeń, sposoby łączenia i wskazówki montażowe, a także schematy połączeń , jeżeli rozwiązanie jest prototypowe i nie posiada odpowiednika w instrukcji montażu producenta. Niezbędnym załącznikiem do dokumentacji są karty katalogowe urządzeń. Umożliwia to bezpośredni kontakt użytkownika z producentem czy dystrybutorem, ale także uwiarygodnia rozwiązanie projektu.

Elementem wyróżniającym dobry projekt od przypadkowego opracowania jest stosowanie przez projektanta zasady optymalizacji kosztów na wykonanie systemu alarmowego przy zachowaniu zasad ochrony i zmniejszenia zagrożenia systemu.

Podstawą wykonania projektu w zakresie technicznym są obowiązujące normy, wytyczne lub przepisy. Zestawienie arkuszy PN-93/E-08390 pod nazwą "Systemy alarmowe" daje podstawy do określenia podstawowych wymagań i kwalifikacji systemów alarmowych w zakresie ochrony osób i mienia w zabezpieczanych obiektach. Klasyfikacja zawarta w Polskiej Normie umożliwia tworzenia przez projektanta wymagań w stosunku do konkretnego rozwiązania systemu alarmowego. Biorąc pod uwagę już tylko cztery klasy systemów, tj. od SA1 do SA4, kategorii zagrożeń od Z1 do Z4 oraz klasy urządzeń odpowiednio stosowanych i zalecanych do tych systemów, tj. A, B, C i S projektant może dokonać kwalifikacji obiektu. Im wyższa klasa systemu, tym większe wymagania stawiane są dokumentacji pod względem szczegółowości wykonania. Systemy klasy SA3 i SA4 (obejmujące obiekty wojskowe) posiadają opracowaną wcześniej dokumentację (przed wykonaniem robót), na ogół przez wyspecjalizowane biuro projektowe czy też osobę nie będącą wykonawcą.

Bardzo ważne jest rozdzielenie etapu projektowania i wykonania w całym procesie realizacji systemu alarmowego w obiektach o dużym stopniu zagrożenia, tj. klas SA3 i SA4. Pozwala to uniknąć inwestorowi pewnych niedociągnięć wykonawczych i zachować pewność, że wykonany system jest zgodny z projektem.

4.1.1. Czynniki decydujące o doborze elementów systemu ochrony obiektu

Poniżej przedstawiono listę najważniejszych czynników mających bezpośredni wpływ na decyzję o doborze elementów systemu ochrony obiektu. Podstawowe czynniki charakteryzujące analizowany obiekt to:

1. Realizowane funkcje i zadania.

   Należy odpowiedzieć na podstawowe pytanie:

   - do jak ważnych zadań przeznaczony jest analizowany obiekt i jakie funkcje spełnia w systemie obronnym państwa?
   - jaki jest priorytet ważności obiektu w strukturze obronnej państwa?
   - czy jest to obiekt zastępowalny w wypełnianiu zadań w strukturze obronnej państwa przez inne obiekty?

2. Informacje organizacyjno – funkcjonalne dotyczące powiązań organizacyjnych w zakresie realizowania postawionych zadań przez poszczególne komórki organizacyjne obiektu, tzn:
   - odpowiedzialność i zakres obowiązków poszczególnych osób. Sposoby kierowania procesami decyzyjnymi, techniczno - administracyjnymi oraz czynniki procesu gospodarowania;
   - zbieranie informacji dotyczących procesów organizacji i zarządzania ludźmi i składnikami materialnymi oraz dokumentacji, a także obróbka, archiwizacja, przechowywanie, rozdział dokumentacji i informacji oraz jej dystrybucja; dobór osób do obsługi przesyłania informacji;
   - wewnętrzne funkcje poszczególnych elementów obiektu: organizacja ruchu osobowego, kontrola wejścia i wyjścia ludzi, ruch ludzi wewnątrz obiektu;
3. Organizacja ruchu materiałowego: kontrola wjazdu i wyjazdu; procesy magazynowania i przechowywania wewnątrz obiektu; obrót materiałami wewnątrz obiektu; dobór ludzi do obsługi obrotu materiałowego;
4. Organizacja obrotu pieniężnego: lokalizacja punktów obrotu pieniężnego; sposób zasilania w pieniądze; dobór ludzi do obsługi ruchu pieniężnego;
5. Budowlano – architektoniczne polegające na zebraniu danych dotyczących: fizycznego opisu obiektu w maksymalnie szczegółowym ujęciu, z uwzględnieniem fasady, piwnic, strychów,

drzwi, okien, ciągów komunikacyjnych i miejsc przyległych. Należy uwzględnić opis konstrukcyjny poszczególnych elementów architektonicznych obiektu, tj. materiał, wymiary, odporność, a szczególnie: lokalizację obiektu i jego kształt przestrzenny, konstrukcję obiektu, użyte materiały, instalacje elektryczne, instalacje wodno-kanalizacyjne, instalacje klimatyzacyjne, instalacje odgromowe, przeciwpożarowe i inne instalacje teletechniczne;

6. Opis położenia obiektu:
   - miejsce lokalizacji;
   - węzły komunikacyjne;
   - otoczenie obiektu (strefa peryferyjna);
   - ogrodzenie obiektu;
   - drogi wewnętrzne;
   - miejsca parkingowe.
7. Powiązania z otoczeniem:
   - łączność przewodowa;
   - łączność bezprzewodowa;
   - inne urządzenia i środki zapewniające wymianę informacji;
   - dobór kadry do obsługi środków łączności.
8. Stan zabezpieczenia technicznego, w tym:
   - zabezpieczenie mechaniczne: drzwi; włazów, klap zapewniane przez: zamki i okucia, kraty, szyby, jak również środki przechowywania i transportu wartości pieniężnych oraz dokumentacji i inne środki mechanicznego zabezpieczenia;
   - techniczne środki kontroli ruchu osobowego i materiałowego;
   - techniczne środki nadzoru nad informacją i dokumentacją;
   - urządzenia i systemy alarmowe i sygnalizacji zagrożeń;
   - urządzenia i systemy przekazywania informacji o zagrożeniach do służb interwencyjnych i sztabów kryzysowych;
9. Stan zabezpieczenia fizycznego, w skład którego wchodzi stan przygotowania działań interwencyjnych, a szczególnie:
   - dokumentacja, w tym: rejestracja i archiwizacja zdarzeń; instrukcje; procedury w wypadku zagrożenia i kryzysów; plan szkoleń;
   - formy ochrony fizycznej;

- liczebność pracowników ochrony;
- wyposażenie i uzbrojenie pracowników ochrony;
- łączność pracowników ochrony;
- wyposażenie pracowników ochrony w środki transportu;
- wykształcenie i przygotowanie zawodowe;
- praktycznie sprawdzona szybkość reakcji pracowników ochrony na zagrożenia;
- powiązania z zewnętrznymi grupami interwencyjnymi.

10. Inne czynniki determinujące funkcjonowanie obiektu wynikające z:
    - unormowań prawnych,
    - porozumień międzynarodowych,
    - polityki zagranicznej państwa,
    - sojuszy międzypaństwowych,
    - ochrony środowiska itd.
11. Występujące zagrożenia:
    - kryminalne - wynikające z zagrożenia czynami przestępczymi, a w tym[12]: przeciwko bezpieczeństwu powszechnemu – niebezpieczeństwa katastrofy zagrażającej życiu lub zdrowiu ludzi albo mienia w znacznych rozmiarach, np: w postaci zawalenia się budowli, eksplozji materiałów łatwo palnych, gwałtownego wyzwolenia energii, substancji trujących, duszących lub parzących, szkodliwemu promieniowaniu, spowodowanie pożaru przez naruszenie przepisów pożarowych, uszkodzenie lub unieruchomienie urządzeń energii elektrycznej jako urządzeń użyteczności publicznej i innych;
    - czyny przeciwko życiu ludzkiemu: spowodowanie śmierci, uszkodzenie ciała przez pobicie, spowodowanie ciężkiego kalectwa, długotrwałej choroby, w tym także psychicznej i inne uszkodzenia ciała;
    - czyny przeciwko mieniu: zagarnięcie mienia społecznego o znacznej wartości, kradzież w sposób zorganizowany, zuchwała kradzież, kradzież z włamaniem, rozbójniczy zabór mienia, kradzież rozbójnicza, rozbój, wymuszanie rozbójnicze; niszczenie mienia, tj.: niszczenie, uszkodzenie lub uczynienie niezdatnym do użytku, w tym obiektu gospodarczego, urządzeń technicznych lub innego mienia w znacznych rozmiarach, powodując przez to istotne zakłócenie w działalności obiektu;

---

[12] Praca zbiorowa, *Zagrożenia przestępczością pospolitą.* Zeszyt 8, Przewodnik Rzeczoznawcy, Warszawa 1995.

- czyny przeciwko funkcjonariuszom publicznym, a w tym: czynna napaść w postaci podstawowej, kwalifikowanej, opór przeciwko czynności służbowej, znieważenie funkcjonariusza publicznego;
- czyny przeciwko tajemnicy państwowej i służbowej, np: ujawnienie tajemnicy państwowej i służbowej, w formie kwalifikowanej, naruszenie zarządzeń dotyczących tajemnicy państwowej i służbowej;
- środowiskowe - wszystkie zagrożenia wynikające z występujących na obszarze i w miejscu lokalizacji obiektu zagrożenia przyrodnicze, tj. powódź lub zalanie, pożar, tąpnięcia itd.;
- przemysłowe, wynikające z funkcji i działalności człowieka w pobliżu obiektów, zakładów przemysłowych, szlaków transportu czy też produkcji niebezpiecznych środków itd;

12. Kierunki i metody ewentualnej penetracji miejsc w otoczeniu obiektu lub jego strony zewnętrznej, przez które może wniknąć potencjalny intruz (zaprezentowanie często w formie graficznej);
13. Analiza „słabych" punktów ochrony w odniesieniu do elementów obiektu, z maksymalnym uszczegółowieniem i uwzględnieniem:
    - wszelkich elementów architektonicznych,
    - ciągów komunikacyjnych,
    - otworów,
    - innych elementów środowiskowych i przemysłowych sprzyjających zagrożeniom przestępczym;
14. Określenie poziomu ryzyka, tj.: kategorii zagrożonych wartości - na bazie dotychczas przeprowadzonej analizy kategorii zagrożenia obiektu i jego elementów (wg Polskiej Normy zakresie od Z1 do Z4):
    - wykonanie listy rankingowej zagrożeń, która jest efektem analizy słabych punktów;
    - dokonanie podziału obiektu oraz jego elementów na grupy ryzyka wystąpienia określonego rodzaju zagrożenia;
    - przedstawienie w zwięzłej formie okoliczności sprzyjających zagrożeniu.
15. Ograniczenia i wymagania dotyczące środków:

    a.) prawnych:

    - jakie akty prawne i w jakim zakresie ograniczają możliwości ochrony obiektu?

- jakie akty prawne wymuszają działania ochronne np. ustawa o ochronie mienia, tajemnicy państwowej, rozporządzenia branżowe, itd.?

b) normatywnych:

- jakie akty normatywne i w jakim zakresie ograniczają możliwości ochrony obiektu?
- jakie akty normatywne wymuszają działania ochronne np. Polska Norma, wymagania branżowe itd.?

c) organizacyjnych:

- jakie powiązania ograniczą lub utrudnią wprowadzenie systemu alarmowego i sygnalizacji zagrożeń, np. opór ośrodka decyzyjnego?
- jakie są zasady funkcjonowania służby ochrony obiektu?

d) technicznych:

- określenie klasy systemu alarmowego (wg PN od SA1 do SA4). Z punktu widzenia optymalizacji nakładów na środki technicznej ochrony nie wszystkie punkty obiektu muszą być jednakowo silnie wyposażone w systemy alarmowe,
- określenie klasy urządzeń zastosowanych w systemie (wg PN od A do C i S). Zastosowane urządzenia muszą odpowiadać jakościowo, funkcjonalnie i użytkowo poziomowi zagrożenia obiektu, stąd wynika klasyfikacja urządzeń stosowanych w systemach alarmowych
- czy są warunki techniczne do wdrożenia systemu alarmowego, np. istniejący stan ogrodzenia umożliwia zastosowanie systemu ochrony płotu;

e) ekonomicznych - czy zaproponowane nakłady finansowe są adekwatne do potrzeb wynikających z potrzeb neutralizacji zagrożeń przez zastosowanie systemu alarmowego i sygnalizacji zagrożeń;

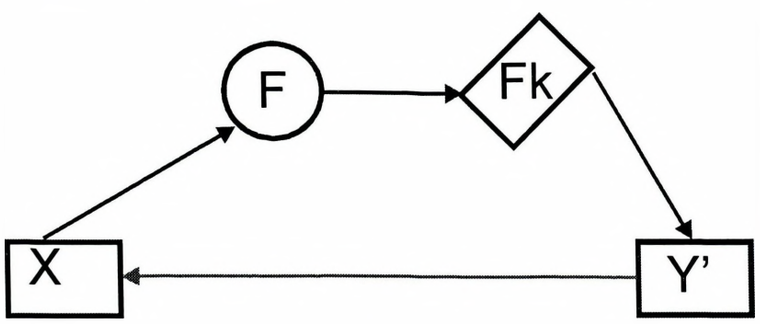
Przeprowadzona analiza pozwala na opracowanie projektu technicznego systemu alarmowego i sygnalizacji zagrożeń ochrony obiektu. Opracowanie projektu musi być zgodne z ogólnymi i szczegółowymi zasadami i normami w tym zakresie. Należy pamiętać, że taka dokumentacja ze względu na syntetyczny opis i analizę słabych punktów musi podlegać szczególnej ochronie, zgodnie z obowiązującymi w tym zakresie przepisami. W tworzeniu schematu powiązań czynników decydujących o doborze elementów systemu wykorzystano schemat badawczy analizy wartości procesów organizacyjnych.

Analiza wartości, jako system składający się z technik analizy funkcjonalnej, których podstawowym celem jest, w sposób systematyczny i zorganizowany, szczególne zwiększenie

sprawności w dziedzinie określania i rozwiązywania różnych problemów, z uwzględnieniem identyfikacji kosztów zbędnych.

Proces badawczy w zakresie powiązań rozpoczęto od zebrania, odpowiedniego przetworzenia i utrwalenia informacji. Informacje te nie są jednak tylko danymi charakteryzującymi badany system. Podstawową ich część stanowią dane z otoczenia obiektu, przede wszystkim od użytkownika obiektu. Informacje te odpowiednio przeanalizowane pozwolą na określenie funkcji badanego systemu ochrony obiektu. Uzyskany w ten sposób zbiór funkcji staje się od tego momentu przedmiotem badania. Zabieg ten pozwolił przejść na inny poziom uogólnienia, wyjść z obszaru konkretnych problemów (obiektów) do poziomu abstrakcji.

Powstały w ten sposób zbiór funkcji (czynników decydujących o doborze elementów systemu ochrony obiektu) został poddany badaniu. Sprowadzono go do sklasyfikowania funkcji oraz ich analizy. Rezultatem tych działań jest określenie tzw. zbioru funkcji koniecznych. Po jego ustaleniu nastąpiło ponowne przejście na następny poziom uogólnienia, gdzie nastąpił powrót od abstrakcji do konkretu. Przejście to polegało na takim zmaterializowaniu ustalonych funkcji koniecznych w systemie ochrony obiektu, aby wypełnić cel, jakim było określenie powiązań newralgicznych elementów systemu. Zbudowano w ten sposób bazę analityczną do modelu systemu ochrony obiektu. Schematycznie proces ten został przedstawiony na rysunku 4.1.1.1.

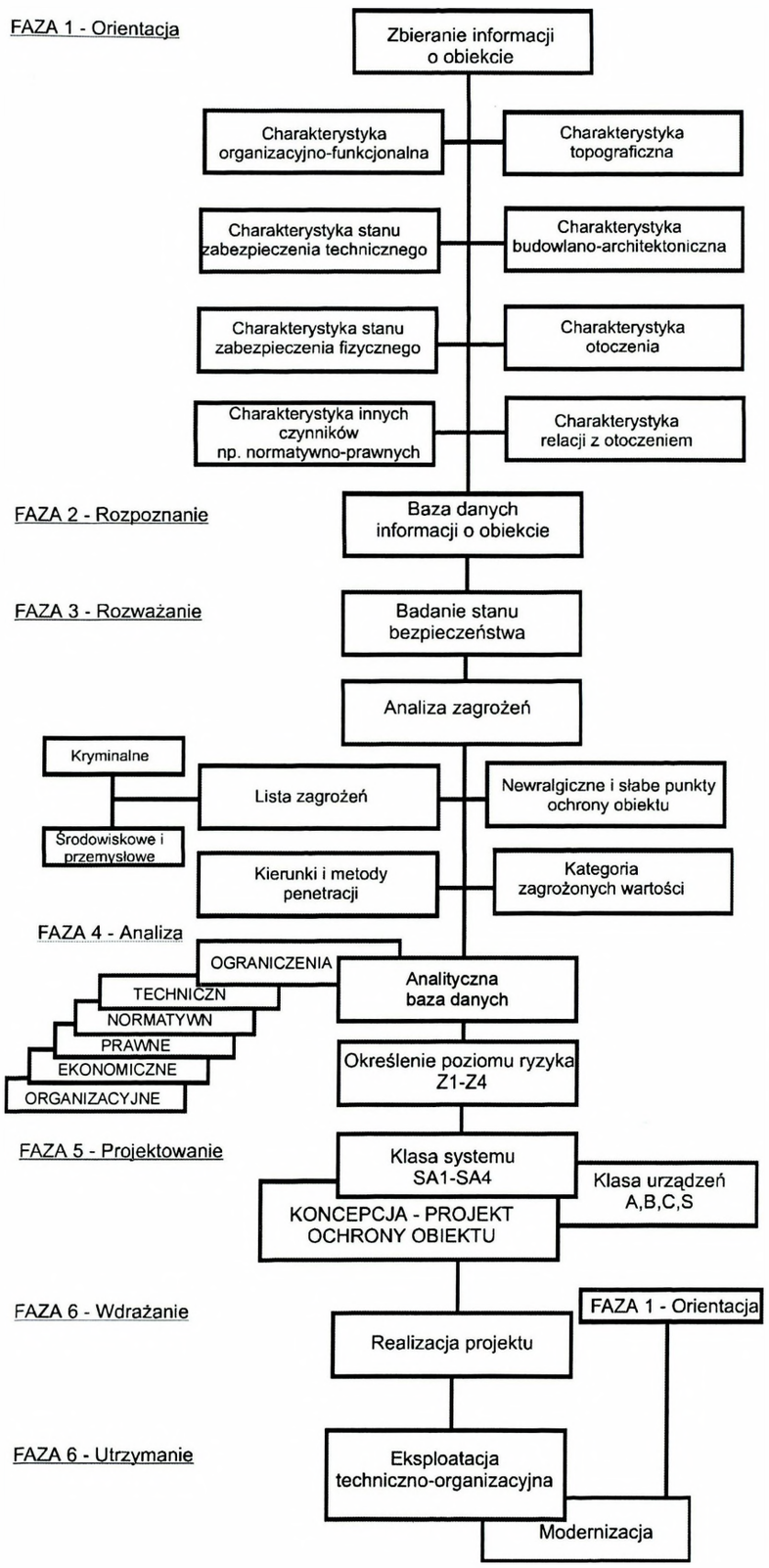


Rys.4.1.1.1.Schemat procesu ustalenia powiązań
za pomocą analizy wartości.

Na rysunku oznacza:

X - system istniejący (przedmiot badania) F - zbiór funkcji systemu istniejącego

Y' - system proponowany (cel badania) Fk - zbiór funkcji koniecznych

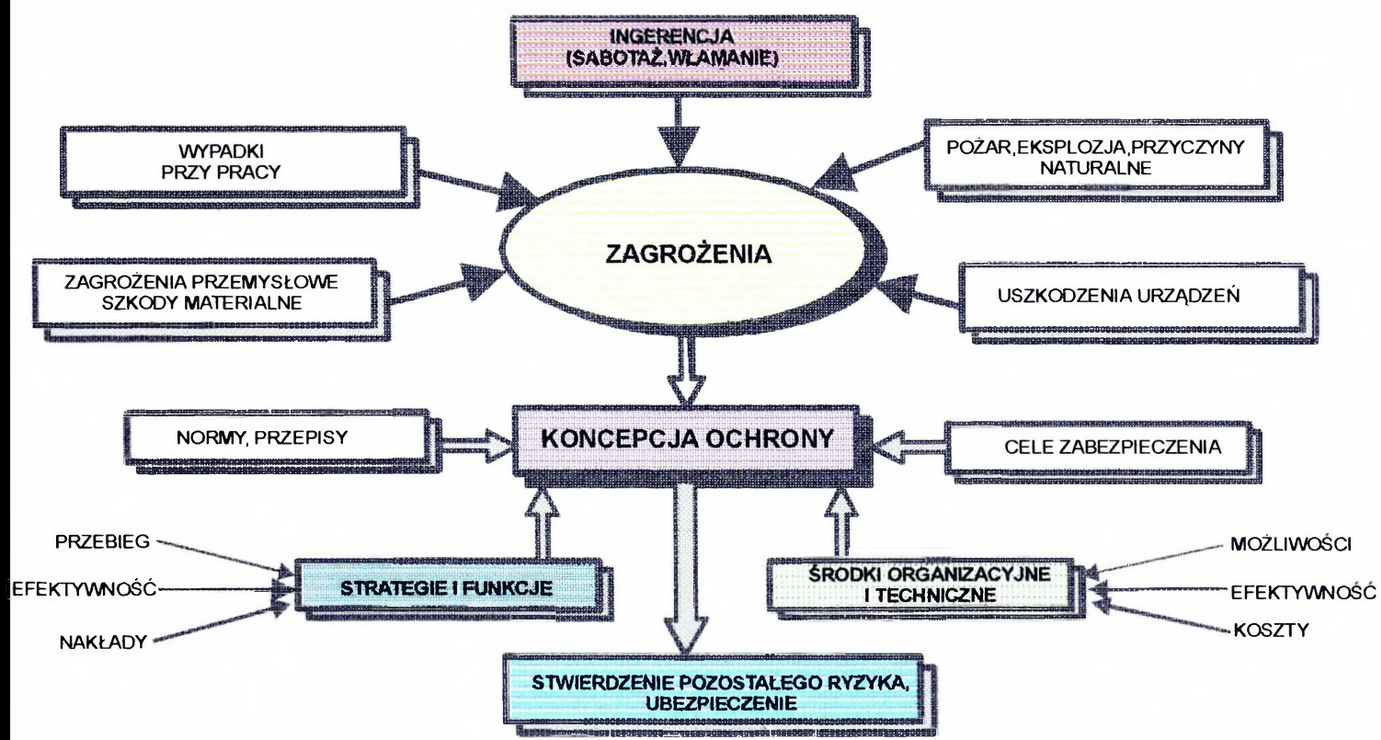


Rys.4.1.1.2. Czynniki decydujące o wyborze elementów systemu ochrony - schemat badawczy analizy wartości organizacji

Na rysunku 4.1.1.2.[13] zostały zaprezentowane czynniki, które są podstawą do opracowania szczegółowej metodologii tworzenia systemu ochrony obiektów.

4.1.2. Określenie stanu bezpieczeństwa obiektu

Rozdział ten został rozszerzony ze względu na podstawę oceny zastosowanego rozwiązania technicznego systemu ochrony obiektu wojskowego.[14]



RYS.4.1.2.1. CZYNNIKI WPŁYWAJĄCE NA KONCEPCJĘ ZABEZPIECZENIA OBIEKTU

Dokumentacja techniczna systemu alarmowego zasadniczo różni się od spotykanych innych dokumentacji branży elektrycznej, ponieważ zawiera rozdziały omawiające szczegółowo analizę słabych punktów obiektu pod względem włamaniowo - napadowym (np. analizę zagrożeń, kierunków penetracji intruza itd.). Brak takiej analizy zagrożeń w zasadzie powinien dyskwalifikować taką dokumentację. Może świadczyć o nieprofesjonalnym podejściu projektanta do problemu zabezpieczeń lub wręcz o nieznajomości tego zagadnienia. Należy z całą siłą podkreślić, że analiza zagrożeń jest punktem wyjścia do rozważań koncepcyjnych w każdej metodyce projektowania

[13] Opracowanie własne.
[14] A. Wójcik, *Wprowadzenie do projektowania systemów alarmowych sygnalizacji zagrożeń*, TECHOM, Warszawa 1996

systemów ochrony. Zagrożenia wynikają nie tylko z ingerencji osób trzecich, ale także z przyczyn naturalnych, złego funkcjonowania urządzeń i innych systemów alarmowych lub zagrożeń, np. przemysłowych, ekologicznych, promieniowania elektromagnetycznego, środowiskowe – powódź, szkody górnicze lub też niewłaściwe warunki BHP, które są przyczyną wypadków przy pracy. Na rysunku 4.1.2.1. zaprezentowano podstawowe czynniki kształtujące zagrożenia. Każdy z wymienionych czynników wymaga odrębnej analizy i podjęcia innych specyficznych sposobów ochrony, także podmiot jest chroniony, ze względu na swoją niekiedy niepowtarzalną specyfikę, inaczej w każdym konkretnym przypadku. Oczywiście istnieje pewna powtarzalność i kategoria stosowanych rozwiązań w określonych obiektach czy też miejscach ochrony, które wymagają pewnego "minimum" zabezpieczeń, wynikających z przepisów i wymagań np. magazyny broni, lecz ostateczne rozwiązanie zawarte w dokumentacji technicznej jest niepowtarzalne, wynikające ze szczegółowej analizy zagrożeń. Dokumentacja techniczna wskazuje "słabe punkty" ochrony mechanicznej obiektu (miejsca zagrożenia), wynikające z jego architektury i konstrukcji.

Największe zagrożenie w wypadku systemów alarmowych sygnalizacji włamania występuje przy otworach drzwiowych (ok. 40% przypadków włamań), oknach parterowych i piwnicznych, mniejsze (od 3-9%) w przypadku świetlików, balkonów itd.. Istotnym elementem analizy jest przedstawienie sposobu określania sygnałów (meldunków) o alarmie, monitorowanie sygnałów alarmu, sposobów reakcji na nie przez człowieka i cały system alarmowy oraz systemy współpracujące. Należy odpowiedzieć na następujące postawione pytania:

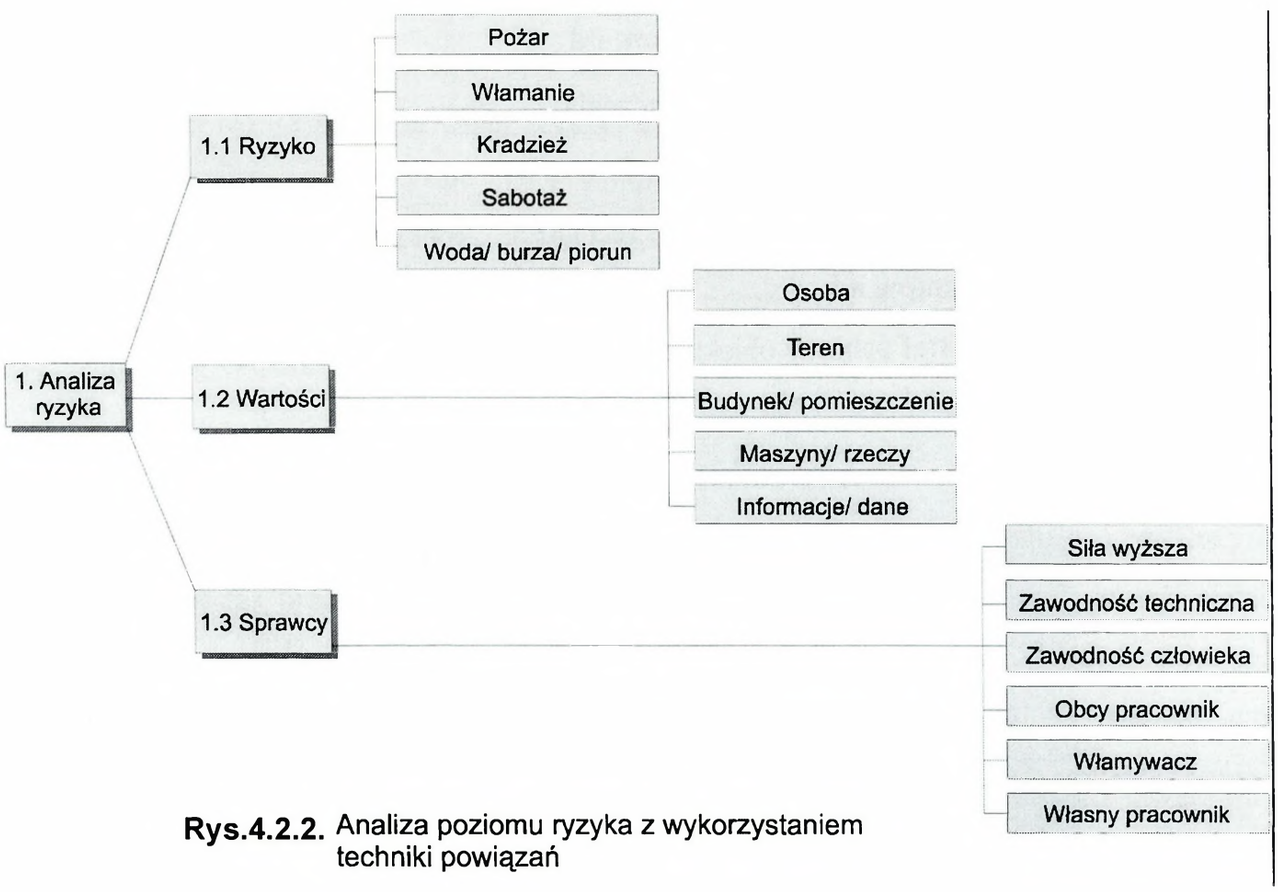
1. Czy alarm powinien być transmitowany dyskretnie do miejscowego centrum nadzoru mienia i po analizie potwierdzony przez obsługę i przekazany do centrum operacyjnego grupy interwencyjnej w przypadku stwierdzenia faktycznego zagrożenia?
2. Czy też techniczny system bezpieczeństwa powinien charakteryzować się pełną automatyzacją (samodzielnością), odczekać określony czas bez potwierdzenia i przekazać sygnał alarmu do zewnętrznego stanowiska nadzoru?

Odpowiedź na te pytania jest uzależniona od kategorii zagrożenia, klasy systemu alarmowego oraz nakładów przeznaczonych na realizację ochrony technicznej obiektu. Niekiedy należy zrezygnować z realizacji systemu alarmowego, w którym nie można spełnić wymagań normatywnych ochrony ze względów finansowych, ponieważ projektant odpowiada za opracowaną koncepcję ochrony i nie może jej ograniczać w przypadkach oczywistych, np. rezygnacji z obserwacji wizyjnej przed punktem przeładunkowym magazynu broni.

Prawidłowe określenie poziomu ryzyka[15] pozwala uniknąć w konsekwencji błędnego ustalenia środków neutralizujących zagrożenia. Prawidłowo dobrane środki techniczne i organizacyjne podnoszą skuteczność systemu alarmowania i sygnalizacji zagrożeń. Jednym z czynników określającym skuteczność jest czas reakcji konieczny na podjęcie interwencji celem neutralizacji zagrożenia oraz przestrzenno -czasowy zasięg działania systemu. Można to ująć w następującą formułą:

$$Trsa + Ttsa + Tpdi <= Tds + Tozmb$$

gdzie:
Trsa - czas reakcji systemu alarmowego (prewencja czasowa), rozpoznanie naruszenia strefy ochronionej;
Ttsa - czas transmisji sygnału o zagrożeniu od czujki do centrali alarmowej, analiza zagrożenia i transmisja wyniku obsłudze;
Tpdi - czas podjęcia działań interwencyjnych w celu neutralizacji zagrożenia;
Tds - czas działania sprawcy, niezbędny do realizacji jego zamiaru oraz oddalenia się od obiektu na bezpieczną odległość;
Tozmb - czas oporu systemu zabezpieczeń mechaniczno-budowlanych na działania sprawcy.



Rys.4.2.2. Analiza poziomu ryzyka z wykorzystaniem techniki powiązań

[15]opracowanie własne na podstawie Z.T. Nowicki, *Alarm o przestępstwie*, T N O i K „Dom Organizatora„ Toruń 1997.

Rysunek 4.1.2.2. przedstawia powiązanie podstawowych czynników mających wpływ na analizę ryzyka[16]. Analiza ryzyka jest istotnym zagadnieniem, które wpływa na ochronę obiektu pod względem doboru środków organizacyjnych i technicznych neutralizacji potencjalnych zagrożeń.

Ważnym elementem ochrony obiektów jest stosowanie ochrony strefowej. Taki sposób realizacji zabezpieczenia w sposób zasadniczy podnosi niezawodność systemu ochrony (alarmowego), powiększa strefę prewencyjnej ochrony, utrudnia wniknięcie potencjalnemu intruzowi, a jednocześnie wydłuża czas przeznaczony na interwencję służb ochrony.

Zasadniczo wyróżnia się cztery podstawowe strefy ochrony:

- strefa ochrony obwodowej - najdalej wysunięta strefa ochrony, obejmująca najczęściej obwód ogrodzenia;
- strefa ochrony zewnętrznej - chroniona przestrzeń na zewnątrz obiektu pomiędzy strefą obwodową a obiektem chronionym;
- strefa ochrony obwodowej obiektu - obejmuje obwód architektoniczny chronionego obiektu z otworami typu drzwi, okna, włazy, itd.;
- strefa ochrony przestrzennej pomieszczenia - obejmuje ochronę pomieszczenia realizowaną za pomocą czujek ruchu;
- strefa ochrony miejscowej - ochrona techniczna konkretnych urządzeń, np. kas pancernych, dokumentów itd..

Graficzna prezentacja stref ochrony obiektu została przedstawiona na rysunku 4.1.2.3.



Rys.4.1.2.3.Podział stref ochrony obiektu (wariant)

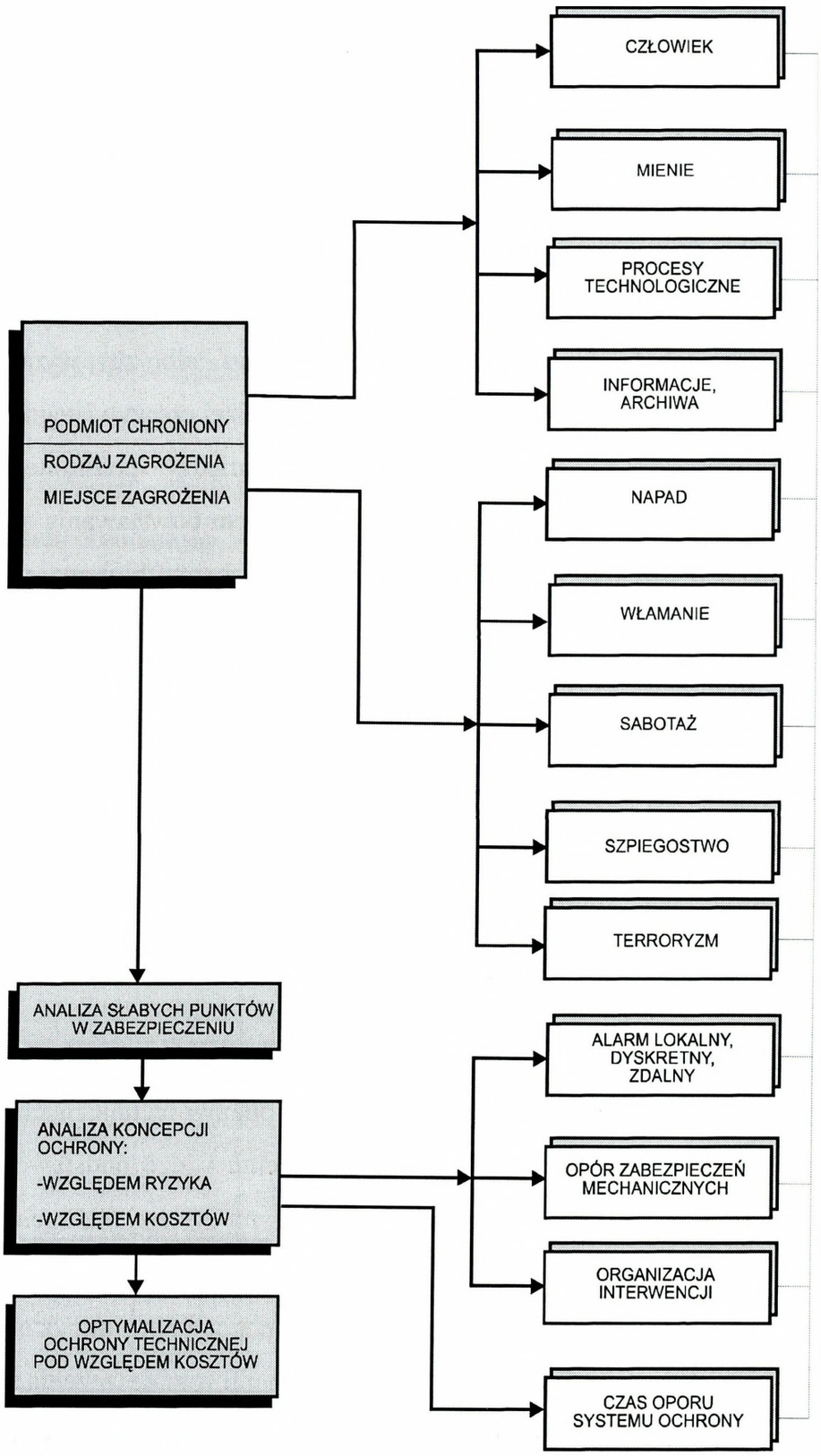
[6] Opracowanie własne.

Jeżeli już wyznaczone są cele ochrony oraz dobrana i sprawdzona baza normatywno-prawna, za pomocą optymalnych środków organizacyjno- technicznych można zabezpieczyć obiekt.

Projektant powinien zdawać sobie sprawę z tego, że jego koncepcja nie jest nigdy idealnym rozwiązaniem, szczególnie gdy istnieje zawsze pewne ryzyko i prawdopodobieństwo przełamania czy też niezadziałania systemu przez ograniczenia nakładów na ochronę. Projektant powinien to uświadomić odbiorcy i zaproponować dodatkowe ubezpieczenie prawne i możliwość rozbudowy systemu. Punktem krytycznym w opracowywaniu modelu ochrony jest właściwe zakwalifikowanie obiektu do klasy zagrożeń i tym samym klasy systemu zabezpieczeń. Konsekwencją tego może być dobranie nieodpowiednich urządzeń sygnalizacji alarmu - albo zbyt wymagających technicznie i tym samym zbyt drogich albo obniżenie klasy systemu poniżej rzeczywistego zagrożenia.

Rysunek 4.1.2.4 określa powiązania pomiędzy podmiotem chronionym, rodzajem zagrożenia, któremu podlega ten podmiot oraz miejscem powstawania zagrożenia, ale także określa analizę koncepcji pod względem ryzyka i kosztów. Schemat blokowy uwzględnia czas interwencji w zależności od typu zastosowanego alarmowania (monitoringu). Należy podkreślić, że wymienione przypadki są nieprawidłowe, ponieważ świadczą o niekompetencji projektanta. W pierwszym przypadku nie powinno być stosowana zasada "asekuracji", przez co podwyższa się klasę systemu, a tym samym zwiększa w sposób nieuzasadniony koszty instalacji systemu ochrony. Decyzja o kategorii ryzyka powinna wynikać tylko i wyłącznie z prawidłowo przeprowadzonej analizy zagrożeń, a w razie wątpliwości zawsze można potwierdzić lub zweryfikować ocenę opinią rzeczoznawcy czy uznanego eksperta.

Schematy organizacyjne i funkcjonalne systemu stanowią odzwierciedlenie przebiegu rozumowania w doborze właściwych środków zabezpieczenia. Jednocześnie są elementem pośrednim, uogólniającym pomiędzy szczegółami planów technicznych i połączeń poszczególnych urządzeń, Pozwalają przedstawić organizację systemu i jego podstawowe funkcje, np. podział na strefy dozoru, priorytety dostępu, współpracę z innymi systemami, spełnianie dodatkowych funkcji. Brak schematów organizacyjnych i funkcjonalnych systemu w poważnym stopniu utrudnia zrozumienie zasad całego systemu, powiązanie funkcjonalne urządzeń, przyporządkowanie linii. Schematy organizacyjne są ściśle powiązane z planami rozmieszczenia urządzeń, tj. czujek, central, manipulatorów szyfrowych, kamer, przełączników wizji itd. Pozwala to na adekwatnie do kategorii zagrożenia i klasy systemu sprawdzenie prawidłowości rozmieszczenia urządzeń pod względem zabezpieczenia przed zagrożeniem, np. czy układ czujek tworzy podwójną strefę ochronną.



RYS.4.1.2.4.CZYNNIKI KSZTAŁTUJĄCE STAN ZAGROŻENIA OBIEKTU CHRONIONEGO

4.2. Modelowanie systemu ochrony obiektu

Do opracowania modelu systemu sygnalizacji zagrożeń i alarmowania wykorzystano schemat struktury systemu, tj. zbioru relacji zachodzących między elementami oraz funkcjonowanie kompletnego systemu ochrony; zachowanie się jego podczas analizy jako całości na tle warunków wewnętrznych i zewnętrznych.

W opracowaniu modelu zaprezentowano formę graficzną jego odwzorowania dlatego, że jest szeroko stosowany nie tylko w projektowaniu technicznym, ale również w organizacji i zarządzaniu oraz posiada wysokie walory komunikowania i instruowania użytkownika a to także jest między innymi celem praktycznym.

Model systemu sygnalizacji zagrożeń i alarmowania (ochrony obiektu wojskowego) uwzględnia dynamicznie zmieniające się warunki jego tworzenia i wdrażania w czasie.

Zaprezentowany model należy do grupy modeli analityczno-graficznych, których zadaniem jest zilustrowanie za pomocą prostych metod rozwiązania problemu w sposób nieskomplikowany i przejrzysty.

Ponadto metoda analityczno-graficzna umożliwiła:

- przeprowadzenie analizy i odzwierciedlenie rzeczywistych przebiegów materialnych i informacyjnych,
- dokonanie symulacji i oceny wariantów organizacyjnych, przebiegów oraz ich powiązań.

Każdy z modułów zaprezentowanych w modelu można niezależnie rozbudować na elementy szczegółowe, uwzględniające zmienne warunki i powiązania. Do każdego z podstawowych modułów można dołączyć procedury rozszerzające modelu. Ostateczny kształt modelu zależy jest od użytkownika i konkretnych zastosowań.

Model jest niezależny od jakichkolwiek parametrów subiektywnych, które mogą ograniczyć jego stosowanie np. konkretna technologia, rozwiązanie techniczne czy też konkretnie rozpatrywany obiekt.

Procedura budowy modelu jest uniwersalna zarówno przy rozpatrywaniu obiektów pod względem urbanistycznym i architektonicznym np. jako skupionych, jak i rozległych rozrzuconych na dużej powierzchni wieloelementowych obiektów, które w sensie rozpatrywania i analizy oraz wzajemnych powiązań rozpatrywane są jako jeden obiekt.

Model umożliwia nie tylko budowę prawidłowego systemu sygnalizacji i alarmowania (ochrony), ale także sprawdzenie i weryfikację już istniejących systemów ochrony.

Przez opracowanie modelu zmniejsza się ryzyko popełnienia błędu oraz nieobiektywnej (subiektywnej) oceny systemu sygnalizacji zagrożeń i alarmowania.

Model uwzględnia, pomijaną w większości opracowań, optymalizację kosztów oraz ograniczenia wynikające z rachunku kosztów. Jednocześnie zaprogramowane nakłady na wykonanie systemu nie ograniczają późniejszej docelowej rozbudowy systemu ochrony obiektu. Stosowanie modelu w sposób zasadniczy powinno zmniejszyć koszty opracowania lub oceny systemu sygnalizacji i alarmowania dla obiektów.[17]

Prezentowana metodologia tworzenia modelu sygnalizacji i alarmowania o zagrożeniach została podzielona na kilka faz, które występują podczas jego budowy. Pozwala to prowadzić fazową budowę modelu i jednocześnie kontrolę realizacji poszczególnych etapów.

Autor uznał, że zakończenie procedur nie kończy się na teoretycznym opracowaniu modelu sygnalizacji i alarmowania (ochrony obiektu), ale konieczne jest także zaprezentowanie jego wdrożenia do eksploatacji oraz nadzór nad jego realizacją.

Konsekwencją takiego rozumowania jest przyjęcie założenia, że eksploatowany model będzie podlegał czynnikom zmieniającym jego funkcjonowanie i skuteczność w czasie.

Przedstawiony w pracy model uwzględnia prowadzoną, w przyjętych odstępach czasu modernizację modelu sygnalizacji i alarmowania

Model systemu sygnalizacji i alarmowania obejmuje następujące podstawowe części:

1. Analizę zagrożeń.
2. Środki neutralizacji zagrożeń.
3. Model systemu sygnalizacji i alarmowania (ochrony obiektu).
4. Weryfikację modelu.
5. Realizację modelu.
6. Modernizację modelu.

Poszczególne etapy tworzenia modelu systemu ochrony obiektu (sygnalizacji i alarmowania o zagrożeniach) podzielono na następujące fazy:

- Opis obiektu.
- Analiza zagrożeń.
- Środki neutralizacji zagrożeń.
- Ochrona techniczna i fizyczna obiektu.
- Systemy techniczne i organizacyjne.

- Koncepcja modelu systemu sygnalizacji i alarmowania
- Weryfikacja modelu.
- Ocena pozostałego ryzyka.
- Model systemu sygnalizacji i alarmowania.
- Planowanie realizacji modelu.
- Realizacja modelu systemu sygnalizacji i alarmowania.
- Odbiór modelu systemu sygnalizacji i alarmowania.
- Eksploatacja modelu systemu sygnalizacji i alarmowania.
- Modernizacja modelu systemu sygnalizacji i alarmowania.

Model został zbudowany jako kombinacja określonego typu wzorca i odzwierciedlenie istniejącego stanu. Zamierzeniem autora jest odwzorowanie rzeczywistego stanu ochrony obiektu, z ukierunkowaniem na identyfikację zakłóceń i odchyleń podczas rzeczywistego jego funkcjonowania. Celowość stosowania takiego rozwiązania uzasadniona jest stopniem złożoności badanego obiektu i wynikającymi z tego tytułu kosztami.

W pierwszym etapie ustalono bazę danych ochrony obiektu uznaną za normę oraz badano zakłócenia i błędy, w dalszym działaniu usunięto przyczyny odchyleń od normy.

Analiza zagrożeń i diagnoza stanu powiązań czynników decydujących o stanie ochrony obiektu odgrywała istotną rolę przy tworzenia modelu systemu sygnalizacji zagrożeń i alarmowego (ochrony obiektu wojskowego).

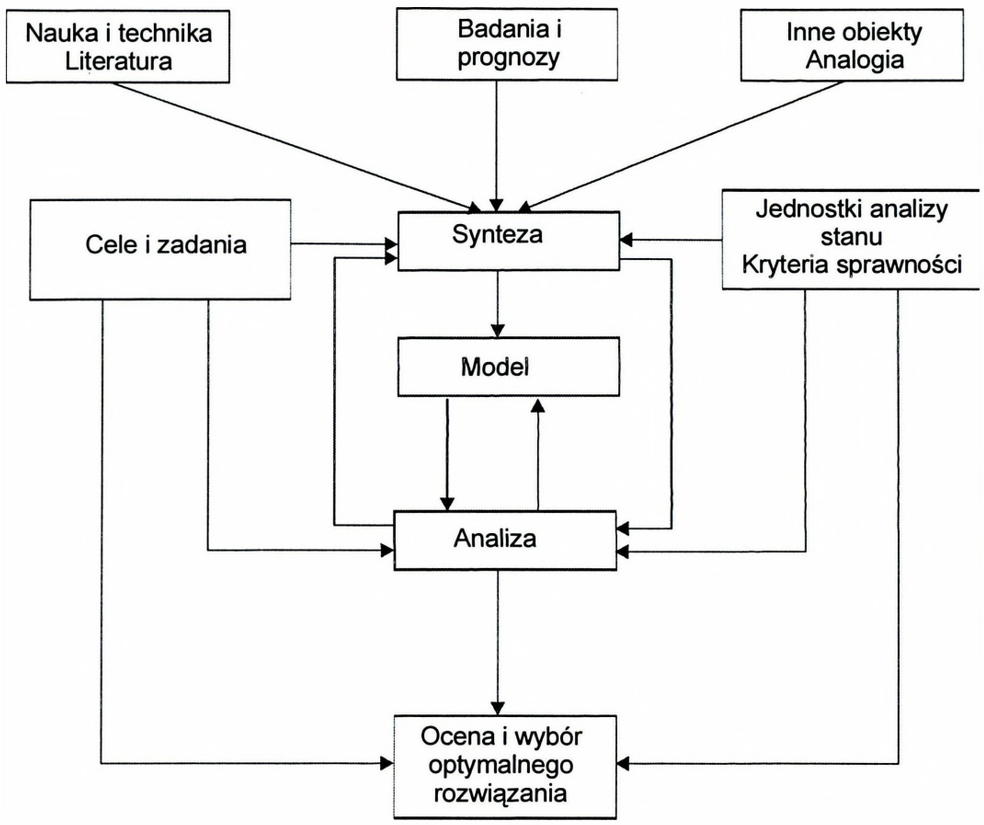
Na rysunku 4.2.a. przedstawiona została organizacja budowy modelu.

W celu oderwania się od dotychczas stosowanych rozwiązań i umożliwienia wprowadzenia innowacyjnych rozwiązań organizacyjnych zastosowano model wzorca. Model ten nie jest odzwierciedleniem konkretnego obiektu (systemu), lecz konstruowany został jako rozwiązanie rozwojowe, rezultat twórczego myślenia, badania tendencji rozwojowych, co umożliwi jego rozwój w przyszłości.

Na rysunku 4.2.b. przedstawiono konstrukcję i wykorzystanie modelu jako wzorca.[18]

---

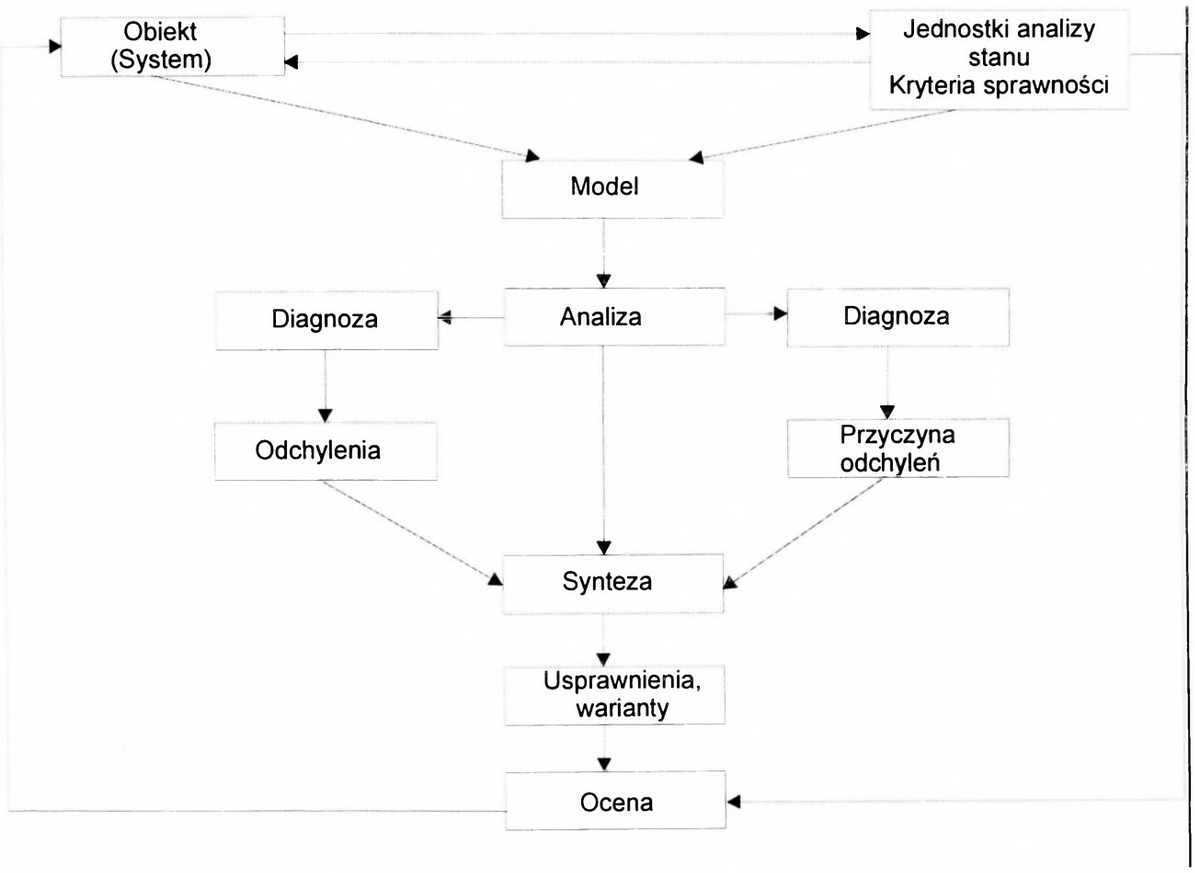
[17] Opracowanie własne.
[18] A.Stabryła i inni, *Organizacja i zarządzanie. Zarys problematyki*, PWN, Warszawa 1986.



Rys. 4.2.a. Organizacja budowy modelu (wariant)

Taka organizacja budowy modelu pozwoliła oderwać się od rozwiązań tradycyjnych i wdrożyć nowoczesne rozwiązania projektowe w modelowaniu systemów ochrony obiektów wojskowych.

Przedstawione metody organizacji i konstrukcji modelu prezentują dwa różne sposoby rozwiązania tego problemu. W rozwiązaniu przedstawionym na rysunku 4.2.a. wykorzystywana jest baza danych w postaci ogólnej wiedzy i naukowych metod postępowania. Taki sposób opracowywania jest przydatny przy budowie modelu od podstaw. W wariancie przedstawionym na rysunku 4.2.b. model opracowywany jest w przypadku modyfikacji już istniejącego modelu lub konkretnego obiektu analizy.

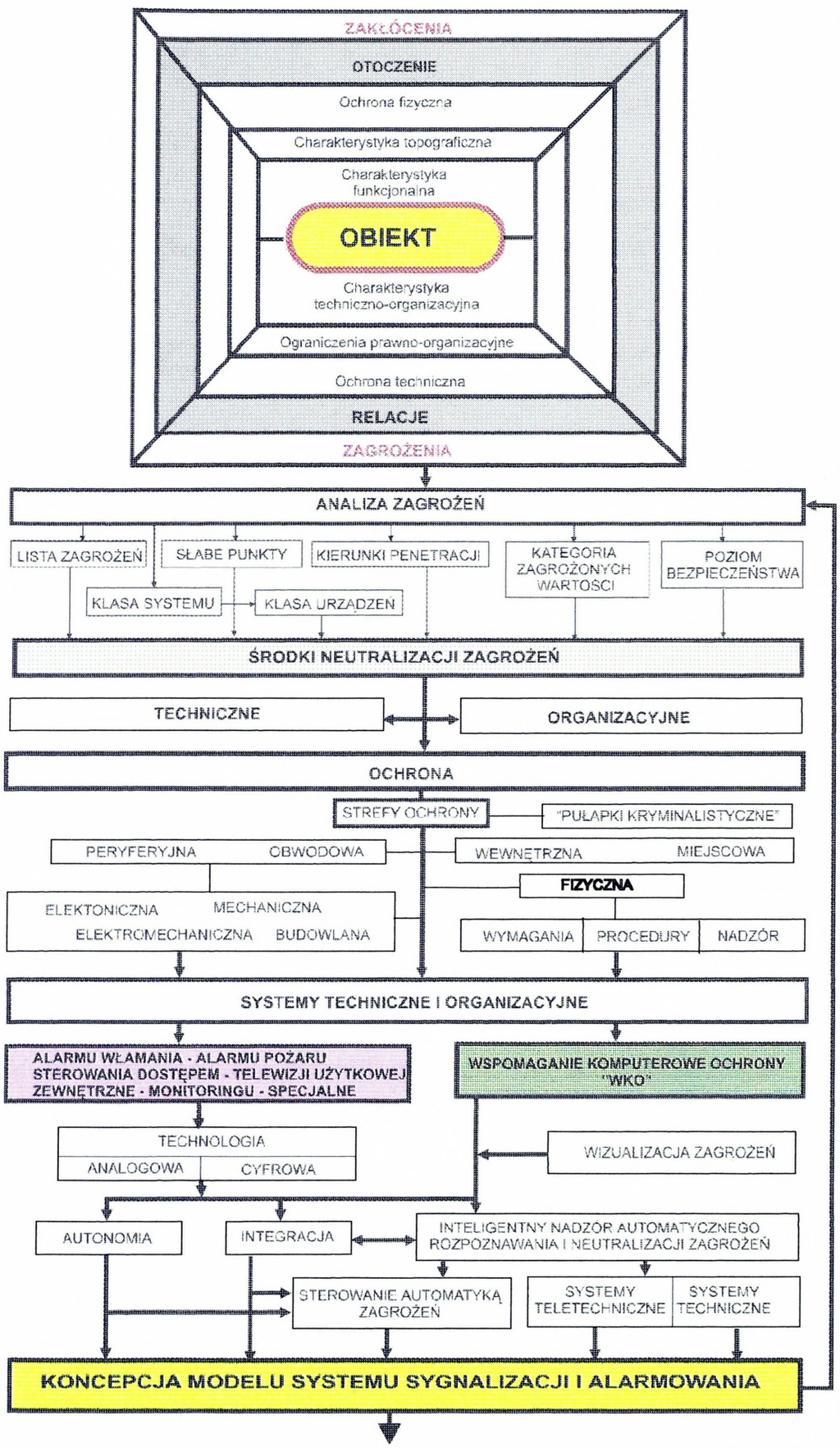


Rys. 4.2.b. Konstrukcja i wykorzystanie modelu jako obrazu (wariant)

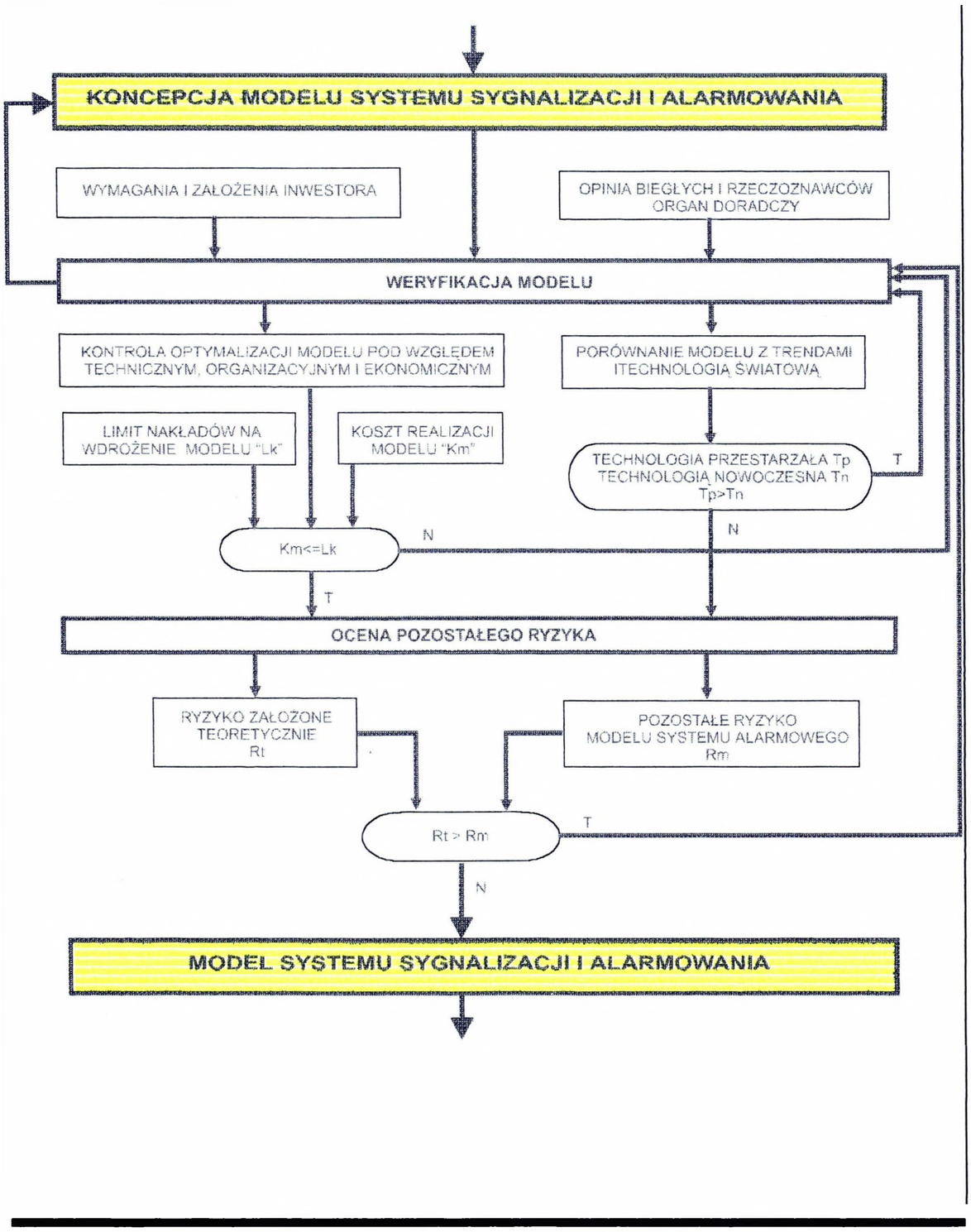
Konstruowanie i wykorzystywanie modelu jako wzorca zostały sprowadzone i wykorzystane do ulepszenia oraz poprawienia stanu istniejącego systemu ochrony obiektu.

Na schematach 4.2.1, 4.2.2, 4.2.3 zamieszczono graficzną prezentację algorytmu opracowanej metodologii, która przedstawia ciąg procedur niezbędnych do budowy modelu systemu alarmowego i sygnalizacji zagrożeń oraz wyjaśnia strukturę poszczególnych modułów i powiązania elementów modelu w prezentowanej metodologii.[19]

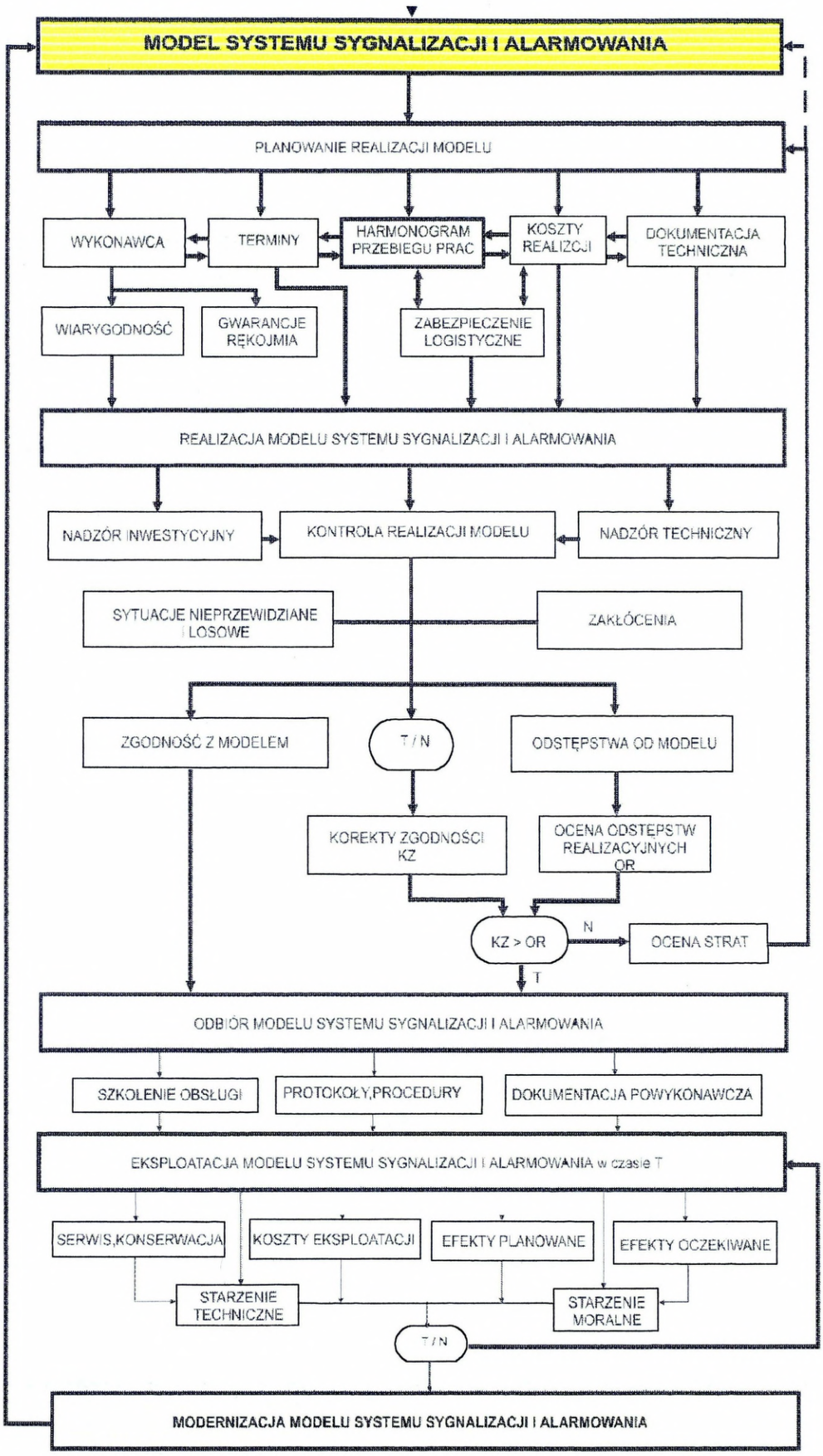
[19] Opracowanie własne.



Schemat 4.2.1.Metodologia tworzenia modelu systemu ochrony obiektu cz.1.



Schemat 4.2.2. Metodologia tworzenia modelu systemu ochrony obiektu cz.2..



Schemat 4.2.3. Metodologia tworzenia modelu systemu ochrony obiektu cz.3.

Model systemu ochrony obiektu wojskowego na potrzeby obronności państwa

Do opracowania modelu systemu alarmowania i sygnalizacji zagrożeniach wykorzystano metodologię tworzenia modelu systemu alarmowego opisaną w rozdziale 4.2. i przedstawioną na rysunkach 4.2.1., 4.2.2., 4.2.3.

W modelu ujęte są wszystkie niezbędne do budowy czynniki i uwarunkowania oraz wzajemne powiązania jego elementów z otoczeniem, tj. czynniki topograficzne i organizacyjne obiektu, analiza oraz kategoria zagrożenia obiektu, środki neutralizacji zagrożenia.

W opracowaniu modelu wykorzystałem formę graficzną odwzorowania modelu, ponieważ jest szeroko stosowana w projektowaniu technicznym oraz organizacji i zarządzaniu i posiada wysokie walory komunikowania i instruowania, co stanowi główny praktyczny cel prezentowanego modelu.

Model systemu sygnalizacji i alarmowania uwzględnia dynamicznie zmieniające się warunki jego tworzenia i wdrażania.

Zaprezentowany model należy do grupy analityczno-graficznych, których zadaniem jest za pomocą prostych metod zilustrowanie rozwiązania problemu w sposób nieskomplikowany i przejrzysty. Model jest niezależny od jakichkolwiek parametrów subiektywnych, które mogą ograniczyć jego stosowanie, np. konkretna technologia, rozwiązanie techniczne czy też konkretnie rozpatrywany obiekt.

Budowa modelu jest uniwersalna zarówno przy rozpatrywaniu obiektów pod względem organizacyjnym, technicznym, urbanistycznym, jak i architektonicznym. Takie same zasady obowiązują dla obiektów wojskowych skupionych, jak i rozległych, rozrzuconych na dużej powierzchni wielu obiektów, które w sensie rozpatrywania i analizy oraz wzajemnych powiązań rozpatrywane są jako jeden obiekt.

Opracowany model umożliwia nie tylko budowę prawidłowego systemu sygnalizacji i alarmowania, ale także sprawdzenie i weryfikację już funkcjonujących. Stosowanie modelu zmniejsza się ryzyko popełnienia błędu oraz nieobiektywnej (subiektywnej) oceny systemu sygnalizacji i alarmowania.

W modelu uwzględniono, pomijaną w większości opracowań, optymalizację kosztów oraz ograniczenia wynikające z rachunku kosztów, poprzez ochronę tylko niezbędnych pomieszczeń.

Jednocześnie zaprogramowane nakłady na wykonanie systemu nie ograniczają późniejszej docelowej rozbudowy systemu sygnalizacji i alarmowania.

Modelowanie w sposób zasadniczy powinno zmniejszyć koszty opracowania lub oceny systemu sygnalizacji i alarmowania obiektów wojskowych.

Model graficzny posiada rozwinięcie w postaci szczegółów dotyczących rodzaju stref ochrony i typów zabezpieczenia obiektu wojskowego. Od zaprezentowanej rozwiniętej formy ochrony na rys.4.2.4 można prześledzić szczegół „A„, ujmujący formy zabezpieczenia zewnętrznego po obwodzie obiektu.[20]

Szczegół „B„ przedstawia modelowy sposób zabezpieczenia stref wewnętrznych obiektu wojskowego. Konstruowanie i wykorzystywanie modelu jako obrazu sprowadzono do ulepszenia i poprawienia stanu istniejącego systemu ochrony obiektu.

Na model systemu ochrony obiektu składa się:

1. Rysunek 4.2.4. przedstawiający kombinację możliwości ochrony elektronicznej obiektu wojskowego z wyszczególnieniem stref ochrony:
2. Rys.4.2.4.a. określający szczegół „A„ - rodzaje ochrony zewnętrznej obiektu wojskowego.
3. Rys.4.2.4.b. informujący o rozplanowaniu strefy ochrony wewnętrznej – szczegół „B"- w modelu systemu ochrony.
4. Rys.4.2.5. przykładowy model przestrzenny systemu ochrony.

- Jeden z wariantów klasyfikacji stopnia zagrożenia obiektu dzieli je na:
- Niski stopień zagrożenia. Ochrona obiektu realizowana jest za pomocą: systemu wizyjnego, systemu ogrodzeniowego.
- Średni stopień zagrożenia. Ochrona obiektu wykonywana jest za pomocą: systemu wizyjnego, systemu barier podczerwieni aktywnej.
- Średni stopień zagrożenia. Obiekt chroniony jest za pomocą: systemu wizyjnego, systemu kabla elektromagnetycznego.
- Wysoki stopień zagrożenia. Ochrona obiektu zbudowana jest za pomocą: systemu wizyjnego; systemu barier mikrofalowych; systemu ogrodzeniowego.
- Bardzo wysoki stopień zagrożenia. Ochrona obiektu realizowana za pomocą: systemu wizyjnego; systemu podwójnych barier mikrofalowych; systemu ogrodzeniowego.

[20] Opracowanie własne.

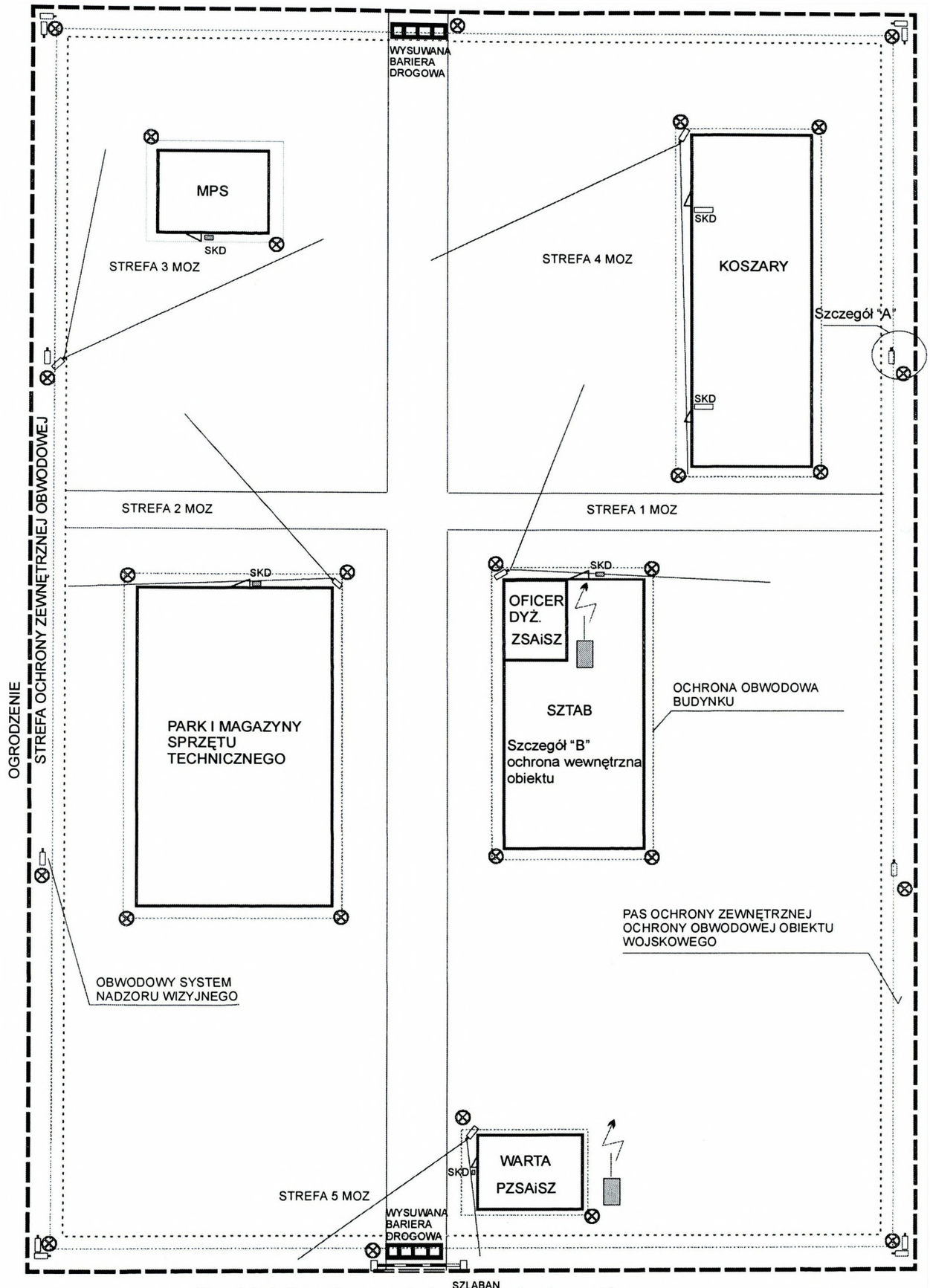
Prezentowany model sygnalizacji i alarmowania o zagrożeniach został podzielony na kilka części, które występują podczas jego budowy. Pozwala to prowadzić fazową budowę modelu i jednocześnie prowadzić kontrolę realizacji poszczególnych etapów.

Model, wraz z opracowaną metodologią, umożliwia praktyczne wdrożenie opracowanego modelu do eksploatacji oraz nadzór nad jego realizacją.

Konsekwencją takiego rozumowania jest przyjęcie założenia, że eksploatowany model będzie podlegał czynnikom zmieniającym jego funkcjonowanie i skuteczność w czasie.

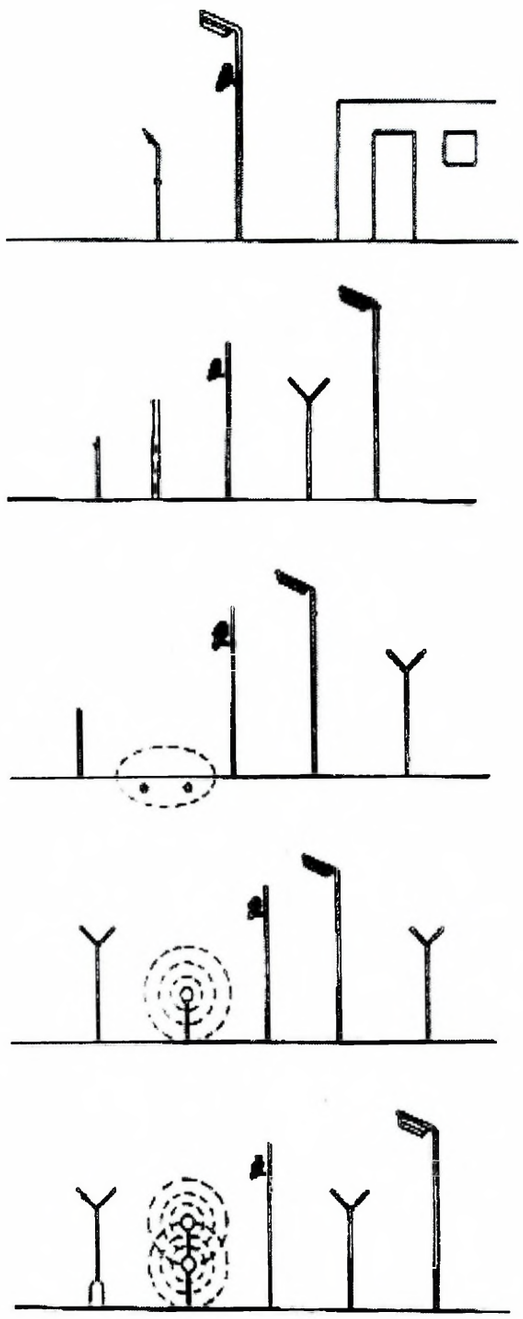
Przedstawiony w pracy model uwzględnia prowadzoną, w przyjętych odstępach czasu jego modernizację.

Zamierzeniem autora było odwzorowanie rzeczywistego stanu ochrony obiektu, z ukierunkowaniem na identyfikację zakłóceń i odchyleń w funkcjonowaniu rzeczywistego obiektu (systemu). Celowość stosowania takiego rozwiązania uzasadniona jest stopniem skomplikowania badanego obiektu i wynikającymi z tego tytułu kosztami.



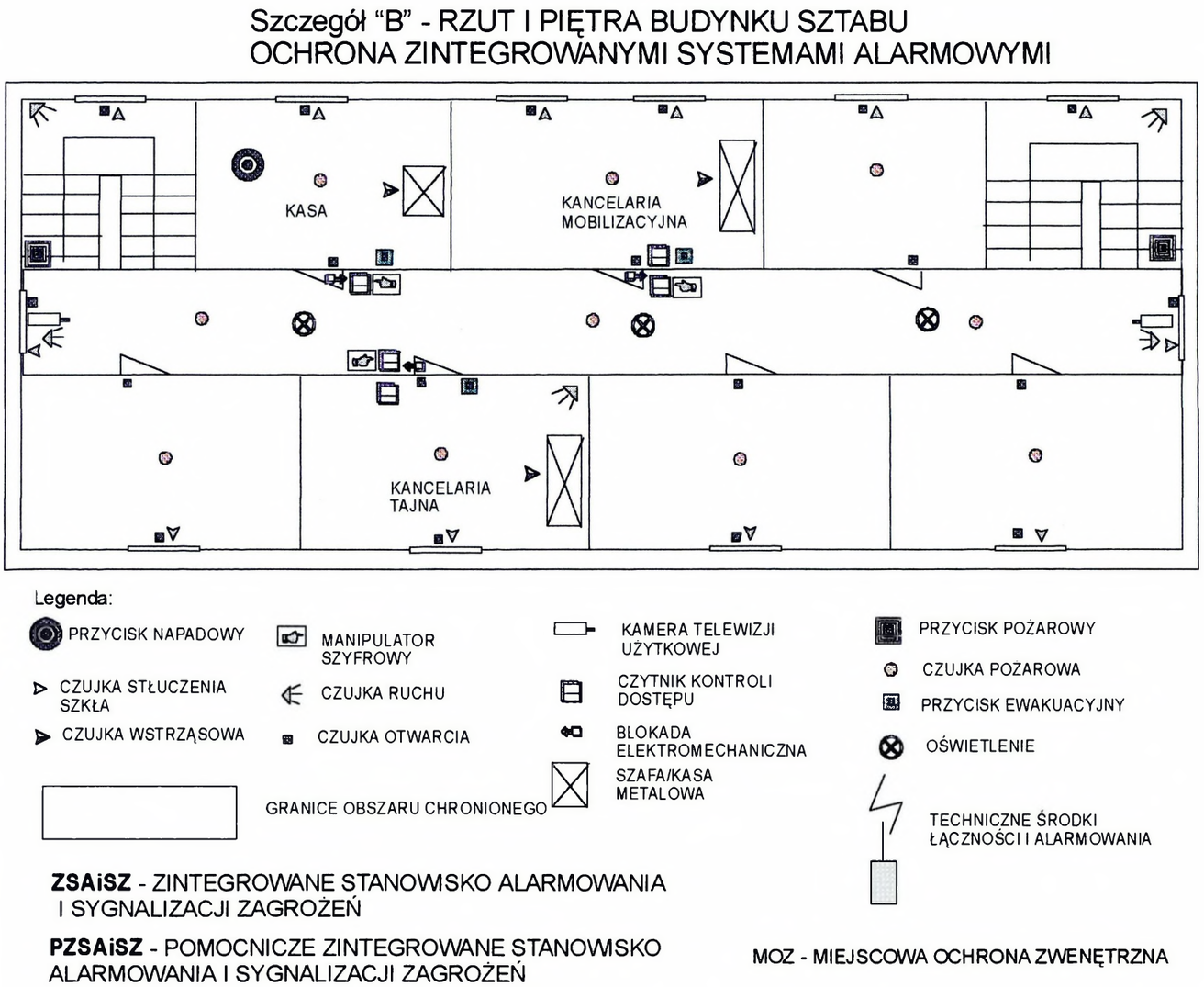
Rys.4.2.4. Rozmieszczenie i powiązanie elementów modelu systemu ochrony obiektu wojskowego (wariant)

Legenda: na rys. 4.2.4.b.



Rys.4.2.4.a. Szczegół „A“ - rodzaje ochrony zewnętrznej obiektu wojskowego (wariant)[1]

[1] A. Wójcik, referat *Wybrane elementy ochrony obiektów wojskowych za pomocą systemów alarmowych i sygnalizacji zagrożeń*", Konferencja Naukowa "Urządzenia i systemy łączności na potrzeby kierowania obronnością i bezpieczeństwem państwa", Akademia Obrony Narodowej, Warszawa, 1996.



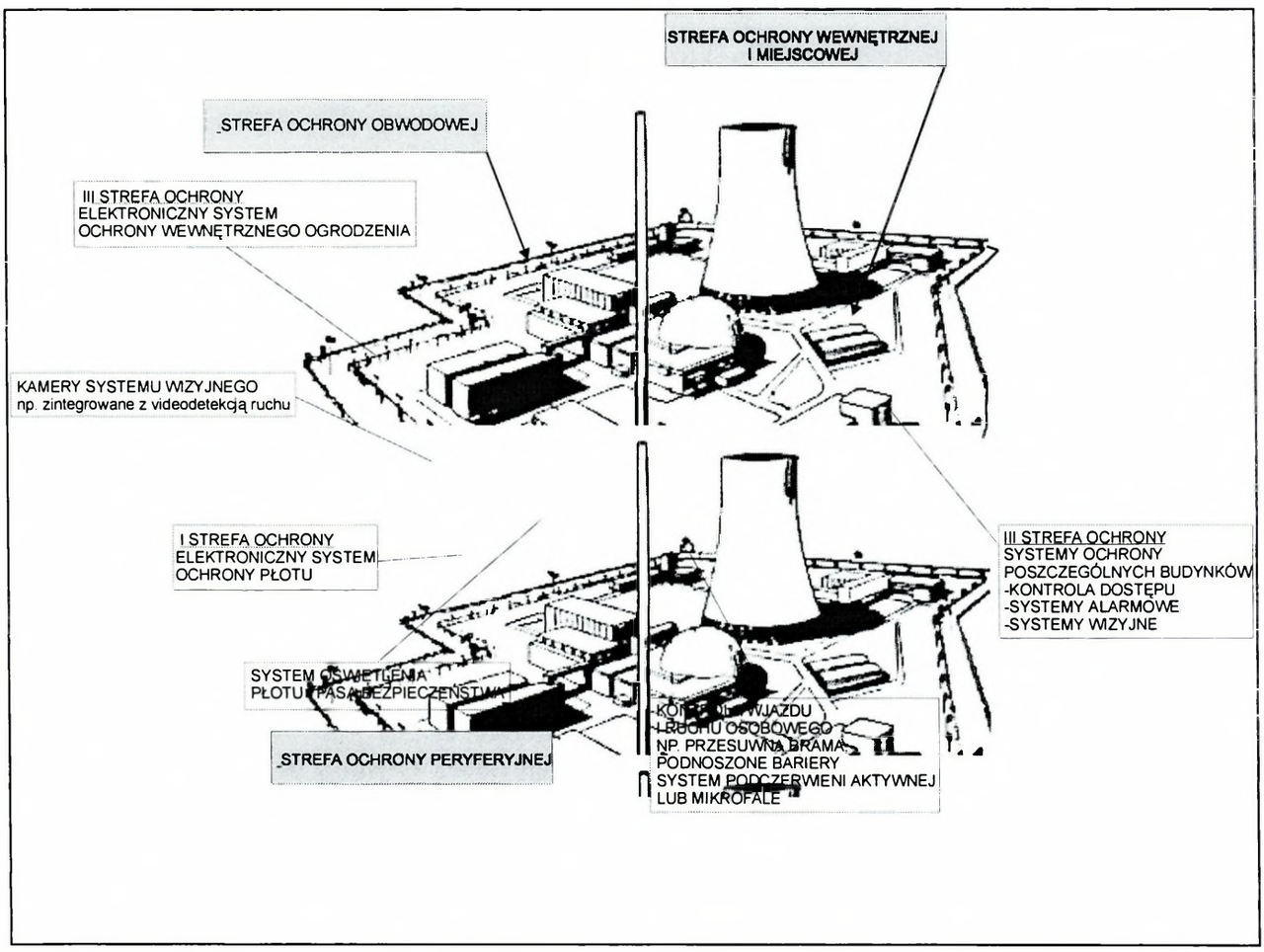
Rys.4.2.4.b. .Prezentacja strefy ochrony wewnętrznej w modelu systemu ochrony obiektu wojskowego (wariant) z rys. 4.2.4. – szczegół „B"[2]

Ochrona wewnętrzna stanowi ochronę poszczególnych budynków wraz ze sterowaniem dostępem osób uprawnionych. Wewnątrz obiektu chronione są węzły komunikacyjne oraz wytypowane, ważne ze względów funkcjonalnych i organizacyjnych, pomieszczenia. Została zastosowana kompleksowa ochrona przed włamaniem i napadem, pożarem itp. Występuje kontrola wchodzących i wychodzących osób do wybranych pomieszczeń wraz z rejestracją zaistniałych zdarzeń. Obiekt nadzorowany jest za pomocą systemu wizyjnego z ciągłym zapisem i archiwizacją zdarzeń.

[2] Opracowanie własne.

Dodatkowo systemy wspomagane są systemem zasilania i oświetlenia awaryjnego. Dla zapewnienia bezpiecznej ewakuacji ludzi podczas pożaru przewidziany jest system ewakuacyjny. Na zewnątrz budynku oraz wewnątrz stosowany jest system sygnalizacji akustycznej i nagłośnienia.

Wszystkie informacje o stanie poszczególnych systemów alarmowych są obrazowane graficznie za pomocą programu zarządzającego zagrożeniami na zintegrowanym stanowisku alarmowania i sygnalizacji zagrożeń (ZSAiSZ) w pomieszczeniu oficera dyżurnego lub (i) wybrane elementy programu - na pomocniczym zintegrowanym stanowisku alarmowania i sygnalizacji zagrożeń - na wartowni.



Rys.4.2.5. Przykładowy model przestrzenny systemu ochrony obiektu wojskowego (wariant)[3]

[2] Opracowanie własne.
[3] A. Wójcik, referat Innowacyjne techniki alarmowania w zakresie elektronicznej ochrony jednostek wojskowych, IV Konferencja KSOŁ-97 AON.

W zaprezentowanym graficznym modelu wykorzystano dostępne systemy sygnalizacji zagrożeń i alarmowania o różnych technikach i technologiach ochrony obiektów, który został przedstawiony na następujących rysunkach[4]:

- Rys. 4.2.1./9. Model podziału stref ochrony obiektu.
- Rys. 4.2.2/9. Model schematu funkcjonalnego modelu systemu ochrony obiektu.
- Rys. 4.2.3/9. Model przykładowego podziału organizacyjnego stref ochrony w obiekcie.
- Rys. 4.2.4/9. Model ochrony obiektu systemem alarmowym włamania i napadu. Prezentacja typowych rozwiązań organizacyjnych i rozmieszczenia elementów systemu.
- Rys. 4.2.5/9. Model ochrony obiektu systemem kontroli dostępu. Prezentacja typowych rozwiązań organizacyjnych i rozmieszczenia elementów systemu.
- Rys. 4.2.6/9. Model ochrony obiektu systemem telewizji użytkowej. Prezentacja typowych rozwiązań organizacyjnych i rozmieszczenia elementów systemu.
- Rys. 4.2.7/9. Model ochrony obiektu systemem sygnalizacji pożaru. Prezentacja typowych rozwiązań organizacyjnych i rozmieszczenia elementów systemu.
- Rys. 4.2.8/9. Model ochrony obiektu przez zintegrowany systemem ochrony obiektu. Prezentacja typowych rozwiązań organizacyjnych i rozmieszczenia elementów systemu.
- Rys. 4.2.9/9. Model organizacji zintegrowanego systemu ochrony obiektu.

W rozprawie został zaprezentowany na dziewięciu rysunkach model ochrony obiektu w ujęciu powiązań organizacyjnych, funkcjonalnych jak i również wymagań technicznych i technologicznych wykorzystywanych w ochronie obiektów, ze szczególnym uwzględnieniem wysokiego stopnia zagrożenia, które występują w wypadku ochrony obiektów wojskowych. Na etapie opracowywania modelu przyjęto szereg założeń, zarówno w postaci wymagań, jak i niezbędnych uproszczeń dla uwzględnienia jak największej ilości czynników, które wpływają na funkcjonowanie modelu w rzeczywistości.

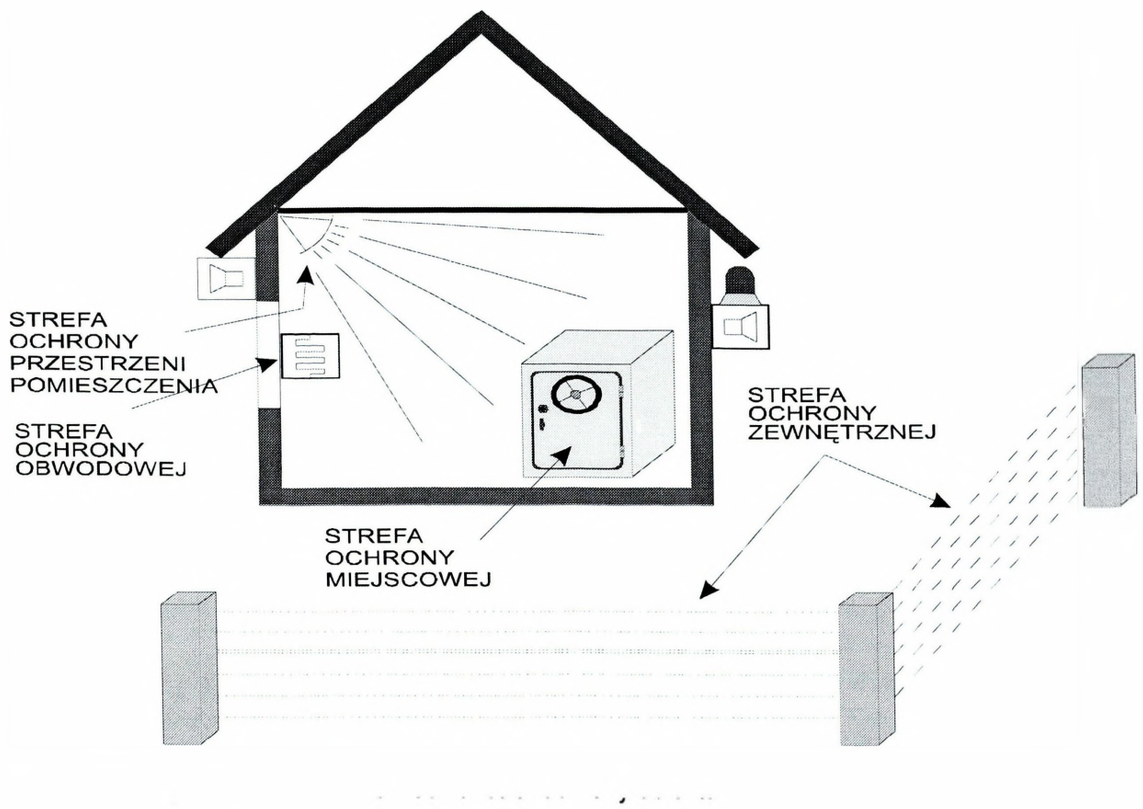
System ochrony obiektu wojskowego, z uwagi na swą specyfikę, wymuszał systemowe podejście do badań, których podstawą, między innymi, było świadome posługiwanie się modelem systemu na określonym poziomie uszczegółowienia – adekwatnym do aspektu analizowanych procesów.

Stąd też istnieje możliwość zaprezentowania szeregu wariantów lub ich modyfikacji, które mogą wystąpić podczas jego wdrażania w warunkach rzeczywistych.

---

[4] Opracowanie własne.

Na zamieszczonym rys. 4.2.1/9 modelu ochrony obiektu został zaprezentowany przykładowy podział stref ochrony. Zwiększenie ilości stref ochrony obiektu utrudnia wniknięcie i penetracje przez intruza obiektu oraz umożliwia bardzo wczesne wykrycie prób (działań) zagrażających bezpieczeństwu obiektu.



Rys 4.2.1/9.Podział stref ochrony obiektu (wariant)

Na schemacie modelu 4.2.2/9 przedstawiono wariant stref ochrony obiektu wojskowego. Pierwsza strefa ochrony zewnętrznej realizowana jest przez zewnętrzne systemy alarmowe. W tym rozwiązaniu wykorzystuje się często już istniejące ogrodzenie obiektu. W dalszej kolejności ochrona obiektu obejmuje strefę obwodową obiektu, ochronę wewnętrzną i miejscową (konkretnego przedmiotu w ochranianym obiekcie np. kasę pancerną). Rysunek 4.2.1/9 przedstawia przykładowy podział ochrony obiektu wojskowego na następujące strefy ochrony:

- peryferyjnej lub (i) zewnętrznej (rys. 4.2.1/9);
- obwodowej (rys. 4.2.1/9);

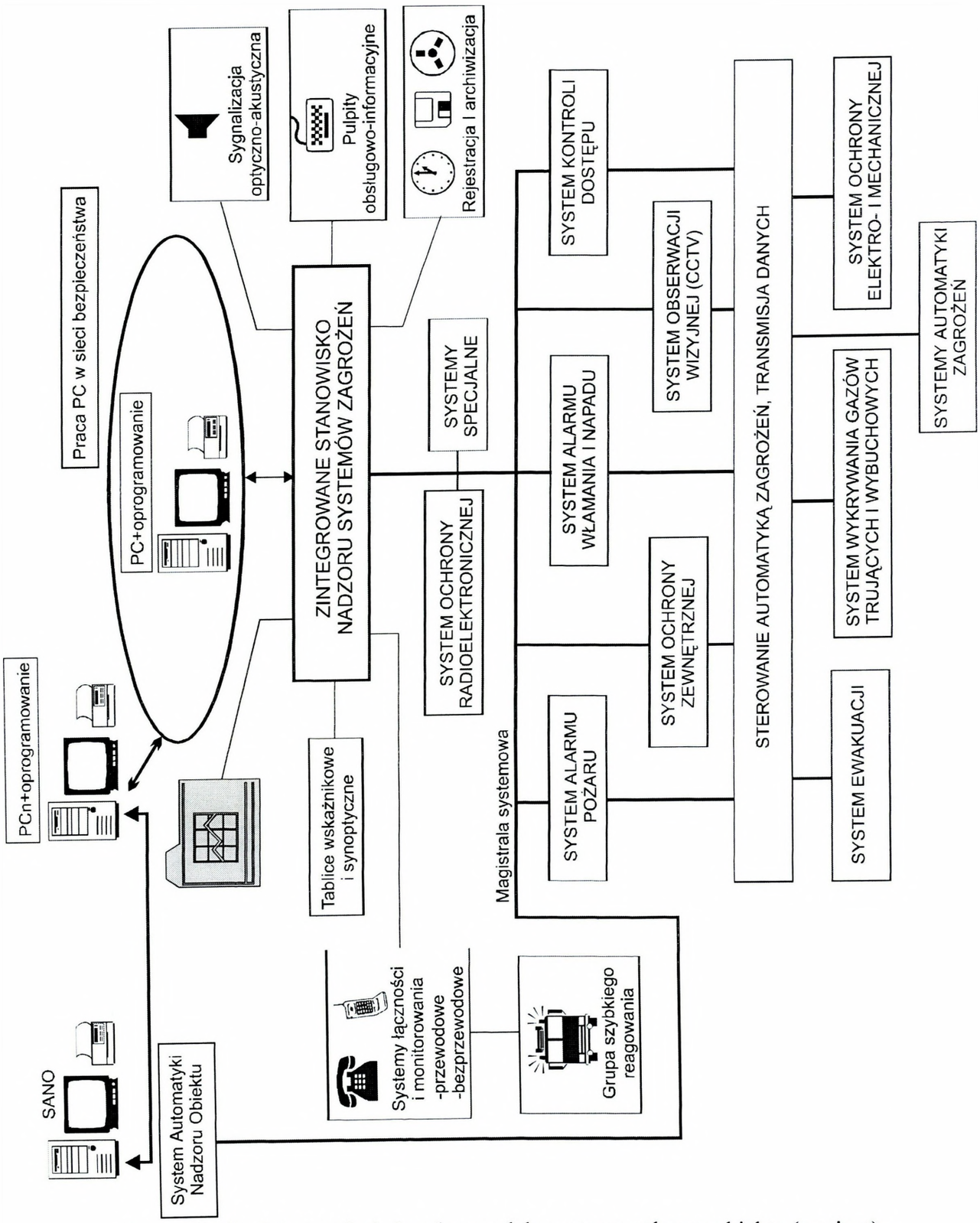
- wewnętrznej i miejscowej (rys. 4.2.1/9).

Ochrona peryferyjna umożliwia daleko idącą prewencję i rozpoznanie ewentualnego intruza. Ochrona obwodowa stanowi bezpośredni dozór elektroniczny obwodu, najczęściej ogrodzenia obiektu wojskowego.

Ochrona wewnętrzna pozwala na wykorzystanie wszystkich urządzeń technicznych systemów sygnalizacji i alarmowych.

Na rys.4.2.2/9 przedstawiony został funkcjonalny model systemu ochrony obiektu z integrowanym stanowiskiem nadzoru systemów zagrożeń i alarmowania. W omawianym modelu zaprezentowany został wariant z jednym stanowiskiem operatora (oficera dyżurnego). Takich stanowisk można utworzyć więcej zależnie od potrzeb użytkownika.

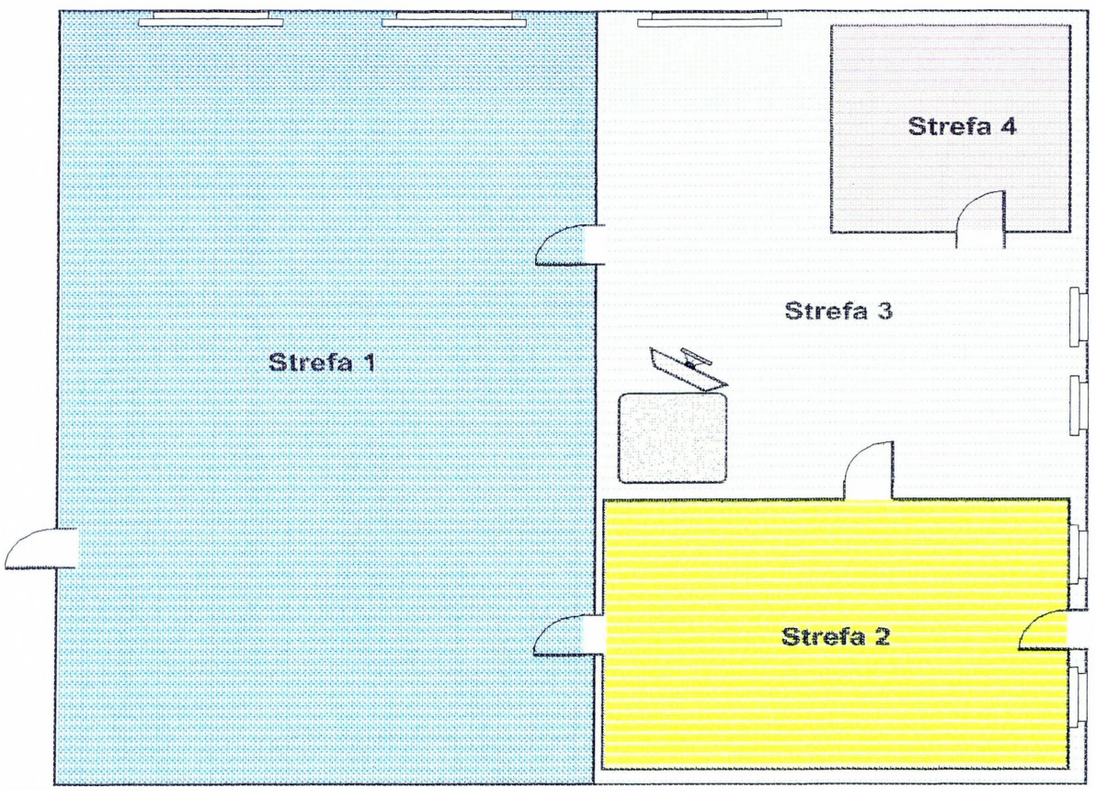
Na zintegrowane stanowisko napływają sygnały ze wszystkich systemów zagrożeń i alarmowania chroniących obiekt. Operator ma możliwość wglądu i raportowania stanu ochrony obiektu.



Rys. 4.2.2/9. Schemat funkcjonalny modelu systemu ochrony obiektu (wariant)

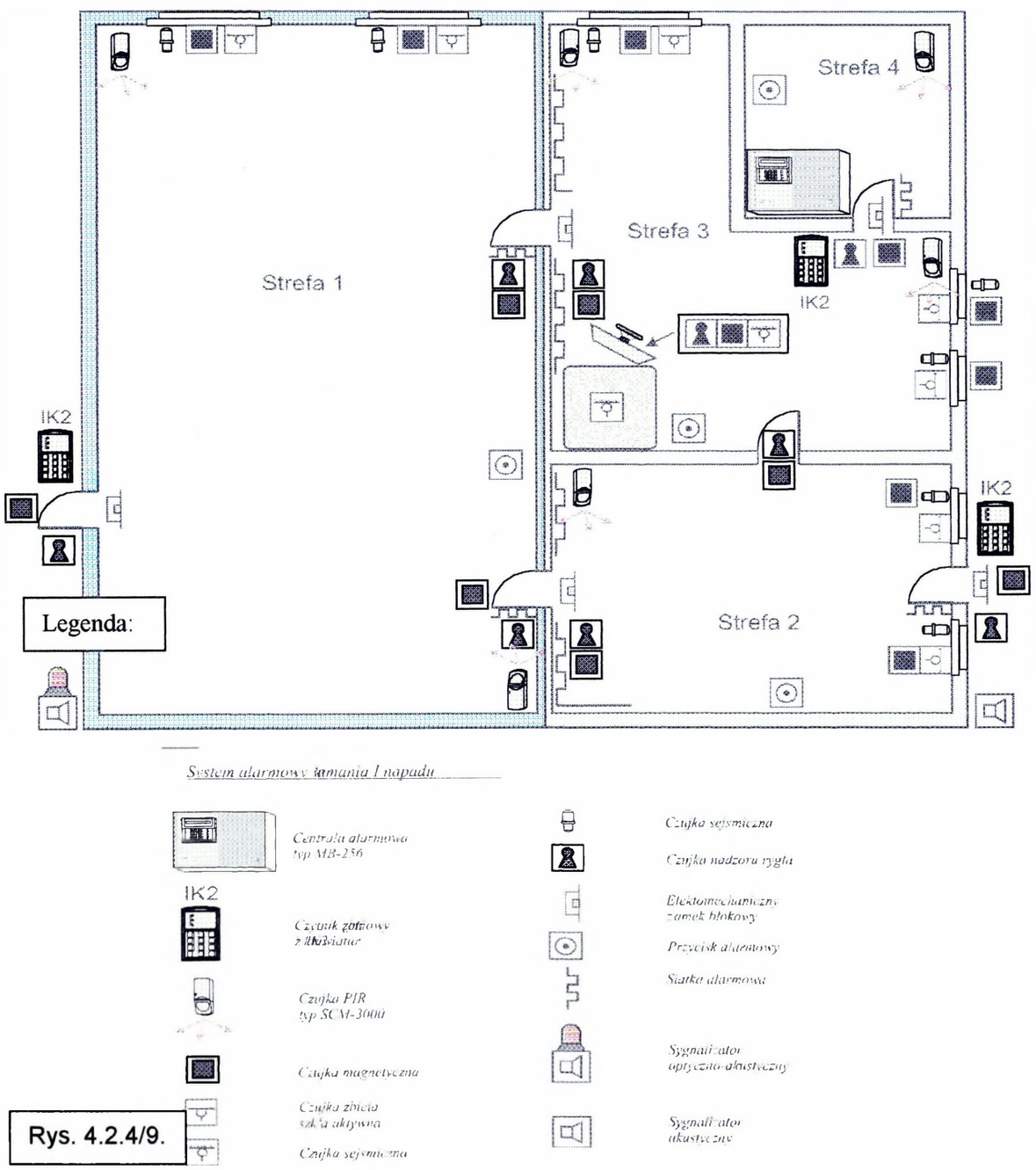
Model 4.2.3/9 prezentuje przykład podziału organizacyjnego stref ochrony wewnętrznej w obiekcie. Organizacja stref ochrony jest jednym z podstawowych zadań przy planowaniu modelu systemu alarmowego.

Strefa 1,2 mogą być strefami klasy I i II, natomiast strefa 3 - strefą administracyjną.



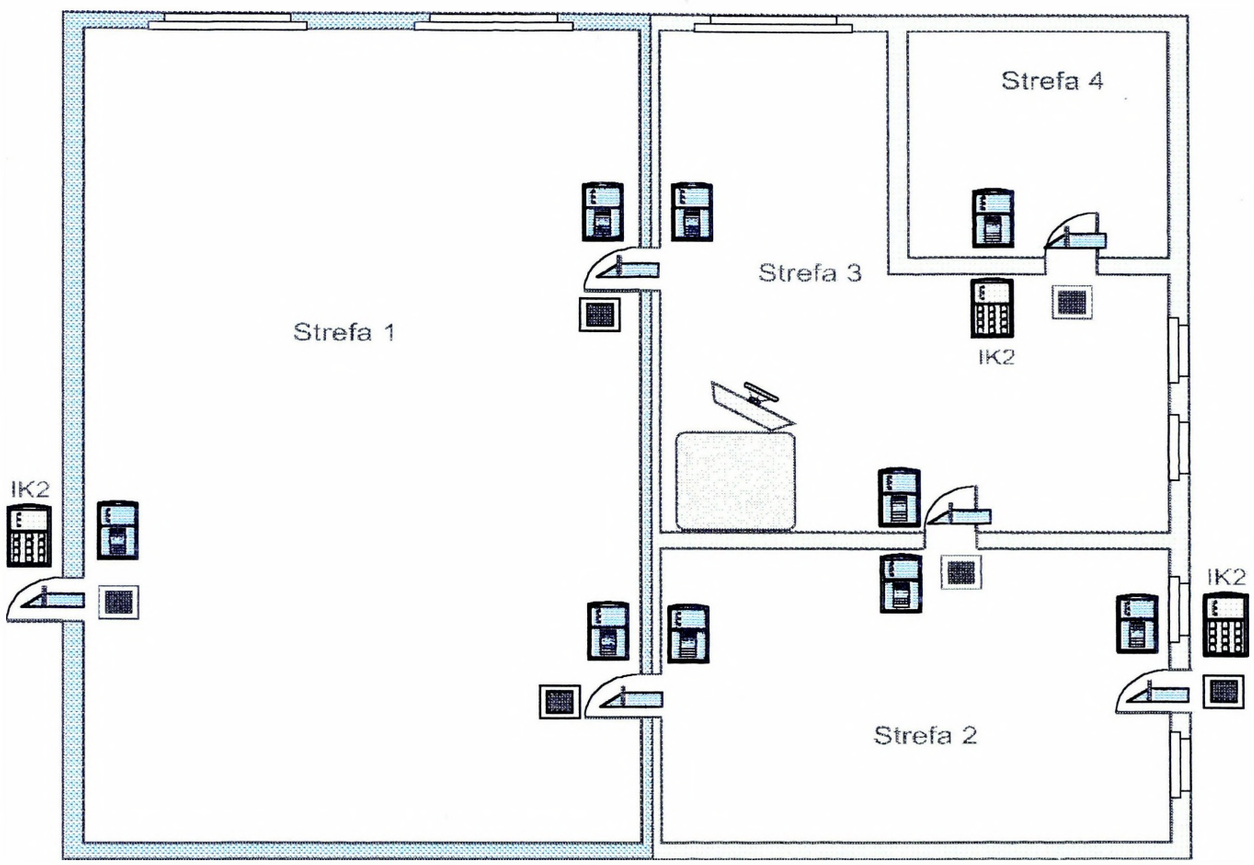
Rys 4.2.3/9. Model podziału organizacyjnego stref ochrony wewnętrznej w obiekcie (wariant)

Model 4.2.4/9 przedstawia wariant rozwiązania systemu alarmowego włamania i napadu (SAWiN). System SAWiN jest podstawowym system eliminującym próby ingerencji intruza do obiektu strzeżonego. W tym systemie wykorzystywany jest największy potencjał taktyczny i organizacyjny ochrony obiektu oraz techniczny urządzeń do wczesnego wykrycia prób włamania i napadu oraz jak najszybszej ich neutralizacji.



Rys. 4.2.4/9.

Model 4.2.4/9.Model ochrony obiektu systemem alarmowym włamania I napadu (wariant)



Legenda:

System kontroli dostępu

IK2 *Czytnik kart zbliżeniowych z klawiaturą*

Czytnik kart zbliżeniowych

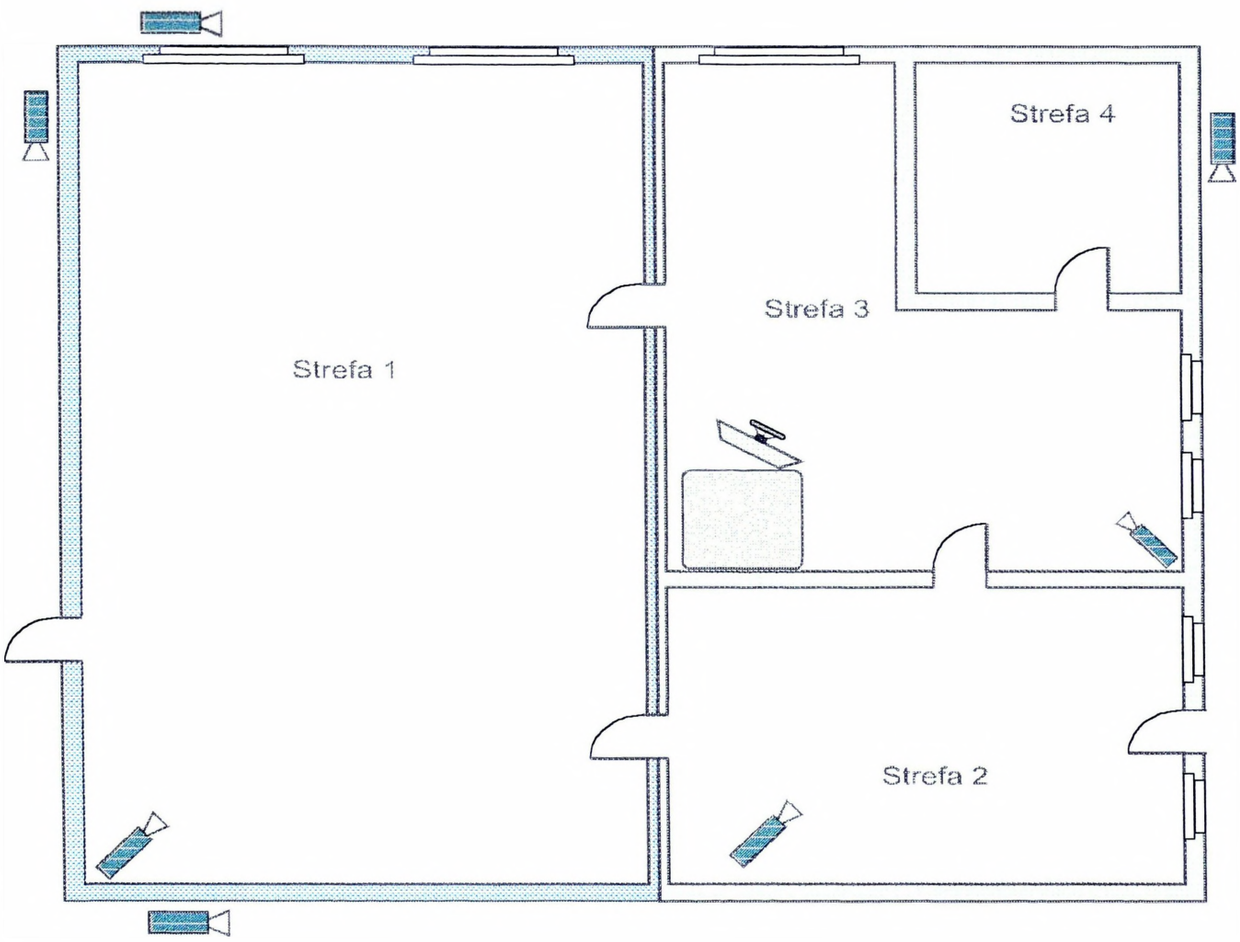
Elektrozaczep

Czujka magnetyczna (otwarcia drzwi)

Stanowisko komputerowe nadzoru systemu SKD

Rys. 4.2.5/9. Model ochrony obiektu systemem kontroli dostępu (wariant)

W modelu 4.2.5/9 zaprezentowano rozwiązanie ochrony obiektu systemem kontroli dostępu. System kontroli dostępu uniemożliwia wejście niepowołanym osobom oraz wjazd pojazdów w strefy chronione. Monitoruje i identyfikuje obecność osób w poszczególnych strefach ochrony. Stanowi podstawowy system ochrony przed dostępem do osób niepowołanych do informacji niejawnych.

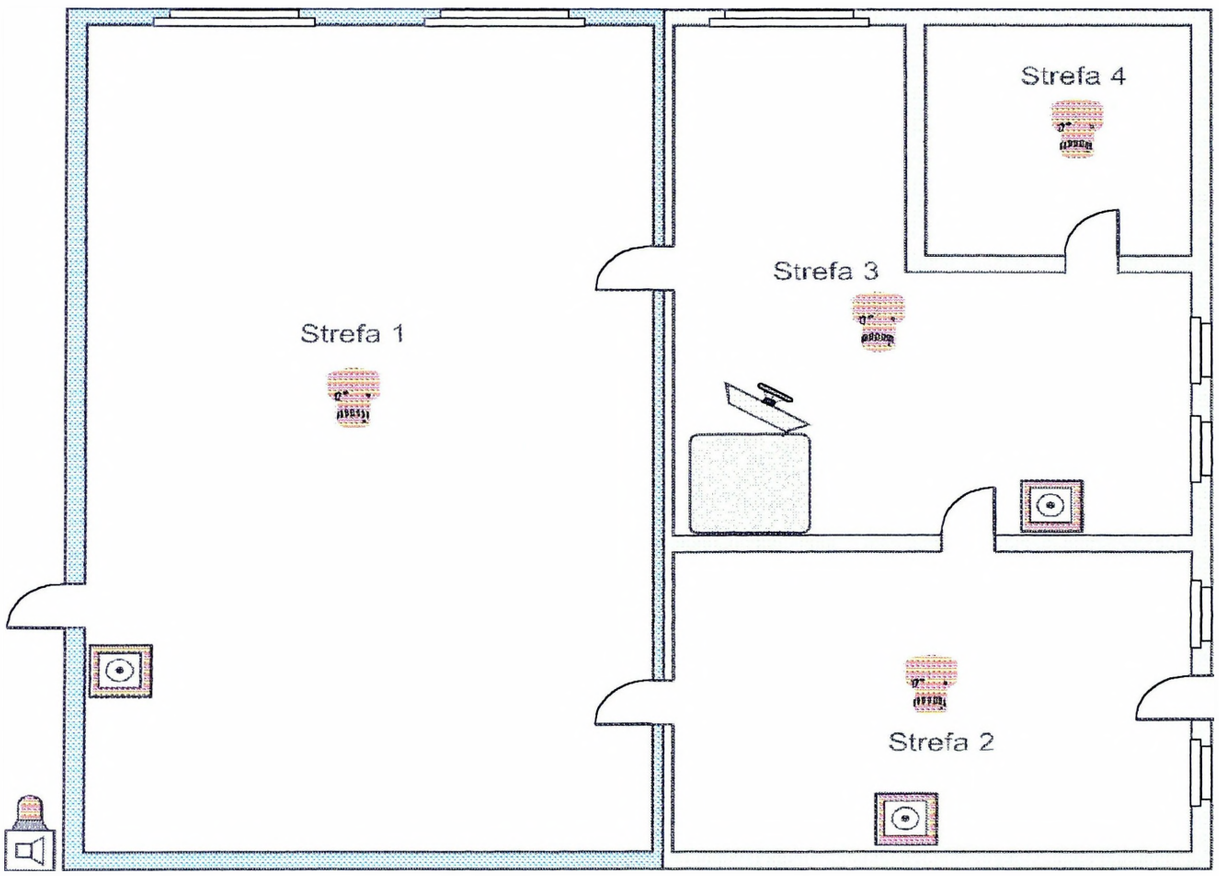


Legenda:



Rys. 4.2.6/9.Model ochrony obiektu systemem telewizji użytkowej - CCTV (wariant)

System nadzoru wizyjnego- CCTV[5] lub telewizji użytkowej przedstawiony w modelu 4.2.6/9 weryfikuje informacje uzyskane z innych systemów oraz spełnia funkcje rozpoznania przez operatora (użytkownika) bezpośredniego zagrożenia za pomocą obrazu..



Legenda:

System alarmu pożaru

Czujka dymu/temperatury

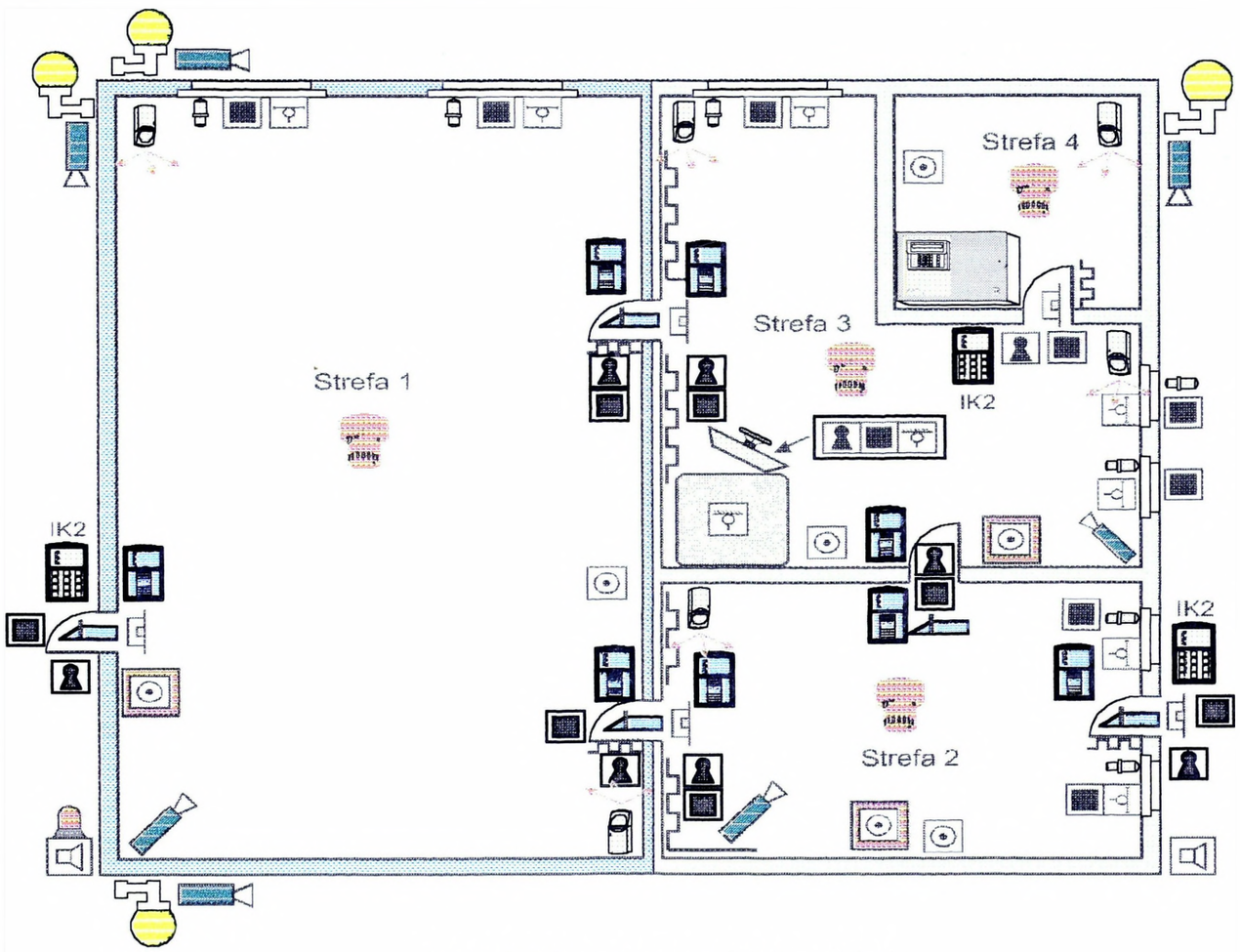
Przycisk alarmu pożaru

Sygnalizator optyczno-akustyczny

Rys. 4.2.7/9. Model ochrony obiektu systemem sygnalizacji pożaru (wariant)

[5] CCTV – closed circuit television – angielskie określenie telewizji użytkowej.

Model 4.2.7/9 przedstawia sposób ochrony obiektu przed zagrożeniem pożarowym. Pożar jako jedno z najważniejszych zagrożeń obiektu, musi być wykrywany w jak najwcześniejszym stadium jego rozpoczęcia. Zadanie to umożliwia nowoczesny system bardzo wczesnego wykrywania zagrożenia dymem, ogniem i gazami trującymi. Wywołanie zagrożenia pożarowego jest jednym z podstawowych działań sabotażowych i terrorystycznych.

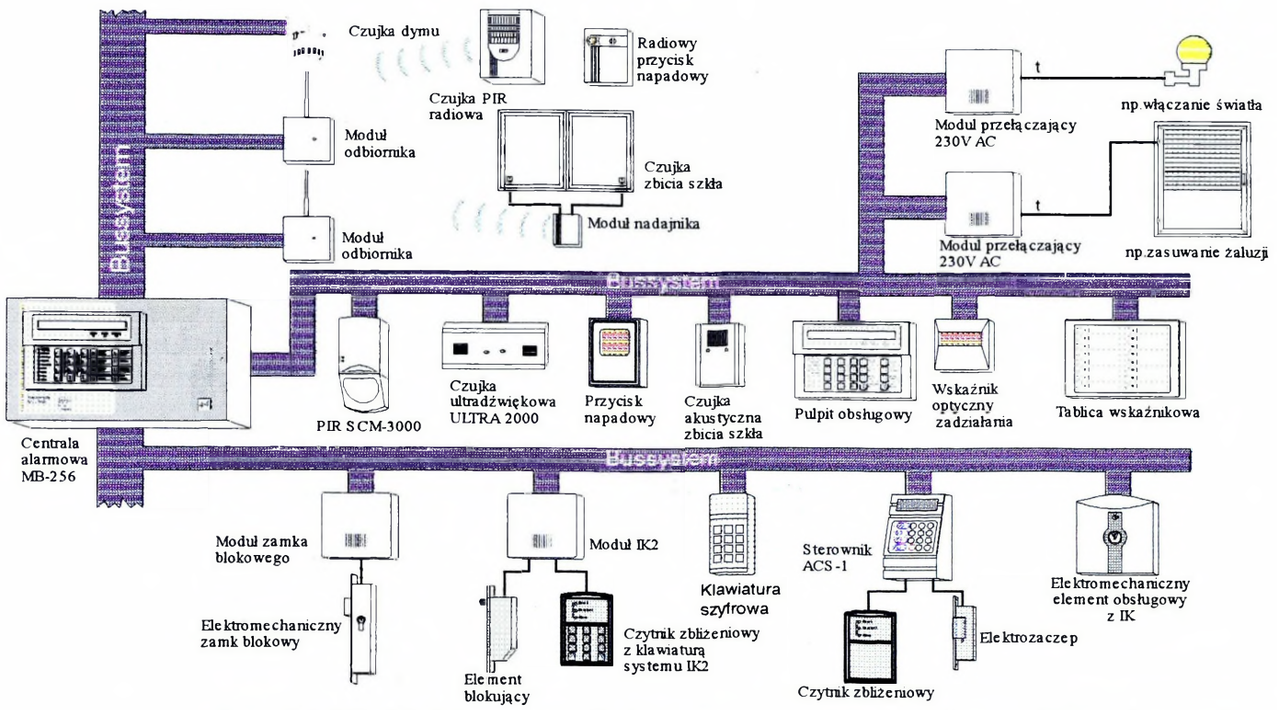


Legenda jak przy poprzednich modelach

Rys. 4.2.8/9. Model ochrony obiektu przez zintegrowany system ochrony obiektu (wariant)

Model 4.2.8/9 jest prezentacją zintegrowanego systemu ochrony obiektu wojskowego. System zintegrowany zwielokrotnia możliwości poszczególnych systemów sygnalizacji zagrożeń, poprzez współdziałanie i koncentrację czynników neutralizujących zagrożenia. System zintegrowany jest skuteczniejszy niż suma pracujących autonomiczne systemów zagrożeń (efekt synergetyczny).

Bazą budowy zintegrowanych modeli systemów ochrony jest nowoczesna centrala alarmowa np. MB-256, która umożliwia poprzez magistrale z cyfrową transmisją informacji podłączenie różnorodnych elementów systemu ochrony obiektu i zintegrowanie ich w jeden funkcjonujący zespół, spełniający stawiane wymagania tej klasy systemom, w modelu ochrony obiektu na rys. 4.2.9/9.



Rys. 4.2.9/9. Model organizacji zintegrowanego systemu ochrony obiektu (wariant)

Wykorzystanie techniki komputerowej zapewnia największą dokładność w prawidłowym określeniu elementów systemu alarmowania oraz jego powiązań[6].

Wspomaga i automatyzuje proces decyzyjny, przy skróceniu czasu otrzymania oczekiwanego wyniku, jednocześnie minimalizuje błędy.

Podstawowe możliwości wykorzystania techniki komputerowej przy opracowaniu modelu systemu sygnalizacji zagrożeń i alarmowego podzielono na następujące grupy:

a. Powszechnie zastosowane i w rozumieniu ogólnym, stosowanie komputerów do opracowania i wspomagania modelu; w tym wypadku komputer wraz z oprogramowaniem zastosowany jest do opracowywania, np. z pomocą pakietu kalkulacyjnego Microsoft Excel, danych uzyskanych podczas analizy przebiegu modelu, a później opisu tekstowego wyników pracy, np. za pomocą edytora tekstów Microsoft Word, oraz archiwizowania i przechowywania uzyskanych wyników w pamięci komputera lub zewnętrznej. W przypadkach bardziej zaawansowanych stosuje się profesjonalne oprogramowanie wspomagania projektowania AutoCad.

b. Zorientowane programowo, tzn.:

[6] A. Wójcik, *Chip. Magazyn komputerowy* numery z 1997/98.

- własne opracowania, tj.: wykorzystanie dostępnego specjalistycznego oprogramowania[7] dla opracowania danych niezbędnych do analizy modelu, np. w bazie danych Microsoft Access dla zautomatyzowania procesu wyboru rodzaju urządzenia alarmowego, typu urządzenia, optymalnej ceny, opisów technicznych, producentów itd.; programy specjalistyczne obejmujące wycinek zagadnienia, np. kosztorysowanie i optymalizacja kosztów inwestycji w zakresie technicznej ochrony. Wariantowe opracowanie kosztorysów systemów alarmowych za pomocą arkuszy kalkulacyjnych, np. Microsoft Excel, wykorzystujących specjalistyczne procedury makroprogramowania.
- programy dialogowe (eksperckie)[8] wykorzystujące bazy danych. Takie rozwiązanie stanowi wyższy stopień zaawansowania technicznego stosowania modelu systemu alarmowego. Na podstawie przebiegu schematu graficznego modelu można przygotować oprogramowanie, w którym użytkownik odpowiada na zadawane pytania, a komputer z pomocą procedur i algorytmów systematyzuje odpowiedzi i sprawdza ich poprawność. Po przejściu całej procedury pytań związanych z modelowaniem systemu alarmowego komputer kończy pracę i prezentuje wyniki wg wybranej przez użytkownika opcji. Przebieg takiego programu wygląda następująco:

np. procedury zbierania danych:

Pytanie: „Podaj nazwę i adres obiektu"

Odpowiedź użytkownika: „....."

Pytanie: „Określ położenie obiektu:

a -wolno stojący, b -w zabudowie zespolonej" itd.

Wszystkie pytania dotyczące utworzenia bazy danych obiektu

np. procedury analizy:

Pytanie: „Obiekt posiada system alarmowy?"

Odpowiedź: „Tak"

Pytanie: „Kiedy system alarmowy został zainstalowany?" itd..

Jest to odpowiedni program do zbierania i systematyzowania danych oraz automatyzacji podejmowania decyzji przez osoby nie posiadające wysokich branżowych kwalifikacji zawodowych. Główne wady to: długi czas opracowywania wyników oraz zdanie się na subiektywną ocenę

[7] D. Boratyn, *Access 97*, Croma,Wrocław 1997.
[8] S. Santarek, K. Strzelczak, *Elastyczne systemy produkcyjne*, WNT, Warszawa 1989.

użytkownika. Taki program w uproszczonej wersji, zbudowany na bazie np. Visual Basic, może być stosowany z powodzeniem wśród kadry ekspertów jako narzędzie wspomagające.

1. Graficzne modele systemu alarmowego. W tych metodach możemy wyróżnić grafikę zorientowaną na dane zagadnienie wykorzystywane jednorazowo lub grafikę prezentującą przetworzone procesy analityczne modelu, połączoną z wynikami otrzymanymi ze stosowania np. omówionego wyżej oprogramowania eksperckiego lub wynikami symulacji komputerowej. W pierwszym przypadku możemy wykorzystać dla podniesienia atrakcyjności i sugestywnego przybliżenia modelu standardowe oprogramowanie do prezentacji wyników np. oprogramowanie graficzne CorelDRAW. Drugi z omawianych przypadków ujmuje syntetyczne połączenie programu przebiegu modelu systemu alarmowego z jednoczesną prezentacją graficzną jego wyników, zarówno cząstkowych, jak i ostatecznych. W tym wypadku można zastosować oprogramowanie prezentacyjne Microsoft PowerPoint .[9]
2. Komputerowe modele symulacyjne systemów alarmowych. Można wyróżnić modele: graficzne; graficzno – matematyczne; matematyczne. Modele symulacyjne służące analizie problemów zarządzania konstruowane są w celu[10]: opisu bieżącego funkcjonowania systemu; analizy hipotetycznego systemu; zaprojektowania udoskonalonego systemu

Przy budowie modelu symulacyjnego wyróżnia się następujące kroki:

Krok I. Sformułowanie modelu.

Należy tak skonstruować model, aby nie popełnić błędu polegającego na wprowadzeniu zbyt dużej liczby szczegółów do modelu. Ochroni to komputer przed zbyt długim czasem opracowania wyników oraz zawieszenia systemu operacyjnego. Najlepszym zabezpieczeniem przeciwko wystąpienie takiej sytuacji jest rygorystyczne przestrzeganie celu, dla którego został zbudowany model.

Krok II. Projektowanie eksperymentu.

Szansę popełnienia błędów można zredukować przez opracowanie szczegółowych procedur eksperymentu przed przystąpieniem do wykonania obliczeń. Należy także określić statystyczne narzędzia, za pomocą których można dokonać pomiaru zmienności wynikającej z błędów.

---

[9] S. Uss, *PowerPoint 7 Pl,*Help, Warszawa 1996.
[10] M. Harvey Wagner, *Badania operacyjne*, PWE, Warszawa 1980.

Krok III. Przygotowanie programu komputerowego.

Eksperymenty symulacyjne są z reguły dokonywane przy użyciu mikrokomputerów z procesorami o dużej szybkości przetwarzania np. Pentium II firmy Intel z zegarem o częstotliwości powyżej 200 MHz. Wszystkie obliczenia i generowane zdarzenia zachodzą w komputerze przy wykorzystaniu specjalistycznych języków oprogramowania np. języka C.

Elementem krytycznym przy opracowywaniu modelu symulacyjnego jest dobranie odpowiednich narzędzi matematycznych dla sformułowania modelu. Istnieje szereg metod matematycznych, które pozwolą zaprezentować opisany model relacjami zależności matematycznych. Zaproponowano jedną z najprostszych metod, stosowanych do systemowej analizy strukturalno-funkcjonalnej systemu, gdy liczba jego elementów jest zbyt duża dla prawidłowej oceny i analizy przez człowieka, np. powyżej 15 elementów. Dla jednego zbioru elementów systemu można zbudować macierze oddziaływań i (lub) przyporządkowań oraz grafy w postaci struktur zorganizowanych, ukierunkowanych tematycznie. Struktura zorganizowana i ukierunkowana tematycznie oznacza pojęciowe (graficzne i (lub) matematyczne) rozmieszczenie w czasie i przestrzeni elementów składowych systemu oraz ukierunkowanych tematycznie zależności między tymi elementami.

Strukturę systemu można przedstawić w postaci dwójki uporządkowanej:

struktura systemu = {X: [Rm] >; m.= 1, ..., M}

gdzie:

X – ilość elementów;

Rm - rodzaj relacji;

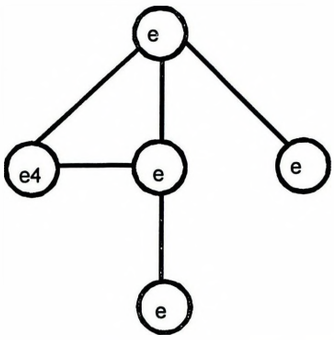
M – liczba rozpatrywanych relacji.

W praktyce strukturę systemu najwygodniej jest rozpoznać opisując wszystkie jej elementy oraz współzależności w macierzach oddziaływań i zależności. Najprostszym sposobem modelowania struktury zorganizowanej jest przedstawienie wzajemnych oddziaływań jej elementów w macierzy oddziaływań i na tej podstawie zbudowanie grafu.

Do modelowania użyto następujących typów grafów:

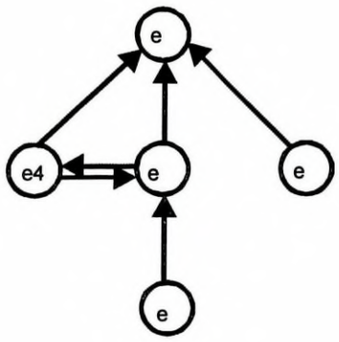
– nie zorientowanych, które nie pokazują kierunku oddziaływań,

– zorientowanych, pokazujących kierunki oddziaływań.



	e1	e2	e3	e4	e5
e1	1	1	0	1	
e2	0	1	1		
e3	0	0			
e4	0				
e5					

Graf i macierz oddziaływań zwykłych



	e	e	e	e	e
e	0	0	0	0	0
e	1	0	0	1	0
e	0	1	0	0	0
e	1	1	0	0	0
e	1	0	0	0	0

Graf i macierz oddziaływań ukierunkowanych

Rys.4.2.7.Typy grafów i macierzy oddziaływa

W macierzach oddziaływań (rys.4.2.7) rozróżnia się oddziaływania bezpośrednie (tzn. pierwszego rzędu) od drugiego i dalszych rzędów. Dla oddziaływań każdego rzędu buduje się odrębne macierze i grafy. Macierze oddziaływań ukierunkowanych są zawsze kwadratowe. Krawędzie ich są takie same jak macierzy oddziaływań nieukierunkowanych. Jeśli element „*i*" działa na element „*j*", to w węźle „*aij*" wstawia się wartość 1. W węźle „*eij*" można postawić 1 tylko wtedy, gdy równocześnie zachodzi ukierunkowane oddziaływanie elementu „*j*" na element „*i*". Zaprezentowany model systemu alarmowego i sygnalizacji zagrożeń (ochrony obiektu) posiada cechy macierzy i grafu oddziaływań ukierunkowanych.

Techniki multimedialne modelowania systemów alarmowych mogą połączyć łatwość dialogu komputerów (komunikujących się z użytkownikiem poprzez tzw. pulpit roboczy - desktop computer) z obrazami i dźwiękiem udostępnionymi na ekranie monitora, tworząc w ten sposób

nowy, ułatwiony sposób komunikacji.[11] Modele zbudowane z wykorzystaniem komputerowej techniki multimedialnej są nie tylko najbardziej atrakcyjne wizualnie, ale także najbardziej skomplikowane i czasochłonne (kosztowne) do przygotowania. Wymagają nie tylko wiedzy eksperckiej z zakresu systemów alarmowych, ale także dużej wiedzy z zakresu informatyki stosowanej, która jest niezbędna do stworzenia takiego modelu. Tak zbudowany model jest doskonałym narzędziem zarówno dla profesjonalisty, jak i przeciętnego użytkownika, którego należy wdrożyć do zagadnień ochrony obiektów wojskowych np. ze względu na objęcie przez niego funkcji kierowniczych związanych z ochroną obiektów.

Model multimedialny wykorzystuje wszystkie omówione techniki wspomagania komputerowego w zakresie zaawansowanym. Ostateczna jego forma może być napisana w specjalistycznym programie zależnie, od skomplikowania zagadnienia, np. Visual Basic lub HTML do opisu pulpitu obsługowego. Do stworzenia animacji można wykorzystać jedno z wielu profesjonalnych aplikacji, np. ActiveX. Program powinien być dostosowany do nowoczesnej internetowej platformy komunikacyjnej, np. za pomocą języka Java lub HTML. Tak przygotowany model systemu alarmowania jest nowoczesną aplikacją programową oddaną użytkownikowi do eksploatacji w przystępnym i rozpowszechnionym systemie Windows 9x/NT.

W tym typie modelowania systemów alarmowych wykorzystuje się omówione wspomaganie multimedialne oraz urządzenia alarmowe lub modele systemów alarmowych, np. na tablicach prezentacyjnych, zaprogramowanych dla konkretnego obiektu, pracujących w czasie rzeczywistym.[12] Taki model umożliwia symulowanie określonych sytuacji i zachowań systemu alarmowego. Wszystkie stany centrali alarmowej systemu przekazywane są na stanowisko komputerowe, gdzie użytkownik (operator) otrzymuje wyniki modelowania określonych sytuacji zagrożeń.

Cechy omawianego modelu mają zintegrowane programy graficznego wspomagania zarządzania zagrożeniami. Profesjonalny program ma moduł symulacji różnych stanów pracy systemów, które można rozbudować o kolejne opcje. Wadą tego typu modeli jest ich wysoki koszt, natomiast niezaprzeczalną zaletą pełna symulacja modelu systemu sygnalizacji zagrożeń i alarmowego. Opisane wyżej warianty budowy modelu ochrony obiektu stanowią ścieżkę do doskonalenia procedury opracowywania modelu systemu ochrony obiektu. Jednocześnie obejmują coraz bardziej zawansowane techniki opisu takiego modelu, od heurystycznego opisu,

---

[11] Na podstawie B. Steinbrink, *Multimedia u progu technologii XXI wieku*, Robomatic 1993.
[12] Opracowanie własne na podstawie materiałów *Produktsliste 98. Einbruchmeldesysteme effeff.*

poprzez techniki analizy wartości i analizy systemowej, aż do komputerowych programów eksperckich opartych na modelowaniu matematycznym.

Omawiane wyżej zasady stały się podstawą do opracowania metodologii weryfikacji modelu systemu ochrony obiektu.

4.3. Weryfikacja modelu systemu ochrony obiektu

W tym rozdziale poddano weryfikacji przykładowy model systemu ochrony obiektu, stosując konfrontację z modelem opracowanym w rozprawie.[13] Dokonano wyboru obiektu do weryfikacji zaproponowanego modelu oraz na podstawie zastosowanych technik zaprezentowano wyniki weryfikacji. Do empirycznej weryfikacji ze względu na cechy i funkcje pełnione w strukturze obronnej państwa autor wybrał model zbudowany na podstawie systemu ochrony Akademii Obrony Narodowej.

Akademia Obrony Narodowej (AON) stanowi zespół obiektów na rozległym obszarze o różnorodnej funkcji i infrastrukturze. AON, ze względu na niepowtarzalny charakter i funkcje, jakie pełni w strukturach obronnych państwa, podlega różnorodnym zagrożeniom.

W zasadzie można stwierdzić, że system alarmowy i sygnalizacji zagrożeń chroniący AON istnieje tylko w postaci fragmentarycznej.

We wnioskach autor ustosunkował się do wyniku badań oraz zaproponował metody podniesienia stanu bezpieczeństwa weryfikowanego systemu ochrony obiektu.

Dlatego do weryfikacji modelu zostały wykorzystane dwie prace zrealizowane na potrzeby AON, a dotyczące sfery bezpieczeństwa:

- Projekt Systemów Alarmowych Sygnalizacji Zagrożeń Akademii Obrony Narodowej opracowany przez Zakład Zarządzania Systemami Informacyjnymi pod kierunkiem płk dr inż. Eugeniusza Piedziuka z marca 1998 roku.
- Bezpieczeństwo Obiektów Akademii Obrony Narodowej. Zapis problemów do zbadania i zaleceń dla projektowania zabezpieczenia technicznymi urządzeniami sygnalizacyjnymi i alarmowymi - ekspertyza opracowana pod kierunkiem gen. bryg. rez. dr. Zbigniewa T. Nowickiego z czerwca 1996 roku.

Wymienione dokumenty są rozpatrywane razem, ponieważ wzajemnie się uzupełniają tematycznie.

---

[13] Opracowanie własne na podstawie *Projekt Systemów Alarmowych Sygnalizacji Zagrożeń Akademii Obrony Narodowej*, opracowanie pod kierunkiem Piedziuk E., AON, Warszawa 1998.

Gdyby rozpatrywano tylko projekt, to zawarte w nim rozwiązania nie znalazłby uzasadnienia z punktu analizy zagrożeń zawartej w dokumencie dotyczącym bezpieczeństwa AON i byłyby ocenione jako niekompletne. Także dokument określający zapis problemów do zbadania nie może występować samodzielnie ze względu na brak konkretnych rozwiązań systemowych w zakresie ochrony obiektów AON.

W dalszej części rozdziału oraz procedury weryfikacyjnej wymieniona pozycja dotycząca oceny bezpieczeństwa AON traktowana jest jako opracowanie kompletne.[14]

Do weryfikacji modelu autor użył techniki tabelarycznego opisu elementów projektu[15] wg procedury zawartej w procedurach metodologii opracowywania modelu systemu alarmowego i sygnalizacji zagrożeń. Tą techniką badał prawidłowość opracowania z weryfikowanym modelem.

Dla uproszczenia obliczeń przyjęto założenie, że AON jest obiektem jednolitym, tzn. nie rozpatrujemy poszczególnych obiektów wchodzących w skład kompleksu. Pozwoliło mi to zmniejszyć liczbę powtarzających się arkuszy analitycznych przy jednoczesnym zachowaniu celu weryfikacji.

Nie rozpatrywano drugiej i trzeciej części modelu, dotyczącej weryfikacji systemu alarmowania i realizacji inwestycji, ponieważ projekt systemu alarmowego AON nie został na dzień dzisiejszy zrealizowany ani także nie jest jeszcze w pełni eksploatowany.

W tabeli wyszczególniono elementy wchodzące w skład systemu alarmowego.[16]

Każdy z elementów oceniono wagowo wg skali od 0 do 5 punktów, nadając następującą skalę ocen:

0 - 2 - ocena niezadowalająca;

3 - ocena zadawalająca;

4 - ocena dobra;

5 - ocena bardzo dobra.

Następnie obliczono sumaryczną liczbę uzyskanych punktów w kolumnie i porównano z maksymalną liczbą punktów możliwych do uzyskania, określając w ten sposób poziom techniczny systemu wg wzoru:

$$\mathbf{Px = \sum Pi}$$

gdzie:

Px - poziom techniczny rozpatrywanego systemu alarmowego,

---

[14] Opracowanie własne na podstawie *Bezpieczeństwo obiektów Akademii Obrony Narodowej. Zapis problemów do zbadania i zaleceń dla projektowania zabezpieczenia technicznymi urządzeniami sygnalizacyjnymi i alarmowymi,* ekspertyza opracowana pod kierunkiem Nowicki Z. T., Warszawa 1996.

[15] Opracowanie własne.

i = 1.....n,

n - liczba rozpatrywanych elementów.

Jego wielkość porównana z normatywną tabelą pozwoliła określić wynik weryfikacji.

W dalszej części obliczono współczynnik sprawności systemu wg wzoru:

$$\eta = Px / Pmax$$

gdzie: Px - poziom techniczny rozpatrywanego systemu ochrony obiektu (alarmowego);

Pmax - maksymalny do uzyskania poziom techniczny systemu ochrony obiektu.

Tabela 4.3.1.Określenie poziomu technicznego systemu ochrony obiektu

Lp	Określenie skuteczności technicznej i organizacyjnej systemu ochrony obiektu*	Symbol	Ilość punktów
1	Idealny	P0	220
2	Wzorcowy	P1	194-219
3	Wysoki	P2	166-193
4	Średni	P3	139-165
5	Niski	P4	110-138
6	Niezadowalający	P5	0-109

*Skuteczność techniczna i organizacyjna systemu alarmowego jest to całokształt środków materialnych i przedsięwzięć organizacyjnych oraz innych nakładów celowych, których zadaniem jest zbudowanie maksymalnie neutralizującego zagrożenia systemu alarmowego służącego ochronie obiektu.

Należy zwrócić uwagę na fakt, że wielkości zawarte w tabeli ulegną zmianie w zależności od tego ile elementów modelu systemu zostanie zawartych. Stwarza to warunki uniwersalności obliczeń.

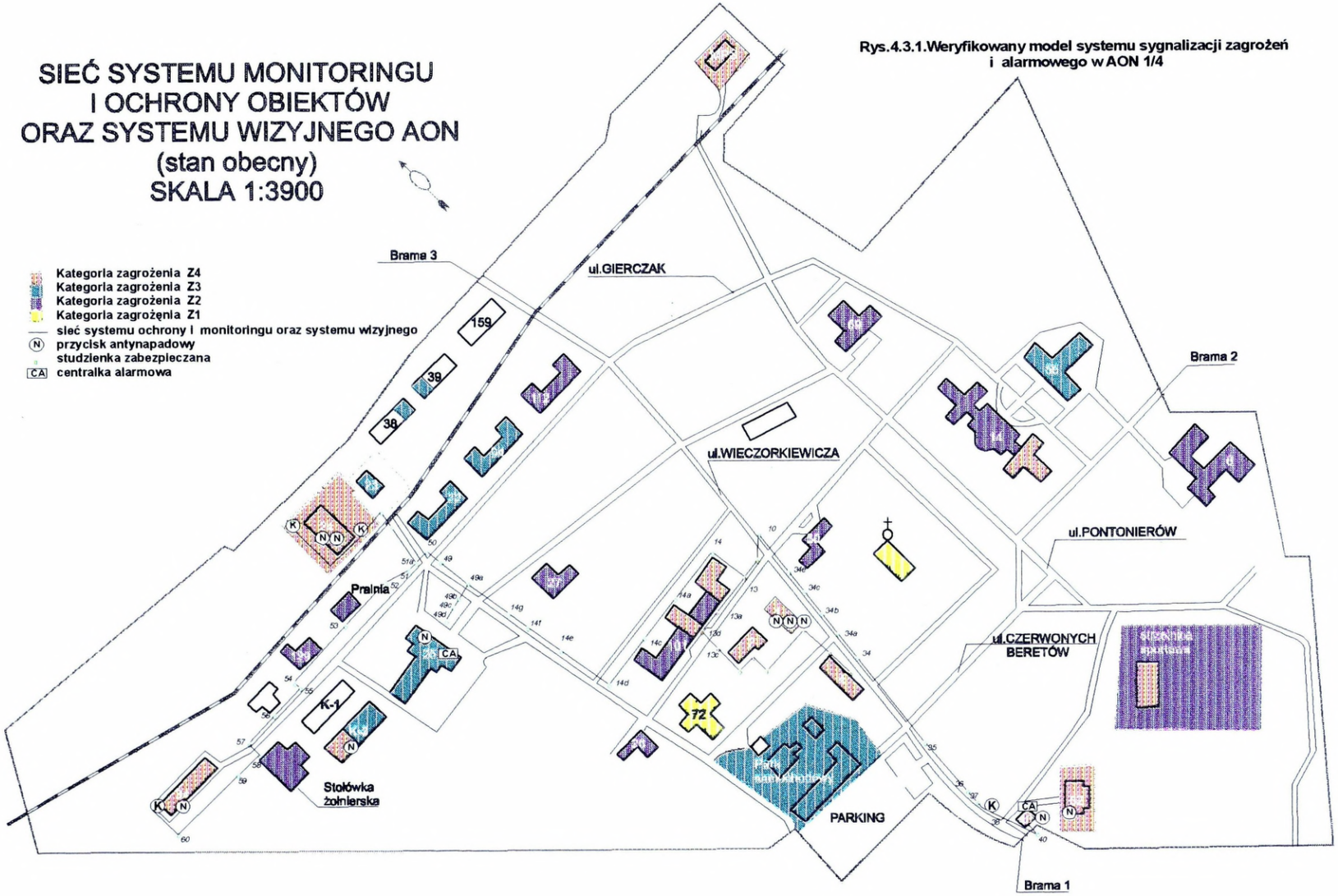
W celu dokonania weryfikacji modelu systemu sygnalizacji zagrożeń i alarmowego zagrożeń w AON załączono następujące rysunki[17]:

- Sieć systemu monitoringu i ochrony obiektów oraz systemu wizyjnego AON.
- Koncepcja sieci kablowej alarmowania służb dyżurnych w AON.
- Koncepcja sieci ochrony i monitoringu obiektów AON.
- Koncepcja sieci systemu wizyjnego AON.

[16] Metoda oceny została zaprezentowana prze autora podczas kursów dla rzeczoznawców Ogólnopolskiego Stowarzyszenia Producentów, Projektantów i Instalatorów Systemów Alarmowych.

[17] Bliższe informacje zawarte są w "Projekt Systemów Alarmowych Sygnalizacji Zagrożeń Akademii Obrony Narodowej" oraz „Bezpieczeństwo Obiektów Akademii Obrony Narodowej. Zapis problemów do zbadania i zaleceń dla projektowania zabezpieczenia technicznymi urządzeniami sygnalizacyjnymi i alarmowymi".

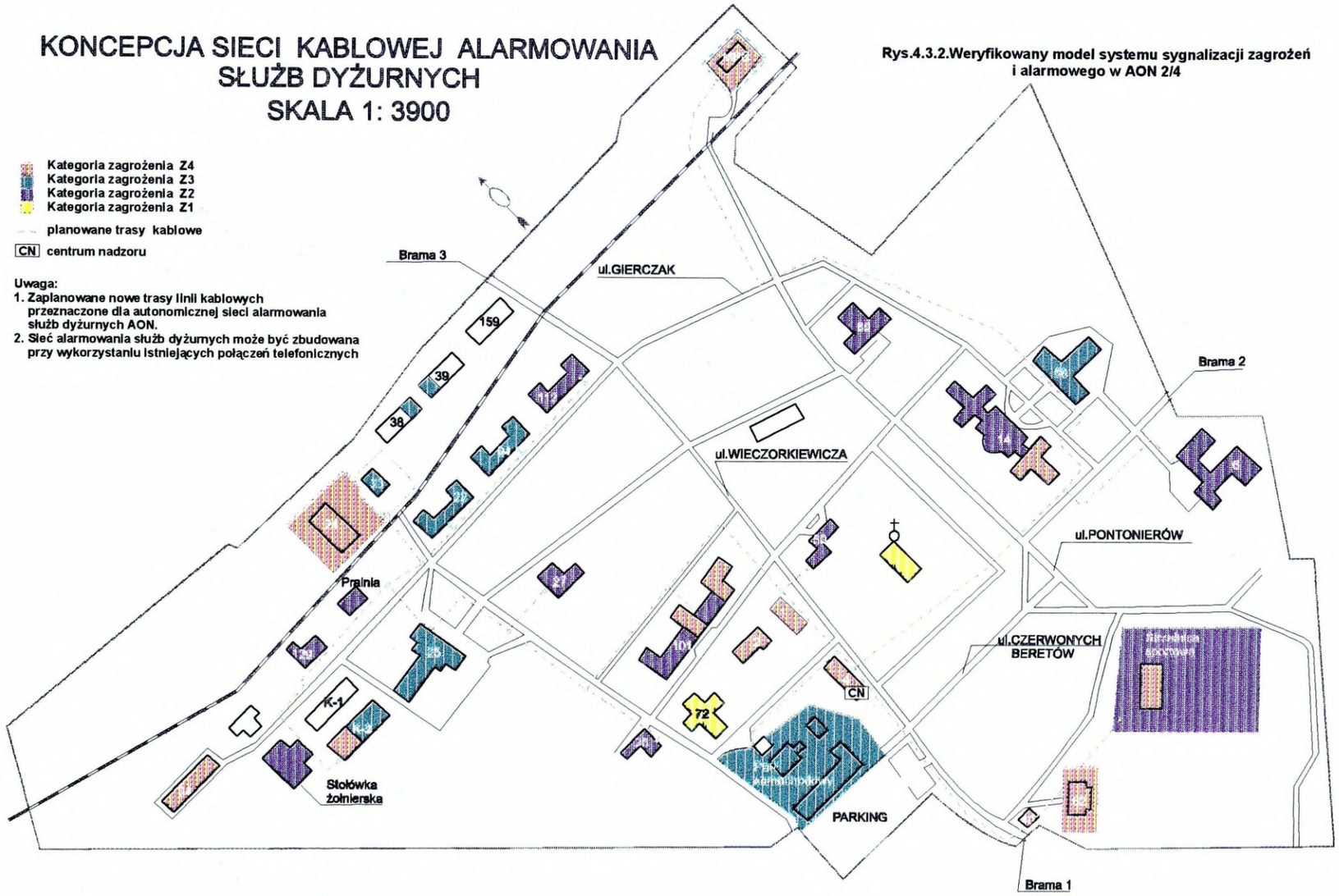
Rys.4.3.1.Weryfikowany model systemu sygnalizacji zagrożeń i alarmowego w AON 1/4



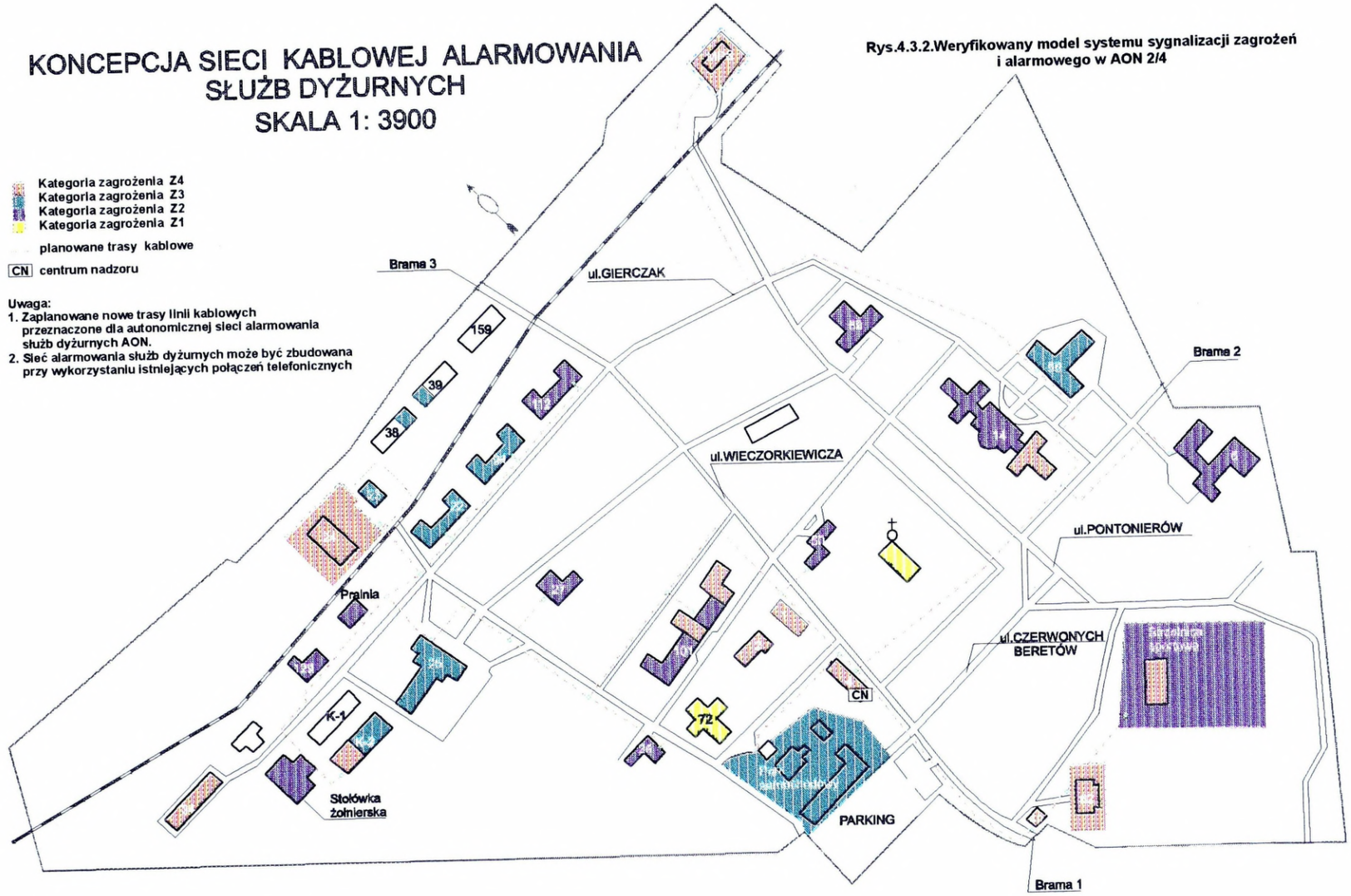
KONCEPCJA SIECI KABLOWEJ ALARMOWANIA SŁUŻB DYŻURNYCH SKALA 1: 3900

Kategoria zagrożenia Z4
Kategoria zagrożenia Z3
Kategoria zagrożenia Z2
Kategoria zagrożenia Z1
planowane trasy kablowe
CN centrum nadzoru

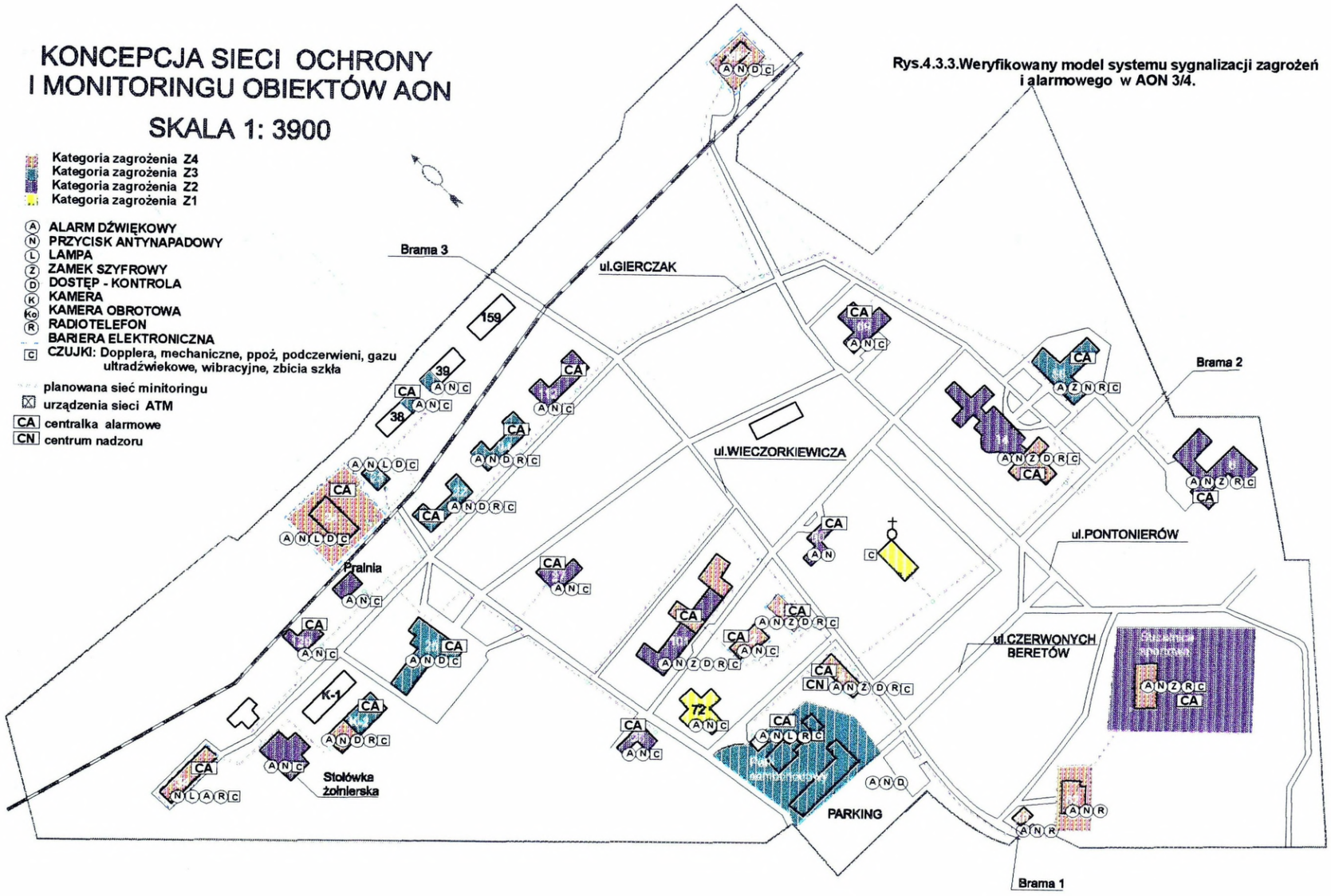
Uwaga:
1. Zaplanowane nowe trasy linii kablowych przeznaczone dla autonomicznej sieci alarmowania służb dyżurnych AON.
2. Sieć alarmowania służb dyżurnych może być zbudowana przy wykorzystaniu istniejących połączeń telefonicznych



Rys.4.3.2.Weryfikowany model systemu sygnalizacji zagrożeń i alarmowego w AON 2/4



Rys.4.3.2.Weryfikowany model systemu sygnalizacji zagrożeń i alarmowego w AON 2/4



Rys.4.3.3.Weryfikowany model systemu sygnalizacji zagrożeń i alarmowego w AON 3/4.

Prezentacja wyników badań

Tabela 4.3.2. Weryfikacja systemu sygnalizacji zagrożeń i alarmowego w AON

Lp	Grupa tematyczna	Podgrupa tematyczna	Wyszczególnienie elementu	Ocena maksymalna	Ocena uzyskana
1	2	3	4	5	6
1	CHARAKTERYSTKA OBIEKTU				
		1.1.Charakterystyka techniczno-organizacyjna		5	5
		1.2.Charakterystyka funkcjonalna		5	5
		1.3.Charakterystyka topograficzna		5	5
		1.4.Ograniczenia prawno-organizacyjne		5	4
		1.5.Ochrona fizyczna		5	4
		1.6.Ochrona techniczna		5	3
		1.7.Relacje wewnętrzne i zewnętrzne		5	3
		1.8.Otoczenie		5	5
		1.9.Zagrożenia		5	5
		1.10.Zakłócenia		5	2
2	ANALIZA ZAGROŻEŃ				
		2.1.Lista zagrożeń		5	5
		2.2.Słabe punkty		5	5
		2.3.Kierunki penetracji		5	5
		2.4.Kategoria zagrożonych wartości		5	5
		2.5.Poziom bezpieczeństwa		5	5
		2.6.Określenie klasy systemu		5	5
		2.7.Określenie klasy urządzeń		5	5
3	ŚRODKI NEUTRALIZACJI ZAGROŻEŃ				
		TECHNICZNE			
		3.1.Strefy ochrony			
			3.1.1.Strefa peryferyjna	5	3
			3.1.2.Strefa obwodowa	5	3
			3.1.3.Strefa wewnętrzna	5	5
			3.1.4.Strefa miejscowa	5	2
			3.1.5.Pułapki kryminalistyczne	5	0
		3.2.Ochrona techniczna			
			3.2.1.Elektroniczna	5	5
			3.2.2.Mechaniczna	5	5

1	2	3	4	5	6
			3.2.3.Elektro-mechaniczna	5	5
			3.2.4.Budowlana	5	5
		ORGANIZACYJNE 3.4.Ochrona fizyczna			
			3.4.1.Wymagania	5	5
			3.4.2.Procedury	5	5
			3.4.3.Nadzór	5	5
			3.4.4.Środki łączności i transportu	5	5
4	SYSTEMY TECHNICZNE I ORGANIZACYJNE				
		4.1.Systemy alarmowe			
			4.1.1.Włamania i napadu	5	5
			4.1.2.Pożaru	5	2
			4.1.3.Kontroli Dostępu	5	4
			4.1.4.Telewizji Użytkowej	5	5
			4.1.5.Ochrony zewnętrznej w tym mechaniczne	5	5
			4.1.6.Monitoringu	5	5
			4.1.7.Specjalne *za każdy system 1pkt	5	2
	Wybór alternatywny *	4.2.Technologia			
			4.2.1.Analogowa*	0	0
			4.2.2.Cyfrowa*	5	3
	Wybór alternatywny *	4.3.Autonomia i zdecentralizowane sterownie*	4.3.1.System autonomiczny	0	0
			4.3.2.Sterowanie automatyką zagrożeń	0	0
	Wybór alternatywny *	4.4.Integracja*	4.4.1.System zintegrowany	0	3
			4.4.2.Centrum nadzoru	0	4
			4.4.3.Wizualizacja procesów	0	3
			4.4.4.Sterowanie automatyką zagrożeń	0	0
	Wybór alternatywny *	4.5.Automatyzacja procesów zarządzania*	4.5.1.System BMS	5	0
			4.5.2.Centrum nadzoru	5	0
			4.5.3.Wizualizacja procesów	5	0

1	2	3	4	5	6
			4.5.4.Sterowanie automatyką zagrożeń	5	0
			4.5.5.Sterowanie systemami teletechnicznymi	5	0
			4.5.6.Sterowanie systemami technicznymi	5	0
5	SUMA PUNKTÓW		**Pmax**	**220**	
			Px		**170**

Na podstawie otrzymanych wyników oraz tabeli wzorcowej 4.3.1 projektowany system ochrony został zakwalifikowany do wysokiego poziomu technicznego P2=170 punktów.

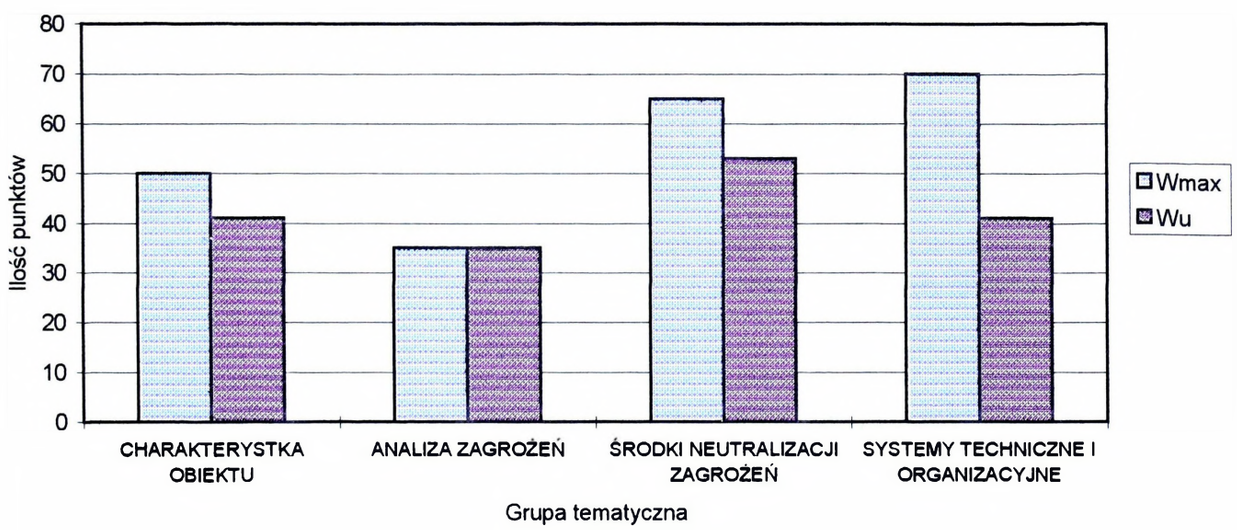
Wykorzystując wzór na sprawność systemu ochrony , uzyskano następujący wynik:

$$\eta = P2 / Pmax = 170/220 = 0,77$$

Stosując analogię urządzeń technicznych można stwierdzić, że sprawność zaprojektowanego systemu ochrony na potrzeby AON należy zaliczyć do średnich.

Systemy i urządzenia sprawne uzyskują poziom 0,7 - 0,9.

Wykres 4.3.1.Porównanie cech systemu weryfikowanego i modelowego



Wykres 4.3.1 pozwala porównać cechy projektowanego systemu ochrony dla AON z cechami systemu modelowego. Na wykresie Wmax oznacza wartość modelową (porównawczą), a Wu -wartość uzyskaną na podstawie przeprowadzonej weryfikacji. Pomimo otrzymania wysokiej oceny zaliczającej projektowany system ochrony do grupy P5, można wykazać, że największe braki opracowany projekt wykazuje w zakresie elementów charakteryzujących systemy techniczne i organizacyjne, występująca różnica dochodzi do blisko 30 punktów. Także środki neutralizacji zagrożeń są w niedostatecznym stopniu wykorzystane, różnica dochodzi do ponad 10 punktów, prawie identyczna sytuacja występuje przy określaniu charakterystyki obiektu. Natomiast osiągnięto doskonałe (identyczne) wyniki przy analizie zagrożeń.

W tabeli 4.3.3 autor zaprezentował wyniki weryfikacji systemu ochrony w ujęciu grup tematycznych charakteryzujących ten system.

Wyniki uzyskane w poszczególnych grupach Wu oraz wzorcowe Wmax (maksymalne do uzyskania) zostały następnie porównane na wykresach 4.3.2. i 4.3.3.

Tabela 4.3.3. Wyniki weryfikacji systemu ochrony obiektu

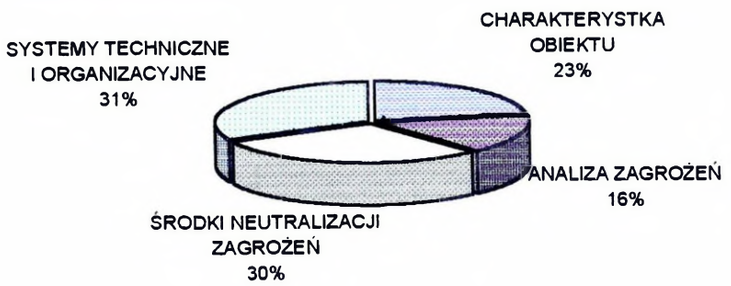
Lp	Grupa	Wmax	Wu
1	CHARAKTERYSTKA OBIEKTU	50	41
2	ANALIZA ZAGROŻEŃ	35	35
3	ŚRODKI NEUTRALIZACJI ZAGROŻEŃ	65	53
4	SYSTEMY TECHNICZNE I ORGANIZACYJNE	70	41

Wmax = wartość maksymalna porównawcza

Wu = wartość uzyskana z obliczeń

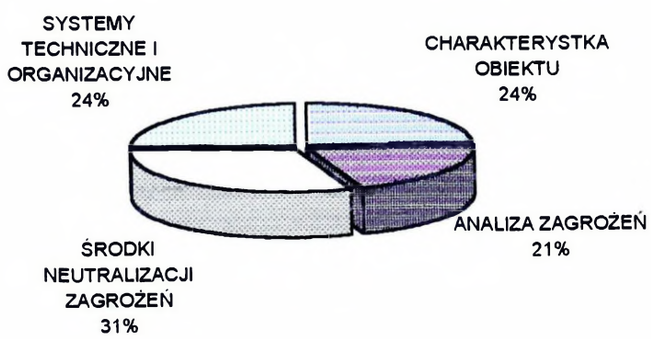
Wykresy 4.3.2 i 4.3.3 prezentują udział procentowy cech systemu ochrony zaprojektowanego i modelowego.

Wykres 4.3.2.Udział w % cech charakteryzujących normatywny system alarmowy



Z analizy wykresu 4.3.2 wynika, że największy nacisk w projekcie systemu ochrony dla AON położono na środki neutralizacji zagrożeń (31%), co potwierdza zawartość opracowania.

Wykres 4.3.3.Udział w % cech weryfikowanego systemu alarmowego dla AON



W modelowym opracowaniu systemu ochrony obiektu największy udział mają systemy techniczne i organizacyjne (31%) oraz środki neutralizacji zagrożeń (30%).

Na zakończenie należy podkreślić, że weryfikacji poddane zostały dwa opracowania, które oceniane pojedynczo osiągnęłyby znacznie gorsze wyniki.

Wnioski

Istotnym elementem przy formułowaniu modelu było zaprezentowanie po raz pierwszy metodologii budowy modelu systemu sygnalizacji zagrożeń i alarmowania oraz metody weryfikacji teoretycznych i funkcjonujących modeli.

Wprowadzenie do powszechnego użycia przez specjalistów tej metodologii umożliwi szeroką kontrolę i analizę oraz weryfikację opracowywanych i istniejących modeli systemów sygnalizacji zagrożeń i alarmowych na potrzeby obronności państwa.

Jednym z podstawowych wniosków zastosowania metodologii w praktyce jest zbudowanie na bazie opracowanych procedur modelu symulacyjnego tj. programu eksperckiego realizującego funkcjonowanie modelu na podstawie wprowadzonych danych oraz prezentującego wyniki symulacji w postaci wniosków do realizacji.

Konieczność opracowania w pełni automatycznego modelu symulacyjnego wykorzystującego multimedialne techniki komputerowe, przyczyni się do upowszechnienia wiedzy na temat ochrony obiektów wojskowych oraz dostępu osób zainteresowanych tym zagadnieniem. Ponadto zapotrzebowanie na tego typu model ochrony występuje zarówno ze strony projektantów, jak i decydentów zajmujących się systemami ochrony obiektów wojskowych.

Zaprezentowany model systemu alarmowego i sygnalizacji zagrożeń charakteryzuje się następującymi cechami:

- modułowość w zakresie budowy i wdrażania;
- skuteczność tworzenia i wdrażania modelu;
- obiektywizm - nie podlega trendom i modom;
- elastyczność - uwzględnia różne sytuacje decyzyjne;
- niezależność - od technologii i stosowanych technik;

- uniwersalność - można zbudować każdy system sygnalizacji i alarmowania i dokonać jego oceny;
- obniża ryzyko błędu;
- możliwość prowadzenia symulacji;
- możliwość dokonania weryfikacji zarówno istniejących, jak i planowanych systemów;
- zmniejszenie kosztów opracowania;
- wprowadzenie rachunku optymalizacyjnego kosztów inwestycji.

Z wyników weryfikacji wynika, że:

Zaprojektowany system ochrony obiektu na potrzeby AON nie jest w zbyt dopracowany od strony technicznej jak i organizacyjnej.

Porównując wyniki weryfikacji systemu ochrony zawartymi w tabeli 4.3.3 z wartościami maksymalnymi do uzyskania możemy stwierdzić, że:

- Obiekt chroniony nie został dostatecznie rozpoznany pod względem organizacyjno - funkcjonalnym i technicznym.
- Analiza zagrożeń została przeprowadzona prawidłowo.
- Zastosowane środki neutralizacji zagrożeń nie odpowiadają rzeczywistemu poziomowi zagrożeń, pomimo wysokiej oceny analizy zagrożeń.
- Zastosowane systemy organizacyjne i techniczne ochrony obiektu nie zaspokoją w pełni rzeczywistych potrzeb.
- Generalnie zaprojektowany system (z uwagami zawartymi w powyższych punktach zaliczony został do poziomu P5 wysokiej skuteczności technicznej i organizacyjnej ochrony obiektu.

Przez zastosowane metody weryfikacji na podstawie modelowego przebiegu projektowania systemu ochrony autor osiągnął zamierzony cel i skutecznie zweryfikował opracowany projekt systemu sygnalizacji zagrożeń i alarmu. Na podstawie dotychczasowych rozważań można stwierdzić, że zastosowana metoda weryfikacji oraz wzorcowy model systemu alarmowego i sygnalizacji zagrożeń opracowany na bazie metodologii spełniła podstawowe cele rozprawy:

- umożliwiła dokonanie analizy zagrożeń wywierających wpływ na poziom bezpieczeństwa obiektów należących do struktury obronnej państwa na bazie zweryfikowanego modelu;
- pozwoliła określić techniczno – organizacyjne środki neutralizacji zagrożeń;

- pozwoliła określić wymagania techniczne i funkcjonalne dla systemów sygnalizacji zagrożeń i alarmowych dla weryfikowanego modelu;
- umożliwiła ocenę zastosowanej metody projektowania rzeczywistego modelu systemów sygnalizacji zagrożeń i alarmowych;
- pozwoliła wskazać kierunki poprawy i opracowanie dalszych kroków dla podniesienia bezpieczeństwa weryfikowanego modelu systemu ochrony obiektu wojskowego;
- umożliwiła uwzględnienie wymagań krajowych i NATO w zakresie ochrony obiektów wojskowych.

ZAKOŃCZENIE

Istnieje ścisły związek pomiędzy stanem bezpieczeństwa powszechnego a zagrożeniami systemu obronnego państwa, wynikający z zagrożeń społecznych, ekonomicznych, psychologicznych, historycznych, etnicznych, językowych, terytorialnych, wyznaniowych, ekologicznych i wojskowych.

Jednym z podstawowych elementów fizycznego przeciwstawiania się tym zagrożeniom oraz ich przewidywania, analizy i diagnozy są systemy ochrony obiektu.

Systemy ochrony obiektu zapobiegają i neutralizują potencjalne zagrożenia oraz podnoszą ogólny stan bezpieczeństwa obiektów zaliczanych do systemu obronnego państwa.

W celu spełnienia norm oraz podniesienia wymagań niezbędne są odpowiednie procedury modelowania systemu ochrony. Dotychczasowe rozwiązania organizacyjno – techniczne nie spełniają wymagań ochrony obiektów systemu obronnego państwa, pomimo ogólnej dostępności do światowych osiągnięć technologicznych w tym zakresie.

Do zbudowania modelu systemu ochrony została opracowana oryginalna metodologia projektowania systemu ochrony obiektu. W modelu powiązano stronę organizacyjno-techniczną rozwiązania projektowego z nakładami ekonomicznymi przeznaczonymi na jego budowę. Na podstawie tak przeprowadzonej procedury można określić dane nie tylko o szczegółach ochrony obiektu, ale także jego poszczególnych stref, zarówno wewnętrznych, jak i zewnętrznych.

Takie funkcjonalne ujęcie modelu pozwala optymalizować nakłady finansowe, przy jednoczesnym zachowaniu innowacyjnej strony technicznej ochrony obiektu.

Zaprezentowany model systemu ochrony został opracowany przede wszystkim na potrzeby ochrony obiektów wojskowych. Jego praktycznym zadaniem jest weryfikacja, modernizacja oraz tworzenie nowych rozwiązań systemów ochrony, szczególnie w realizacji procesu integracji struktur obronnych Polski ze strukturami NATO.

Opracowana unikalna metodologia tworzenia modelu systemu ochrony obiektów poddaje się łatwo modyfikacji zależnie od konkretnych potrzeb. Model ochrony obiektów ma szereg cech umożliwiających szerokie zastosowanie w systemach ochrony obiektów wojskowych oraz umożliwia jego symulację komputerową z wykorzystaniem wszelkich technik w tym zakresie, a w szczególności komputerowe modelowanie optymalizacyjne.

Elementem zamykającym proces modelowania jest weryfikacja modelu systemu ochrony obiektu. Przeprowadzony proces weryfikacji potwierdził skuteczność oceny modelu teoretycznego oraz ujawnił niedociągnięcia systemów dotychczas budowanych - bez stosowania symulacji komputerowej.

Zastosowana procedura weryfikacyjna umożliwia sprawdzenie skuteczności i prawidłowości oraz staranności przeprowadzonej analizy zagrożeń, poziomu bezpieczeństwa obiektu, określenia środków organizacyjno – technicznych oraz kierunków i środków niezbędnych dla podniesienia bezpieczeństwa chronionego obiektu.

Zamierzony główny cel badawczy rozprawy doktorskiej został osiągnięty ponieważ:

- określone przez autora uwarunkowania umożliwiły przedstawienie modelu systemu ochrony obiektu (sygnalizacji zagrożeń i alarmowania) na potrzeby obronne państwa;
- opracowane procedury metodologii budowy modelu systemu ochrony (alarmowego i sygnalizacji zagrożeń) obiektu umożliwiły weryfikację rzeczywistego modelu.

Również cele szczegółowe, wynikające z głównego celu badawczego zostały spełnione ponieważ:

- dokonano analizy zagrożeń wywierających wpływ na poziom bezpieczeństwa obiektów należących do struktury obronnej państwa;
- określono wymagania techniczne i funkcjonalne systemów alarmowych i sygnalizacji zagrożeń ze szczególnym uwzględnieniem potrzeb obronnych państwa;
- oceniono istniejące metody projektowania systemów alarmowych i sygnalizacji zagrożeń na potrzeby obronne państwa;
- opracowano model systemu alarmowego i sygnalizacji zagrożeń ze szczególnym uwzględnieniem potrzeb obronnych państwa;

a także dodatkowo:

- wprowadzono procedury weryfikacji modelu systemu alarmowego i sygnalizacji zagrożeń, wprowadzając pojęcie poziomu skuteczności technicznej i organizacyjnej systemu alarmowego.

Autor dokonał weryfikacji modelu przez porównanie z rzeczywistym system alarmowym obiektu należącym do struktury obronnej państwa i stwierdza, że otrzymane wyniki potwierdziły słuszność przyjętych rozwiązań.

Z pracy wynikają ogólne wnioski do dalszych prac projektowych i badawczych:

- istnieje konieczność opracowania modelu matematycznego dla podniesienia stopnia obiektywności procesu weryfikacji modelu systemu alarmowego;
- na bazie wypracowanego modelu matematycznego należy opracować oprogramowanie komputerowe z cechami multimedialnymi;
- opracowane oprogramowanie multimedialne powinno zwiększyć stopień automatyzacji procesów weryfikacyjnych i analitycznych modelu systemu

alarmowego i będzie stanowić narzędzie dla osób zajmujących się problematyką bezpieczeństwa obiektów, a w szczególności wojskowych;

- oprogramowanie powinno posiadać także cechy:
- modułowej rozbudowy o specjalistyczne bazy danych pomocnych projektantowi tj. grupy urządzeń, producenci, dane techniczne, zakres zastosowań, ceny;
- uwzględniać normy prawne i zalecenia w zakresie systemów alarmowych i sygnalizacji zagrożeń;
- wspomagać proces projektowania poprzez weryfikowanie i analizę jego przebiegu;
- posiadać moduł kalkulacyjny umożliwiający optymalizowanie kosztów realizacji systemu alarmowego i sygnalizacji zagrożeń;
- posiadać dla opcji ogólnej cechy komercyjne umożliwiające rozprowadzanie wśród szerokiej rzeszy odbiorców zajmujących się problematyką bezpieczeństwa.

Z przeprowadzonych rozważań i oceny autora oraz obecności Polski w strukturach NATO wynika, że w niedalekiej perspektywie, klasa ochrony obiektów wojskowych będzie porównywalna ze standardami państw członków NATO, co jeszcze bardziej podniesie walory użytkowe badań zawartych w rozprawie.

Autor jest przekonany, że zbudowany model systemu ochrony (alarmowy i sygnalizacji zagrożeń), jak też cała rozprawa doktorska, mogą stanowić wydatną pomoc w sferze teoretycznej jak i praktycznej podczas budowy systemów standaryzujących ochronę obiektów wojskowych , jak również wskazać kierunki dalszych badań i prac w celu podniesienia ich jakości i efektywności.

WYKAZ TABEL

Nr	Opis	Str
2.3.1.	Niektóre rodzaje przestępstw stwierdzonych w latach 1989-1994	42
2.3.2.	Przestępczość w okresie styczeń- styczeń 1997/1998- dane ogólnokrajowe	42
2.3.3.	Kategorie wybranych przestępstw w wojsku	46
4.3.1.	Określenie poziomu technicznego systemu	150
4.3.2.	Weryfikacja systemu alarmowego i sygnalizacji zagrożeń w AON	155
4.3.3.	Wyniki weryfikacji systemu alarmowego	158

WYKAZ RYSUNKÓW I SCHEMATÓW

Nr Rysunki	Opis	Str
2.1.1.	Ogólny schemat systemu obronnego państwa	22
2.1.2.	Struktura systemu kierowania siłami zbrojnymi (w czasie pokoju)-wariant	23
2.1.3.	Struktura systemu kierowania siłami zbrojnymi (w czasie wojny)- wariant	24
2.1.4.	Ogólna struktura podsystemu kierowania obronnością państwa	28
2.1.5.	Schemat podsystemu kierowania obroną państwa (wariant)	32
2.2.1.	Systemy kierowania reagowaniem kryzysowym	37
2.2.2.	Struktura i obsada stanowiska kierowania reagowaniem kryzysowym MON	38
3.2.1.	System ochrony informacji niejawnych w resorcie obrony narodowej	54
3.2.2	Rodzaje systemów ochrony obiektów (wariant)	58
3.2.3.	Struktura organizacyjna systemu alarmu włamania i napadu	59
3.2.4.	Struktura organizacyjna systemu sygnalizacji pożaru	63
3.2.5.	Elementy systemu kontroli dostępu	64
3.2.6.	Główne elementy systemu telewizji użytkowej	65
3.2.7.	Prezentacja modelu upraszczającego zarządzanie i procesy automatyzacji obiektu	69
3.2.1.1.	Części składowe systemu SAiWN	71
4.1.1.	Fazy procesu projektowania systemu alarmowego	94
4.1.2.	Przebieg procesu projektowania systemu ochrony obiektu ujęciu praktycznym	96
4.1.3.	Przykład adresowego wielofunkcyjnego systemu alarmowego	100
4.1.4.	Model optymalizacji kosztów przy projektowaniu systemów ochrony obiektu	101
4.1.5.	Zależność wyboru rozumowania projektanta stosującego koncepcję tradycyjną i Nadlera a kosztami zastosowanej techniki zabezpieczeń	102
4.1.1.1.	Schemat procesu ustalania powiązań za pomocą analizy wartości	109
4.1.1.2.	Czynniki decydujące o wyborze elementów systemu ochrony - schemat badawczy analizy wartości organizacji	110
4.1.2.1.	Czynniki wpływające na koncepcję zabezpieczenia obiektu	111
4.1.2.2.	Analiza poziomu ryzyka (wariant)	114
4.1.2.3.	Podział stref ochrony obiektu	115
4.1.2.4.	Czynniki kształtujące stan zagrożenia obiektu chronionego	117
4.2.1.	Organizacja budowy modelu (wariant)	121
4.2.2.	Konstrukcja modelu – wzorca (wariant)	122
4.2.3.	Rozmieszczenie i powiązanie elementów modelu systemu ochrony obiektu wojskowego (wariant)	128

4.2.4.	Szczegół "A"- rodzaje ochrony zewnętrznej obiektu wojskowego	130
4.2.5.	Prezentacja strefy ochrony wewnętrznej w modelu systemu ochrony obiektu wojskowego (wariant) z rys.4.2.3 – szczegół „B”	131
4.2.6.	Przykładowy model przestrzenny systemu ochrony obiektu wojskowego (wariant)	132
4.2.7.	Typy grafów i macierzy oddziaływań	146
4.3.1.	Weryfikowany model rzeczywisty systemu alarmowego i sygnalizacji zagrożeń w AON ¼	151
4.3.2.	Weryfikowany model rzeczywisty systemu alarmowego i sygnalizacji zagrożeń w AON 2/4	152
4.3.3	Weryfikowany model rzeczywisty systemu alarmowego i sygnalizacji zagrożeń w AON ¾	153
4.3.4.	Weryfikowany model rzeczywisty systemu alarmowego i sygnalizacji zagrożeń w AON 4/4	154
Schematy		
1.1.	Przebieg procesu badawczego	10
2.3.1.	Wpływ zagrożeń i ich relacje na funkcjonowanie systemu obronnego państwa	39
3.2.2.1.	System ochrony zewnętrznej ogrodzeniowy – elektromechaniczny naciągowy	79
3.2.2.2.	System ochrony zewnętrznej ogrodzeniowy – wstrząsowy	80
3.2.2.3.	Zasada działania bariery mikrofalowej	81
3.2.2.4.	Nadajnik mikrofalowy systemu ochrony zewnętrznej obwodowej	81
3.2.2.5.	Kompleksowy system ochrony ogrodzenia reagujący na zbliżenie intruza	82
3.2.2.6.	Montaż czujnika akustycznego na metalowej siatce	82
3.2.2.7.	Potrójna strefa ochrony zewnętrznej oddzielona ogrodzeniem z nadzorem systemu alarmowego	83
3.2.2.8.	Ochrona strefy zewnętrznej za pomocą systemu ogrodzeniowego i specjalnych drutów kolczastych uniemożliwiających podejście do ogrodzenia	83
3.2.2.9.	Plan instalacji systemu zbliżeniowego ochrony kas, sprzętu, wyposażenia biur i pojazdów	84
3.2.2.10.	System wizyjny z wykorzystaniem analizy ruchu w warunkach nocnych (obraz na monitorze)	84
4.1.1.	Ogólny schemat blokowy procesu projektowania systemu ochrony obiektów...	87
4.2.1.	Metodologia tworzenia modelu systemu ochrony obiektu cz.1	123
4.2.2.	Metodologia tworzenia modelu systemu ochrony obiektu cz.2	124
4.2.3.	Metodologia tworzenia modelu systemu ochrony obiektu cz.3	125

WYKAZ WYKRESÓW I MODELI GRAFICZNYCH

Nr	Opis	Str
Wykresy		
2.3.1.	Dynamika wybranych czynów przestępczych w latach 1989-94	42
2.3.2.	Udział % wybranych czynów przestępczych w okresie 1997/1998	43
2.3.3.	Przestępczość w wojsku 1997/98	46
4.3.1.	Porównanie cech systemu weryfikowanego i modelowego	157
4.3.2.	Udział w % cech charakteryzujących normatywny system alarmowy	159
Nr	Opis	Str
4.3.3.	Udział w % cech weryfikowanego systemu alarmowego dla AON	159
Modele		
4.2.1/9	Model podziału stref ochrony obiektu (wariant)	134
4.2.2/9	Model funkcjonalny systemu ochrony obiektu (wariant)	135

4.2.3/9 Model podziału organizacyjnego stref ochrony wewnętrznej w obiekcie (wariant)..... 136
4.2.4/9 Model ochrony obiektu systemem alarmowym włamania i napadu (wariant)..... 137
4.2.5/9 Model ochrony obiektu systemem kontroli dostępu (wariant)..... 138
4.2.6/9 Model ochrony obiektu systemem telewizji użytkowej (wariant)..... 139
4.2.7/9 Model ochrony obiektu systemem sygnalizacji pożaru (wariant)..... 140
4.2.8/9 Model ochrony obiektu przez zintegrowany systemem ochrony obiektu (wariant)..... 141
4.2.9/9 Model organizacji zintegrowanego systemu ochrony obiektu (wariant)..... 142

SPIS ZAŁĄCZNIKÓW

w odrębnym opracowaniu

Nr	Opis	Str
2.1.	Wyciąg z Konstytucji Rzeczypospolitej Polskiej zawierający artykuły dotyczące obronności państwa.....	5
2.2.	Zestawienie miejsc występowania różnych zagrożeń na terenie Polski.....	10
2.3.	Możliwe stany w stosunkach międzypaństwowych i międzynarodowych (wariant).....	11
2.4.	Planowanie działań NATO na wypadek zagrożeń cywilnych.....	13
2.5	Zagrożenie obiektów wojskowych ze strony zorganizowanej przestępczości....	22
2.6.	Terroryzm nowe oblicze zagrożenia świata.....	24
3.1.	Systemy Alarmowe Włamania i Napadu (SAWiN).....	26
3.2.	Systemy alarmowe sygnalizacji pożaru.....	46
3.3.	Systemy Kontroli Dostępu.....	52
3.4.	Systemy Telewizji Użytkowej (CCTV).....	62
3.5.	Systemy ochrony zewnętrznej.....	82
3.6.	Systemy budowlane, mechaniczne i elektromechaniczne.....	96
3.7.	Systemy i urządzenia monitoringu alarmowania i sygnalizacji zagrożeń.....	102
3.8.	Zintegrowane Systemy Alarmowania i Sygnalizacji Zagrożeń.....	110
3.9.	Zintegrowane systemy zarządzania automatyką budynków.....	114
3.10.	Systemy ewakuacyjne i antypanikowe.....	117
4.1.	Sieć telekomunikacyjna AON.....	129
4.2.	Sieć systemu monitoringu i ochrony obiektów oraz systemu wizyjnego AON...	130
4.3.	Koncepcja sieci światłowodowych AON.....	131
4.4.	Koncepcja sieci kablowej alarmowania służb dyżurnych.....	132
4.5.	Koncepcja sieci ochrony i monitoringu obiektów AON.....	133
4.6.	Koncepcja sieci systemu wizyjnego AON.....	134
4.7.	Koncepcja rozbudowy sieci radiowej AON.....	135

BIBLIOGRAFIA

1. Balcerowicz B., *Strategia wojenna, strategia militarna w warunkach współczesnej Polski*, AON, Warszawa 1993
2. Balcerowicz B., *Strategiczna obrona Rzeczpospolitej Polskiej lat dziewięćdziesiątych*, AON, Warszawa 1997
3. Balcerowicz B., *Wybrane problemy obronności państwa – materiał studyjny*, AON, Warszawa 1997
4. Bednarz M., Robekowski Z., *Rozwój systemu obronnego (Prognozowanie i planowanie obronne),* AON, Warszawa 1998
5. *Bezpieczeństwo obiektów Akademii Obrony Narodowej. Zapis problemów do zbadania i zaleceń dla projektowania zabezpieczenia technicznymi urządzeniami sygnalizacyjnymi i alarmowymi,* ekspertyza opracowana pod kierunkiem Nowicki Z. T., Warszawa 1996
6. Bielecki R., *Pustynna burza*, Bellona, Warszawa 1991
7. Boratyn D., *Access 97,* Croma,Wrocław 1997
8. Borzymek M., Kuczkowski W. referat pt.: *Ochrona obiektów bankowych - aktualne tendencje i wnioski dla projektantów*, I Ogólnopolska Konferencja Techniczna Elektronicznych Systemów Ochrony Mienia i Osób OSPPiISA, Brok n/Bugiem 22-23 maja 1998
9. *Catalogue Aritech Europe*
10. Ciszewski J., *Zasady projektowania instalacji sygnalizacji pożarowej*, CN-BOP, firex Warszawa 1996
11. Derfler F., Freed L., *Jak działają sieci,* PWN, Warszawa 1995
12. Diem W., *Ochrona przed włamaniem,* Muza S.A., Warszawa 1998
13. Drukheim E., *Zasady metody socjologicznej*, Warszawa 1968
14. Dworecki S., Kęsoń T., Kalisz M., *Współczesne konflikty zbrojne. Aspekt prognostyczny*, AON RCSS, Warszawa 1988
15. Dworecki S., *Od konfliktu do wojny*, BUWIK, Warszawa 1996
16. Dyrda wykład PZSOP, *Psychospołeczne problemy zagrożenia bezpieczeństwa*, AON, Warszawa 1998
17. *Dyrektywa bezpieczeństwa ACE (Zjednoczonego Dowództwa Europejskiego) nr 70-1*, NATO jawne, 1997
18. *Equipment Catalogue. Computar CCTV 1998-1999*

19. European Committee for Electrotechnical Standardization (SENELEC). Technical Committee 79; Alarm Systems, *Detailed work program prepared by the Secretary of TC79*, 20/01/1998
20. Friedl W., *Praxis der industriellen Sicherungstechnik*, Resch Verlag KG 1990
21. Fuhrmann H., *Gefahrenmeldesysteme. Technik und Strukturen*, Hüthig Buch GmbH, Heidelberg 1992
22. Gąsiorek K., Skobel W., Berliński T., *Współdziałanie terenowych organów administracji wojskowej z organami administracji rządowej i samorządowej w realizacji zadań operacyjno-obronnych*, AON, Warszawa 1998
23. Gąsiorek K., Skobel W., *Rola i zadania województwa w systemie obronnym państwa w czasie pokoju, zagrożenia (kryzysu) i wojny*, AON, Warszawa 1998
24. Gearty C., *Terroryzm*, Prószyński i S-ka, Warszawa 1998
25. *General Security Concept*, IBCOL Security Division, Aug./93
26. Harke W., Waneck P., *Gebäude-Management-Systeme*, Hüthig 1997
27. Hoffman B., *Oblicza terroryzmu*, Bertelsmann Media Sp. z o.o., Warszawa 1999
28. Hołyst B. referat pt.:*Ocena bezpieczeństwa w Polsce* - Konferencja SECUREX'98
29. Hołyst B., *Kryminologia*, Warszawa 1994
30. *Inteligentny budynek. Integracja systemów.* III Ogólnopolska Konferencja, materiały konferencyjne + suplement, Raport, 6-7 maja, 1998 Wrocław
31. *Internet*, Wydawnictwo Pascal, 1996
32. Kitler W., *Obrona narodowa. Konieczność nowego podejścia*, Myśl Wojskowa 4/1997, Warszawa 1997
33. Komański A., Dworecki S., Piedziuk E., *Perspektywiczny model systemu obronnego państwa "KRAJ"* , AON, Warszawa 1993
34. Komenda Główna Policji - *Dane statystyczne luty 1998*
35. Konferencja Branżowa, *Branża security w Polsce - stagnacja czy rozwój?*, zbiór referatów, Warszawa 26-27.10.1995
36. Konferencja, *Polska krajem bezpiecznym...? Branża zabezpieczeń w programie zapobiegania przestępczości*, zbiór referatów, Warszawa 24-25.10.1996, VI Ogólnopolska Wystawa Systemów Ochrony GARDA'96
37. Koziej S., Biedrzycki M., *Ministerstwo Obrony Narodowej jako organ kierowania obronnością państwa*, Myśl Wojskowa 1/1997, Warszawa 1997
38. Koziej S., *Kierowanie obroną narodową Rzeczypospolitej Polskiej*, DBM MON, Warszawa 1996

39. Koziej S., *Podstawy sztuki wojennej*, AON, Warszawa 1992
40. Koziej S., *Polska doktryna wojenna i jej modyfikacja w obliczu integracji z NATO*, DBM MON, Warszawa 1996
41. Koziej S., Wołkowicz F. *Podstawowe założenia polityki bezpieczeństwa i strategii obronnej*, AON, DSO MON, Warszawa 1998
42. Krauze M. *Wojskowe aspekty współczesnych zagrożeń ekologicznych,*AON, Warszawa 1990
43. Krauze M., *Planowanie i współpraca w sytuacjach zagrożeń według poglądów NATO*, AON, KSOŁ-96, Warszawa 1997
44. *Kurzanleitung für Projektierung von Brandmeldeanlagen effeff, 1997*
45. Laszczkowski Cz., *Kształtowanie bezpieczeństwa narodowego RP*, BBN, Warszawa 1993
46. Magazyn komputerowy, *Chip*, zbiór numerów z 1997/98
47. Marczak J., Dworecki S., Piedziuk E., Duda W., *Operacyjne przygotowanie obszaru kraju do obrony*, Wiedza Obronna nr 2/181, Warszawa 1997
48. *Materiały szkoleniowe efefeff 1997/98*
49. Materiały z międzynarodowego sympozjum – *Rozwój techniki wojskowej*, AMW, Gdynia 1996
50. Michalak J., *Ostrzeganie i alarmowanie ludności*, AON, US OCK, Warszawa 1998
51. *Microsoft Office 97. Szybki kurs*, Medium 1998
52. Mielczarek W., *Szeregowe interfejsy cyfrowe*, Helion 1993
53. Nowicki T. Z., *Bank wobec przemocy. Poradnik dla personelu banków i pracowników ochrony*, Agencja Wydawnicza i Marketingowa MEDIABANK S.A.,Warszawa 1997
54. Nowicki Z. T., *Alarm o przestępstwie*, Towarzystwo Naukowe Organizacji i Kierownictwa "Dom Organizatora", Toruń 1997
55. Nowicki Z. T., *Jak chronić?*, BWG 1994
56. Nowicki Z. T., *Ochrona osób i mienia,* TNOiK, Toruń 1999
57. Nowicki Z. T., *Ochrona osób i mienia. Suplement,* TNOiK, Toruń 1999
58. *Ochrona zbiorów publicznych*, Informator nr 5, Ośrodek Ochrony Zbiorów Publicznych, Warszawa 1993
59. Pawłowski J., Marczak J., *O obronie militarnej Polski przełomu XX-XXI w.*, Bellona, Warszawa 1995
60. Pawłowski J., Tarasiuk B. *Polski model kierowania obronnością państwa*, AON, Warszawa 1997
61. Piedziuk E., *Systemy alarmowe sygnalizacji zagrożeń*, AON, Warszawa 1998

62. Pieter J., *Z zagadnień pracy naukowej*, Zakład Narodowy im. Ossolińskich – Wydawnictwo, Wrocław 1974
63. Pokruszyński W. i in., *System bezpieczeństwa publicznego Polski,* AON, Warszawa 1995
64. Prac pod redakcją naukową prof. dr hab. Czesława Grzeszczaka, *Vademecum Agenta Ochrony i Detektywa*, Wydawnictwa Crimen s.c., Warszawa 1996
65. Praca zbiorowa pod kier. Balcerowicza B., *Przygotowanie i prowadzenie wojny obronnej przez Polskę po 2000 roku. "Kappa"*, AON, Warszawa 1996
66. Praca zbiorowa pod kier. Piedziuka E., *Urządzenia i systemy łączności na potrzeby kierowania obronnością i bezpieczeństwem państwa*, AON, Warszawa 1996
67. Praca zbiorowa pod kierunkiem Z. Michnowskiego, *Podstawy organizacji zarządzania i technologii w budownictwie*, Arkady, Warszawa 1985
68. Praca zbiorowa pod redakcją A.Stabryły i J.Trzcienieckiego, *Organizacja i zarządzanie. Zarys problematyki*, PWN, Warszawa 1986
69. Praca zbiorowa, *Aspekte der Sicherungstechnik*, Kriminalistik Verlag GmbH, Heidelberg 1989
70. Praca zbiorowa, *Zagrożenia przestępczością pospolitą oraz sposoby i środki jej neutralizacji. Zeszyt 8, Przewodnik Rzeczoznawcy,* OSPPiISA Warszawa 1995
71. *Proces weryfikacji urządzeń i systemów zabezpieczenia i ochrony na tle obowiązujących kryteriów normatywnych.* Zeszyt 5, Przewodnik Rzeczoznawcy OSPPiISA Warszawa 1994
72. *Produktsliste 98. Brandmeldesysteme, Einbruchmeldesysteme, Zutrittskontrollsysteme, Türöffnersysteme effeff*
73. *Projekt Systemów Alarmowych Sygnalizacji Zagrożeń Akademii Obrony Narodowej*, opracowanie pod kierunkiem Piedziuk E., AON, Warszawa 1998
74. Radziejewski R., *Ochrona osób. Poradnik dla każdego*, Wydawnictwo PAW, Warszawa 1997
75. Regan G., *Błędy militarne*, VASCO, Warszawa 1992
76. Rehborn K., *Praxis der Alarmanlagen*, Karamanolis Verlag, München 1985
77. *Richtlinien für automatische Brandmeldeanlagen. Planung und Einbau.* 1993
78. *Richtlinien für Einbruchmeldeanlagen. Planung und Einbau, VdS 2311 12/93 (01)*, Verband der Sachversicherer e.V. Köln
79. Ruff H., *Zabezpieczenie wyjść awaryjnych i drzwi ratunkowych na drogach ewakuacyjnych*, Referat na sympozjum Securex'96
80. Rusin M., *Systemy transmisji*, WKŁ, Warszawa 1990
81. Rusin M., *Wizyjne przetworniki optoelektroniczne*, WKŁ, Warszawa 1990

82. Ryczer A., Cieślak W., *Systemy alarmowe włamania i napadu,* Inteligentny budynek. Raport 1997/98
83. Santarek S., Strzelczak K., *Elastyczne systemy produkcyjne*, WNT, Warszawa 1989
84. Sawicki L., *Przygotowanie organizacyjno-mobilizacyjne układu pozamilitarnego systemu obronnego państwa*, AON, DSO MON, Warszawa 1998
85. Schiffel P Dr., *Elektronische Sicherungstechnik*, Richard Boorberg Verlag Stuttgart München Hannover 1988
86. Schmidhäusler F., *Zutrittskontrolle richtig planen*, Hüthig 1995
87. *Schulungsunterlagen effeff. Materiały szkoleniowe*. Februar/Luty 1998"
88. Serafin K., *Nowoczesne komputerowe systemy kontroli dostępu*, opracowanie, Warszawa 1996
89. *Sicherheit. Ein Urbedürfnis als Herausforderung für die Technik*, Bachmann Ch., Herausgegeben zum 50jährigen Bestehen der Cerberus AG, Männedorf/Schweiz 1991
90. *Sicherundsrichtlinien für Gäschäfte und Betriebe*, VdS 2333 08/93 (02), Verband der Sachversicherer e.V. Köln
91. *Sicherundsrichtlinien für Haushalte (SH) - Einbruchdiebstahl* -, VdS 691 11/95 (03), Verband der Sachversicherer e.V. Köln
92. Siemens E., *Handbuch Sicherungstechnik. Technische Hilfen für denAnwender in Industrie und Behörden*, Kriminalistik Verlag GmbH, Heidelberg 1993
93. Sienkiewicz P. – red. nauk., *Wystarczalność obronna*, Bellona, Warszawa 1996
94. Sienkiewicz P., *Analiza systemowa – podstawy i zastosowania*, Bellona, Warszawa 1994
95. Sienkiewicz P., *Inżynieria systemów*, Wydawnictwo MON, Warszawa 1983
96. Sienkiewicz P., red. nauk., *Wystarczalność obronna*, Bellona, Warszawa 1996
97. Sławik K., *Patologia w III Rzeczypospolitej*, Katowice 1994,
98. *Sondernummer zum Thema Zutrittskontrolle*, Protector, August 1992
99. Springer G. (Hrsg.), *SILEX. Lexikon der Sicherungstechnik*, Hüthig GmbH, Heidelberg 1994
100. Steinbrink B., *Multimedia u progu technologii XXI wieku,*Robomatic 1993
101. Stoner J., Wankel Ch., *Kierowanie*, PWN, Warszawa 1994
102. Stoner James A.F., Carles Wankel, *Kierowanie*, PWE, Warszawa 1994
103. Störmer W., *Elektronische Kartensysteme*, Hüthig 1997
104. Strasburger D., *Zasady sztuki wojennej*, Bellona, Warszawa 1996
105. Sus P., *Zamki*, artykuł Murator 8/172/1998
106. *System automatyki. "INFINITY" v.01*, Andover Controls

107. *Systemy alarmowe. Kompatybilność elektromagnetyczna - Norma dla grupy wyrobów. Wymagania dotyczące odporności urządzeń systemów alarmowych pożarowych, włamaniowych i osobistych.* Projekt PN-EN-50130-4, PKN

108. *Systemy alarmowe. Systemy alarmowe osobiste. Wytyczne stosowania.* Projekt PN-EN 50134-7, PKN

109. *Systemy alarmowe. Systemy dozorowe TVU w zastosowaniach dotyczących zabezpieczenia. Zalecenia dotyczące zastosowań.* Projekt PN-EN 50132-7, PKN

110. *Systemy alarmowe. Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia. Wymagania systemowe.* Projekt PN-EN 50133-1, PKN

111. *Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania central.* Projekt PN-E-08390-3, PKN

112. *Systemy alarmowe. Włamaniowe systemy alarmowe. Wymagania i badania sygnalizatorów.* Projekt PN-E-08390-5

113. *Systemy Alarmowe*. Wybór artykułów 1992/98

114. *Systemy alarmowe. Zbiór arkuszy Polskiej Normy*. PN-93/E-08390-14: 1993

115. Sztab Generalny WP Zarząd Obrony Terytorialnej, *Tymczasowe normy zabezpieczenia w techniczne urządzenia sygnalizacyjne i alarmowe terenów, obiektów i mienia wojskowego*, Warszawa 1999

116. Świerczyński J., *Wybrane zagadnienia taktyczne stosowania kryminalistycznych systemów zabezpieczających z wykorzystaniem urządzeń elektronicznych*, Systemy Alarmowe 1/92

117. Świętochowska U., *Patologie cywilizacji współczesnej*, Toruń 1998

118. Świętochowska U., *Systemowe rozwiązania w zakresie zapobiegania i ograniczania patalogii społecznej*, Gdańsk 1995

119. Tarasiuk B., Czarniecki A., Suwiński W., *Kierowanie obronnością państwa w czasie pokoju, kryzysu i wojny. Materiał studyjny*, Warszawa 1998

120. Tatarowski B, Wójcik A., *Tendencje rozwojowe elektronicznych urządzeń zabezpieczających*, referat na konferencję "Urządzenia i sposoby zabezpieczenia mienia." SECUREX '92, Poznań 6-7.02.1992

121. *Technische Erläuterungen zu den Sicherundsrichtlinien*, VdS 2334 08/93 (02), Verband der Sachversicherer e.V. Köln

122. *The Specifiers Guide to Sony CCTV 1998*

123. Tomczak A., *Charakterystyka techniczna i funkcjonalna elementów systemów kontroli dostępu. Przewodnik rzeczoznawcy.*"

124. *Urządzenia i sposoby zabezpieczenia mienia.* SECUREX '95, '96, '98.

125. Uss S., *PowerPoint 7 Pl,*Help, Warszawa 1996
126. *Ustawa o ochronie informacji niejawnych,* Dz.U.Nr 11, poz.95
127. *Ustawa o ochronie osób i mienia,* Dz. U. Nr 114, poz.740
128. *Videor Technical. CCTV Technische Änderungen vorbehalten*, 1998
129. *Videotechnik*, W&S Special Sondernummer, Kriminalistik Verlag Juli 1992
130. *Videv Fernsehüberwachungssystme*. Produktsliste 1997
131. W&S Special Sondernummer, *Brandschutz*, Hüthig Juli 1994
132. Wagner M. Harvey, *Badania operacyjne*, PWE, Warszawa 1980
133. Walczyk J., *Podstawy systemów telewizji użytkowej*, Wydawnictwa Komunikacji i Łączności, Warszawa 1992
134. Walczyk J., *Urządzenia i systemy telewizji użytkowej*, Wydawnictwa Komunikacji i Łączności, Warszawa 1982
135. Weber W., *Alarmtechnik. Elektronische Sicherheits- und Überwachungssysteme,* Pflaum Verlag KG München 1979
136. Wege A., *Video-Überwachungstechnik. CCTV-Handbuch für Planer, Berater und Anwender*, Hüthig GmbH, Heidelberg 1997
137. Woźnicki J., *Podstawowe techniki przetwarzania obrazu*, WKŁ, Warszawa 1996
138. Wójcik A,. referat *Wybrane elementy ochrony obiektów wojskowych za pomocą systemów alarmowych i sygnalizacji zagrożeń*", Konferencja Naukowa "Urządzenia i systemy łączności na potrzeby kierowania obronnością i bezpieczeństwem państwa", Akademia Obrony Narodowej, Warszawa, październik 1996
139. Wójcik A., *Analiza światowego rynku systemów sygnalizacji zagrożeń. Charakterystyka rynku polskiego*, Podyplomowe Studium Marketingu i Analizy Rynku Handlu Zagranicznego SGPiS, Warszawa czerwiec 1990
140. Wójcik A., *Charakterystyka techniczna i funkcjonalna elementów systemów sygnalizacji włamania i napadu. Charakterystyka systemów ewakuacji i panikowych,* Przewodnik Rzeczoznawcy Ogólnopolskiego Stowarzyszenia Producentów, Projektantów i Instalatorów Systemów Alarmowych. Zeszyt Nr 4. Warszawa 1994.
141. Wójcik A., *Elektrozaczepy - prosty sposób zabezpieczenia*, artykuł "Ochrona mienia", lipiec 1998
142. Wójcik A., *Metodyka kosztorysowania prac projektowych i wykonawstwa elektronicznych systemów alarmowych*, skrypt ZTOM TECHOM 1999
143. Wójcik A., *Niezawodność systemów sygnalizacji pożaru firmy effeff gwarancją bezpieczeństwa*, artykuł Instalator Polski, czerwiec 1998

144. Wójcik A., *Podstawowe cechy dokumentacji projektowej. Weryfikacja powykonawcza projektu i kosztorysu*, Przewodnik Rzeczoznawcy Ogólnopolskiego Stowarzyszenia Producentów, Projektantów i Instalatorów Systemów Alarmowych. Zeszyt Nr 4. Warszawa 1994.
145. Wójcik A., praca studyjna *Wybrane problemy wykorzystania innowacyjnych technik alarmowania w zakresie elektronicznej ochrony jednostek wojskowych*, Akademia Obrony Narodowej Podyplomowe Zaoczne Studium Obronności Państwa 1998
146. Wójcik A., *Przebieg procesu projektowania*, Przewodnik Rzeczoznawcy Ogólnopolskiego Stowarzyszenia Producentów, Projektantów i Instalatorów Systemów Alarmowych. Zeszyt Nr 4. Warszawa 1994.
147. Wójcik A., referat *Innowacyjne techniki alarmowania w zakresie elektronicznej ochrony jednostek wojskowych,* IV Konferencja KSOŁ-97 AON
148. Wójcik A., referat *Niezawodność systemów sygnalizacji pożaru gwarancją bezpieczeństwa. Kryteria wyboru nowoczesnego systemu alarmu pożaru*, I Ogólnopolska Konferencja Techniczna Elektronicznych Systemów Ochrony Mienia i Osób OSPPiISA, Brok n/Bugiem 22-23 maja 1998
149. Wójcik A., *Systemy kontroli dostępu. Budowa, wymagania, zasady projektowania*, skrypt ZTOM TECHOM 1998
150. Wójcik A., *Systemy nadzoru wideo*, cykl artykułów Elektroinstalator 1994/95
151. Wójcik A., *Systemy ochrony zewnętrznej. Przegląd urządzeń i ich zastosowań cz.1 i 2*, artykuły Systemy Alarmowe
152. Wójcik A., S*ystemy telewizji użytkowej. Budowa, wymagania, zasady projektowania*, skrypt ZTOM TECHOM 1998
153. Wójcik A., *Wprowadzenie do projektowania systemów alarmowych sygnalizacji zagrożeń, ver.2.0/04/96*, Zakład Rozwoju Technicznej Ochrony Mienia Warszawa kwiecień 1996
154. Wójcik A., *Zasady projektowania systemów alarmowych sygnalizacji pożaru wg wytycznych VdS cz1. Urządzenia i systemy alarmowe pożaru effeff, wydawnictwo* EFECTA 1995
155. Wójcik A., *Zasady projektowania systemów alarmowych sygnalizacji pożaru wg wytycznych VdS cz2. Urządzenia i systemy alarmowe pożaru effeff. Technologia i przykłady aplikacji,* wydawnictwo EFECTA 1995
156. Zieliński J., *Siły zbrojne sąsiadów Polski*, Bellona, Warszawa 1993
157. Zubek J., *Doktryny bezpieczeństwa*, Studium AON, Warszawa 1992
158. *Zugangskontrolle*, W&S Special Sondernummer, Kriminalistik Verlag Juli 1992

BIBLIOTEKA GŁÓWNA Akademii Obrony Narodowej Nr ewid. 60943 II
BIBLIOTEKA GŁÓWNA Akademii Obrony Narodowej Nr ewid. ..... Działu Zbiorów Jawnych

Ugt Rozprawy oddz. i hab

17,80 5/4128