Grey Scale #13
Colour Chart #13
Blue Cyan Green Yellow Red Magenta White 3/Color Black
Centimetres Inches

AKADEMIA OBRONY NARODOWEJ

Przedłużono okres ochrony do dnia
1105
7060 Anna Kołat
BIBLIOTEKA NIEJAWNA
Nr ewid.
I-9/S
JAWNE
ZASTRZEŻONE
BIBLIOTEKA GŁÓWNA
Z-6081/S
Przeklasyfikowano
Prot. nr 486/30. 8
z dnia 7/10 07 dnia 31.10.07
Anna Kołat
Egz. Nr 1
JAWNE

KIEROWANIE OBRONNOŚCIĄ PAŃSTWA W STANACH NADZWYCZAJNYCH

Praca studyjna

JAWNE
ZASTRZEŻONE
BIBLIOTEKA GŁÓWNA - AKADEMIA OBRONY NARODOWEJ
Nr ewid.
63614

WARSZAWA 2000

Przeklasyfikowano
Prot. nr 4316/36 &
z dn. 21.10.08 r. dnia 13/10/
Anna Kowalska
JAWNE
Zastrzeżone
Egz. Nr ..1..
Z-608/S
Z-9/S

AKADEMIA OBRONY NARODOWEJ

KIEROWANIE OBRONNOŚCIĄ PAŃSTWA W STANACH NADZWYCZAJNYCH

63614

Praca studyjna

Etap I 01.10. – 30.12.2000 r.

Z – 1/P/

JAWNE
Zastrzeżone
1 z 211

Warszawa grudzień 2000

SKŁAD ZESPOŁU PRACY STUDYJNEJ

Autorzy opracowania:

Kierownik tematu - gen. bryg. prof. dr hab. Michał KRAUZE:

- wstęp – założenia metodologiczne;
- wnioski do rozdziału 1.

Z - ca kierownika - płk rez. dr inż. Eugeniusz PIEDZIUK:

- podrozdziały: 4.1., 4.2., 4.3., 4.4., 4.6., 4.7., 4.8., 4.10.;
- wnioski do rozdziału 4.

Płk dr hab. Jacek PAWŁOWSKI:

- podrozdziały: 1.1., 1.2., 2.1., 2.2., 2.3., 2.5, 3.2.;
- wnioski do rozdziału 2.

Płk dr inż. Stanisław KRYSIŃSKI:

- podrozdziały: 2.4., 4.13., 4.14., 4.15., 3.2.;
- wnioski do rozdziału 3.

Ppłk mgr inż. Marek ŻOCHOWSKI:

- porozdziały: 4.5., 4.9., 3.1.1., 3.1.2.;
- wnioski do rozdziału 3.

Ppłk mgr inż. Bogusław JAWORSKI:

- podrozdziały: 4.11., 4.12., 3.1.3., 3.1.4.;
- wnioski do rozdziału 3.

Sekretarz – mgr Urszula JARASZEK:

- tłumaczenie tekstu z języka obcego;
- adiustacja i korekta redakcyjna.

JAWNE
Zastrzeżone

SPIS TREŚCI

WSTĘP (ZAŁOŻENIA METODOLOGICZNE) 5

1. ZAGROŻENIA SYSTEMU OBRONNOŚCI PAŃSTWA 12

1.1. System obronności państwa jako obiekt zagrożeń 12

1.2. Charakterystyka prawdopodobnych zagrożeń systemu obronności państwa 28

Wnioski 40

2. KIEROWANIE OBRONNOŚCIĄ PAŃSTWA - STAN AKTUALNY 42

2.1. Rola, miejsce i zadania podsystemu kierowania obronnością państwa 42

2.2. Charakterystyka wybranych elementów podsystemu kierowania 42

2.3. Procesy i zależności między elementami systemu kierowania 60

2.4. Ocena aktualnego systemu kierowania obronnością 64

2.5. Stany nadzwyczajne w kontekście prawdopodobnych zagrożeń 67

Wnioski 69

3. SYSTEMY KIEROWANIA OBRONNOŚCIĄ W WYBRANYCH PAŃSTWACH NATO 72

3.1. Kierowanie obronnością w wybranych państwach NATO 72

3.1.1. Kierowanie obronnością w USA 75

3.1.2. Kierowanie obronnością w Republice Federalnej Niemiec 78

3.1.3. Kierowanie obronnością w Wielkiej Brytanii 82

3.1.4. Kierowanie obronnością we Francji 84

3.2. Analiza porównawcza systemów kierowania w wybranych państwach NATO wynikające stąd wskazania dla własnych (narodowych) rozwiązań w tym zakresie 87

Wnioski 90

JAWNE
Zastrzeżone

4. OCENA WYKORZYSTANIA I MOŻLIWOŚCI SYSTEMU TELEKOMUNIKACYJNEGO W KIEROWANIU OBRONNOŚCIĄ PAŃSTWA 95

4.1. Sieć telekomunikacyjna kraju 95

4.2. Klasyfikacja telekomunikacji 100

4.3. Zintegrowana usługowo sieć cyfrowa ISDN 106

4.4. Zintegrowane usługowo sieci szerokopasmowe B-ISDN 110

4.5. Telefonia komórkowa 111

4.6. Transmisja danych 118

4.7. Systemy komutacyjne 123

4.8. Technologie w sieciach teleinformatycznych 126

4.9. Radiokomunikacja 134

4.10. Techniki realizacji systemów i struktury sieciowe 141

4.11. Usługi telekomunikacyjne 156

4.12. Rozbudowa infrastruktury telekomunikacyjnej kraju w aspekcie potrzeb obronności 162

4.13. Bezpieczeństwo systemów telekomunikacyjnych 171

4.14. Wskaźniki oceny systemów łączności 180

4.15. Wymagania stawiane systemom łączności 188

Wnioski 191

WNIOSKI KOŃCOWE 196

BIBLIOGRAFIA 201

ZAŁĄCZNIKI 204

JAWNE
Zastrzeżone

WSTĘP (ZAŁOŻENIA METODOLOGICZNE)

Po roku 1989 przed polską myślą obronną i naukami wojskowymi, które przede wszystkim tę myśl rozwijają i czynią coraz pełniejszą, stanęły nowe wyzwania. Młode demokratyczne państwo zaczęło wówczas swoje funkcjonowanie w zmienionych uwarunkowaniach wewnętrznych i zewnętrznych. Te pierwsze sprawiły, iż zaistniała pilna potrzeba dokonania zmian o charakterze ustrojowym, politycznym, ekonomicznym i społecznym. Drugie zaś otworzyły szerokie możliwości uzyskania przez Polskę statusu państwa w pełni demokratycznego, z możliwością stania się równoprawnym członkiem międzynarodowych - światowych i europejskich - struktur politycznych, gospodarczych i militarnych.

Zmiana orientacji politycznej, przemiany geopolityczne w Europie i na świecie, a przede wszystkim upadek Związku Radzieckiego, stały się przyczyną sprawczą zawarcia nowych sojuszy w celu zapewnienia państwu bezpieczeństwa, suwerenności i niepodległości nie tylko współcześnie, ale także w przyszłości. Pojawiła się wówczas całkiem realna szansa przyjęcia Polski do Paktu Północnoatlantyckiego, szansa, która została w pełni wykorzystana, bowiem niedawno obchodziliśmy pierwszą rocznicę tego ważnego wydarzenia.

`W okresie reformowania państwa, nie sposób było pominąć tak ważnego jego segmentu strukturalno-funkcjonalnego, jakim jest niewątpliwie system obronnosci. W nowych uwarunkowaniach polityczno-militarnych, w polskiej myśli wojskowej czy, mówiąc szerzej, w myśli obronnej RP, musiał być dokonany swoisty remanent. Polegał on na określeniu, wskazaniu i wyeksponowaniu tych zdobyczy myśli wojskowej okresu poprzedniej formacji społeczno-ekonomicznej, które są ciągle aktualne, mają charakter uniwersalny i ponadczasowy, a więc mogą być nadal źródłem inspiracji teoretycznej, jak również różnego rodzaju rozwiązań praktycznych. Natomiast te fragmenty dociekań teoretycznych i te rozwiązania o charakterze utylitarnym, które nie nadawały się do bezpośredniego wykorzystania lub zaadaptowania w nowych warunkach, musiały zostać odłożone na półki archiwalne, gdzie pozostaną jako źródło wiedzy o myśli wojskowej właściwej dla poprzedniej formacji społeczno-ekonomicznej, ówczesnej polityce militarnej państwa, jego sojuszach wojskowych, doktrynie, strategii, sztuce operacyjnej i taktyce.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

W tym miejscu należy stwierdzić, że problematyka niniejszej pracy studyjnej, a więc wszystko to, co dotyczy systemu obronnego państwa, współczesnych zagrożeń, stanów nadzwyczajnych, a zwłasza szeroko rozumianej problematyki kierowania obronnością państwa, stanowi absolutną nowość. W zmienionych uwarunkowaniach, jakie zaistniały na przełomie lat osiemdziesiątych i dziewięćdziesiątych straciły bowiem swoją aktualność wszystkie opracowania teoretyczne i rozwiązania praktyczne dotyczące tego obszaru funkcjonowania państwa. Przeprowadzony, wspomniany wyżej, swoisty „remanent stanu posiadania" w tej dziedzinie jednocześnie wykazał, że teoria i praktyka sprzed 1989 roku, może mieć znaczenie jedynie archiwalne.

Wobec takiej rzeczywistości i takiej negatywnej oceny przydatności „spadku" odziedziczonego po poprzedniej formacji politycznej i społeczno-ekonomicznej, należało rozpocząć prace badawcze i projektowe nad nowym systemem bezpieczeństwa i obronności państwa, odpowiadającym zmienionym uwarunkowaniom i nowym wymaganiom formułowanym przez różne układy zewnętrzne i wewnętrzne. Wymagania te wynikały głównie z aspirowania Polski do europejskich i światowych struktur politycznych, ekonomicznych i militarnych, a następnie miały bezpośredni związek z przyjęciem naszego kraju do Paktu Północnoatlantyckiego.

W nowej rzeczywistości Polska funkcjonuje już ponad 10 lat. Wprowadzonych zostało, z różnym skutkiem, wiele reform, ciągle trwa reformowanie systemu obronnego państwa, które wyraża się zwłaszcza w przyjęciu nowych założeń doktrynalnych, dostosowaniu rozwiązań systemowych dotyczących obronności do tych, które obowiązują w państwach NATO, restrukturyzacji i redukcji sił zbrojnych, podejmowaniu strategicznych decyzji związanych z systemami uzbrojenia itp. Praktyka wykazuje, że proces ten mieć będzie charakter ciągły, i że osiąganie nowych celów stanie się długotrwałe oraz wymagać będzie ogromnych nakładów, a co się z tym łączy, znaczących wyrzeczeń społecznych.

W czasie minionych dziesięciu lat uczyniono wiele w dziedzinie tak ważnej, jaką jest kierowanie obronnością państwa w różnych sytuacjach polityczno-militarnych. System kierowania obronnością państwa, obok podsystemu militarnego i pozamilitarnego jest jednym z zasadniczych elementów systemu obronnego. Jego rola polega na informacyjnym sprzężeniu tych elementów w jednolitą sprawnie funkcjonującą całość. O jego efektywności decyduje nie tylko właściwy dobór ludzi na kierownicze funkcje, jego struktura gospodarcza, ale przede wszystkim infrastruktura telekomunikacyjna i informatyczna.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Podstawowym elementem systemu kierowania i zarządzania państwem, sterowania gospodarką narodową, dowodzenia siłami zbrojnymi oraz funkcjonowania organów bezpieczeństwa publicznego jest niezawodnie działający system łączności państwa. Zdolność wykonania stojących przed nim zadań zależy między innymi od stanu rozbudowy infrastruktury systemu łączności na obszarze całego kraju, jego sprawności organizacyjno - technicznej, przepustowości i niezawodności. Natomiast szczególne ważną rolę spełnia łączność w okresie zagrożenia bezpieczeństwa państwa a zwłaszcza stanów nadzwyczajnych.

Systemy łączności, wykorzystywane w okresie stanów nadzwyczajnych, projektuje się już w czasie pokoju. Następnie są one modyfikowane stosownie do stawianych stawianych wymagań oraz aktualnych potrzeb i uwarunkowań.

Pojawiło się na ten temat sporo różnego rodzaju i różnego autorstwa pomysłów, propozycji, mniej lub bardziej rozwiniętych koncepcji projektów. Nadal jednak problem ten ma charakter dyskusyjny i polemiczny. Wydaje się więc, że czeka nas jeszcze dość długa droga do rozstrzygnięć jednoznacznych i ostatecznych, w konkretnych warunkach optymalnych, a więc najlepszych z możliwych. W takiej konwencji utrzymana zostanie niniejsza praca studyjna. Stanowić ona będzie, mamy nadzieję, bardzo ważny i liczący się głos w dyskusji na temat kierowania obronnością państwa. Głos ten stanie się zapewne o tyle ważny i godny zainteresowania, że dotyczyć będzie dziesięcioletniej już historii zmagania się z tą trudną materią badawczą i z tym skomplikowanym problemem naukowym.

Dlatego ***celem pracy*** jest:

- *w pierwszym etapie – dokonanie krytycznej oceny aktualnego stanu rozwiązań dotyczących kierowania obronnością państwa i systemu telekomunikacyjnego kraju w stanach nadzwyczajnych;*

- *w drugim etapie –zaprezentowanie nowego (zmodyfikowanego) spojrzenia na system kierowania obronnością państwa i system łączności w stanach nadzwyczajnych;*

Sformułowanemu wyżej celowi badań podporządkowane zostały problemy badawcze, hipotezy robocze i przyjęty układ pracy. Należy przy tym podkreślić, że niezależnie od zajęcia stanowiska wobec szeroko rozumianego systemu kierowania obronnością państwa, autorzy

JAWNE
Zastrzeżone

pracy skoncentrują się w swoich badaniach na systemie łączności i w związku z tym najwięcej miejsca poświęcą problematyce telekomunikacyjnej szczególnie, wykorzystaniu sieci i środków najnowszej generacji, eksponując w tym zakresie rozwiązania zapewniające sprawne i niezawodne funkcjonowanie systemu.

Główny problem badawczy, biorąc pod uwagę sformułowany *cel badań* oraz inne przesłanki z tym związane, można ująć następująco:

Jakie są pożądane kierunki zmian w istniejącym systemie kierowania obronnością państwa (lub jaki powinien być jego nowy model), w kontekście wniosków wynikających z oceny rozwiązań krajowych i zagranicznych w tym zakresie oraz możliwości telekomunikacyjnego zabezpieczenia jego funkcjonowania?

Aby stworzyć dogodne warunki i zgromadzić niezbędny materiał badawczy umożliwiający rozwiązanie głównego problemu naukowego, należy udzielić odpowiedzi na następujące *pytania badawcze,* traktowane jako *problemy szczegółowe*:

1. *Na czym polega i do czego się sprawdza istota systemu obronności państwa?*

2. *Jakiego rodzaju zagrożenia są szczególnie niebezpieczne dla systemu obronności państwa; do odparcia jakich zagrożeń powinien on być przede wszystkim przygotowany?*

3. *Co do tej pory (w ciągu dziesięciu minionych lat) ustalono w dziedzinie kierowania obronnością państwa – na czym ono polega, jaka jest jego organizacja, jakie obowiązują w tym zakresie zasady i reguły?*

4. *Jaka jest istota stanów nadzwyczajnych, jakie istnieją związki i zależności pomiędzy nimi, a prawdopodobnymi zagrożeniami?*

5. *Jaki wpływ na funkcjonowanie systemu kierowania obronnością państwa mogą wywierać przewidywane zagrożenia i co z tego wynika dla systemu?*

JAWNE
Zastrzeżone

6. *Jakie są zadania i wymagania stawiane systemowi łączności przez system kierowania obronnością i jak może im sprostać obecna infrastruktura telekomunikacyjna kraju?*

7. *Jakie nauki wypływają z analizy porównawczej natowskich systemów kierowania obronnością dla rozwiązań narodowych (polskich)?*

8. *Jaki powinien być model systemu kierowania obronnością państwa oraz jaki należy przyjąć model organizacji systemu łączności kierowania obronnością?*

Udzielenie odpowiedzi na przedstawione wyżej pytania oraz rozstrzygnięcie innych kwestii, które pojawiły się w toku badań, stanowić będzie podstawę do zaprezentowania, w drugiej części pracy, nowego podejścia do systemu kierowania obronnością państwa, co zostanie uczynione w formie opisowej (kierunki zmian) lub w postaci stosownego rozwiązania modelowego (model systemu kierowania i jego system łączności).

Ogólna *hipoteza robocza* pracy sprowadza się do stwierdzenia, opartego w pewnym stopniu na intuicji, ale przede wszystkim na doświadczeniui ujęta została następująco:

Dotychczasowe rozwiązania w zakresie kierowania obronnością państwa i systemu łączności nie spełniają współczesnych, a tym bardziej przyszłych oczekiwań, i jako takie nie gwarantują sprawnego funkcjonowania systemu obronności (procesy, procedury, kompetencje, organizacja, techniki i technologie, środki techniczne, zabezpieczenie itp.)

Zespół autorski wyraża nadzieję, że hipoteza ta zostanie, w wyniku przeprowadzonych badań, zweryfikowana, a wnioski będące rezultatem tej weryfikacji, stanowić będą podstawę do twórczego i nowatorskiego spojrzenia na problem w fazie konstruowania zmodyfikowanego lub nowego systemu kierowania obronnością państwa i systemu łączności.

Praca zespołu badawczego polegać będzie głównie na studiowaniu literatury przedmiotu, zarówno polskiej, jak i obcojęzycznej, dokonywaniu przy tej okazji stosowanych porównań, uogólnień, analogii, abstrahowań, a szczególnie analiz i syntez w celu udzielenia odpowiedzi na postawione pytania oraz na prowadzeniu licznych konsultacji i dyskusji z osobami uznawanymi za ekspertów (metoda badania sądów i ocen ekspertów) w dziedzinie kierowania obronnością

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

państwa – tak w aspekcie organizacyjnym, kompetencyjnym i funkcjonalnym, jak również technicznym. W niezbędnym zakresie będzie stosowane podejście systemowe i modelowanie.

Część pierwsza pracy składa się ze wstępu i czterech rozdziałów głównych zawierających stosowne podrozdziały.

We wstępie omówione zostały przesłanki, które sprawiły, że problem badawczy, w zaproponowanym ujęciu, został podjęty. Przedstawiono w nim także podstawowe założenia metodologiczne – cel główny i cele szczegółowe, problemy badawcze, ogólną hipotezę roboczą, metody badawcze, układ pracy oraz ocenę literatury przedmiotu.

Rozdział pierwszy dotyczy zagrożenia systemu obronności państwa. System ten został rozpatrzony jako obiekt zagrożeń z wyeksponowaniem ich poszczególnych rodzajów i charakterystycznych cech.

W rozdziale drugim przedstawiono analizę aktualnego stanu kierowania obronnością państwa. Ażeby stało się to możliwie najpierw dokonany został opis istniejących rozwiązań (rola, miejsce, zadania, charakterystyka wybranych elementów systemu oraz procesy i zależności zachodzące między nimi). W oparciu o tak sporządzony opis, mogła być dokonana w miarę wszechstronna i głęboka ocena aktualnego systemu kierowania obronnością państwa, co dla dalszych badań miało pierwszorzędne znaczenie. Temat pracy studyjnej ma bezpośredni związek ze stanami nadzwyczajnymi, bowiem właśnie one stanowiły podstawę (tło, kanwę) do prezentacji systemu kierowania obronnością państwa. Aby zatem była pełna jasność co do terminologii i jej rozumienia w podrozdziale 2.5. dokonano opisu trzech rodzajów stanu nadzwyczajnego tzn. stanu wojennego, stanu wyjątkowego i stanu klęski żywiołowej. Specyfika każdego z tych stanów wymagała specjalnego potraktowania w czasie formułowania i budowania systemu kierowania obronnością państwa.

Rozdział trzeci ma dla części pierwszej pracy studyjnej posiłkowe, choć bardzo ważne znaczenie. Rozpatrzono w nim bowiem, w sposób porównawczy, systemy kierowania obronnością takich państw, jak: Stany Zjednoczone, Republika Federalna Niemiec, Wielka Brytania i Francja. Pozwoliło to na poszukiwanie pewnych analogii pomiędzy różnymi systemami oraz takich rozwiązań, czy raczej ich elementów, które maja znaczenie uniwersalne i mogą ewentualnie znaleźć zastosowanie w różnych warunkach funkcjonowania państwa, także państwa średniej wielkości, jakim jest Polska.

JAWNE
Zastrzeżone

W rozdziale czwartym przeprowadzono analizę istniejącego systemu telekomunikacyjnego kraju, przedstawino również nowe techniki i technologie telekomunikacyjne oraz urządzenia nowej generacji, aby móc dokonanć oceny jego wykorzystania i możliwości w kierowaniu obronnością państwa. Zostały określone potrzeby rozbudowy infrastruktury telekomunikacyjnej kraju w zakresie obronności państwa. Zagadnienia ochrony i zachowania bezpeczeństwa przesyłanych informacji, wskaźniki oceny i wymagania stawiane systemom łączności kończą rozdział i stanowią podstawę do prowadzenia dalszych prac, celem określenia koncepcji (modelu) systemu łączności kierowania obronnością państwa.

Rozdziały kończą się *wnioskami,* które będą przydatne w dalszym etapie badań.

Opracowanie zkończono *wnioskami końcowymi.* Stanowią one wskazania i uwagi do opracowania drugiego etapu pracy studyjnej.

W trakcie badania literatury dotyczącej podjętych problemów stwierdzono, że pomimo, iż jest ona dość bogata, to obejmuje jednak podstawowe zagadnienia w sposób zbyt ogólny lub też fragmentaryczny. Ogólnie można stwierdzić, że literatura przedmiotu jest stosunkowo skromna i jako taka była mało przydatna w procesie badań. Mamy tutaj na myśli przede wszystkim literaturę związaną bezpośrednio z tematem pracy. Dość dobrze natomiast odzwierciedlone jest w literaturze „tło" badań, a więc np.: system obronny państwa, strategia obronności RP, podstawowe założenia polityki bezpieczeństwa i strategii obronnej, problematyka różnego rodzaju zagrożeń, w tym militarnych, system telekomunikacyjny kraju itp. Był to jeden z istotnych czynników, który skłonił autorów do szerokiego zastosowania wielu metod badawczych. W sumie zgromadzona literatura stała się pewnym pretekstem i podstawą do generowania nowych treści, które stanowią oryginalny i nigdzie nie publikowany dorobek zespołu autorskiego.

JAWNE
Zastrzeżone

1. ZAGROŻENIA SYSTEMU OBRONNOŚCI PAŃSTWA

1.1. System obronności państwa jako obiekt zagrożeń

Aktualna doktryna obronna Rzeczpospolitej Polskiej, wyrażona w strategii bezpieczeństwa RP i strategii obronności RP, dokonujące się przekształcenia struktur państwowych, reorganizacja sił zbrojnych kształtująca nowy model ich organizacji, wymuszają jakościowe zmiany w systemie obronności państwa.

Celem strategicznym Rzeczpospolitej Polskiej obronności jest zapewnienie bezpiecznych warunków realizacji interesów narodowych poprzez ich obronę przed zewnętrznymi zagrożeniami kryzysowymi i zagrożeniami wojennymi. Oznacza to w szczególności:

- obronę terytorium Rzeczpospolitej Polskiej przed agresją zbrojną, w tym zapewnienie nienaruszalności polskiej przestrzeni powietrznej i morskiej oraz granic lądowych;
- obronę i ochronę wszystkich obywateli RP;
- udział we wspólnej obronie terytorium państw członkowskich NATO, zgodnie z art. 5 Traktatu Waszyngtońskiego;
- wspieranie akcji instytucji i organizacji międzynarodowych w reagowaniu kryzysowym oraz polityczno-militarnych działaniach stabilizujących;
- kształtowanie bezpiecznego otoczenia Polski poprzez rozwijanie partnerskiej współpracy wojskowej z innymi państwami, zwłaszcza sąsiednimi[1].Podstawowym atrybutem suwerenności Rzeczpospolitej Polskiej jest posiadanie własnego potencjału obronnego.

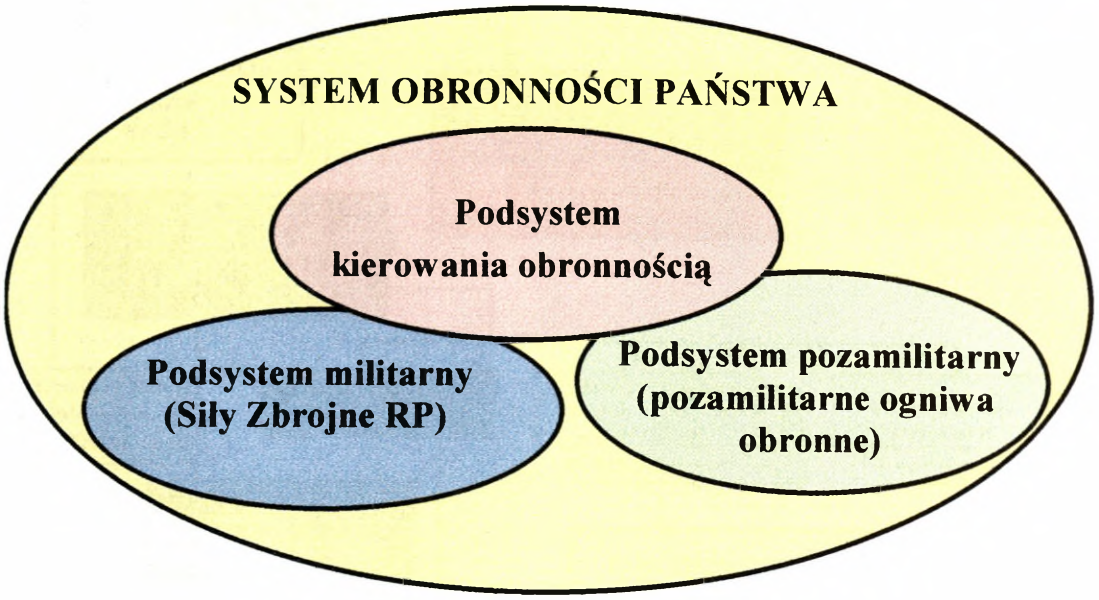
Potencjał ten opiera się na utrzymywanym w czasie pokoju i rozwijanym na okres kryzysu i wojny systemie obronności (Rys. 1.1.).

Zbiór elementów, tworzących strukturę systemu obronności państwa, można podzielić na podsystemy:

- podsystem kierowania obronnością państwa, który tworzą najwyższe organa władzy i administracji państwowej;
- podsystem militarny, który stanowią i tworzą siły zbrojne;
- podsystem pozamilitarny, w skład którego wchodzą pozamilitarne ogniwa obronne.

[1] Strategia obronności RP, Wyd. Biuro Prasy i Informacji AON, Warszawa 2000 r., str. 10

JAWNE
Zastrzeżone

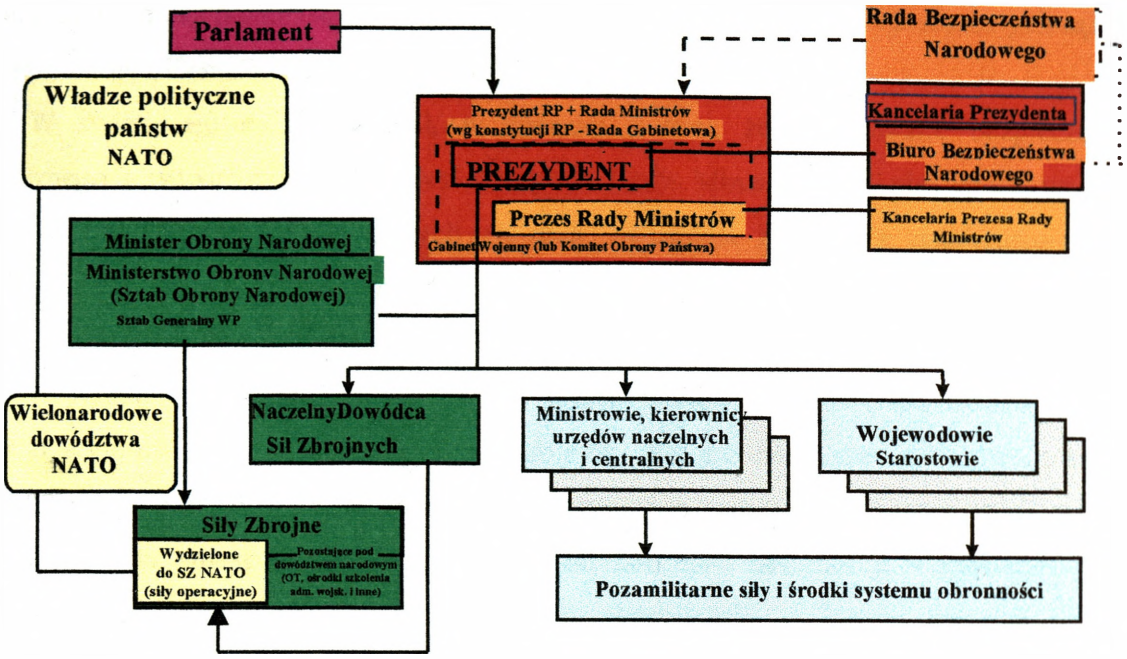


Rys.1.1. Ogólny schemat systemu obronności państwa (wariant)

Podsystem kierowania obronnością

Podsystem kierowania obronnością tworzą wszystkie organa kierowania odpowiadające za realizację zadań obronnych w ustanowionych prawnie relacjach kompetencyjnych. Do zasadniczych funkcji podsystemu należy: kierowanie przygotowaniami obronnymi w czasie pokoju, kierowanie reagowaniem na zagrożenia kryzysowe oraz kierowanie obronnością państwa w czasie wojny.

Kierowanie obronnością - jeden z trzech podstawowych elementów struktury funkcjonalnej systemu obronności – polega m.in. na przygotowaniu i utrzymywaniu wszystkich elementów i ogniw tego systemu w gotowości do jego mobilizacyjnego rozwinięcia (Rys.1.2.).Realizację decyzji państwa w dziedzinie obronności zapewniają organa kierowania na wszystkich szczeblach struktury państwowej – centralnym (resortowym) i terenowym, w tym organy dowodzenia sił zbrojnych – stosownie do swych kompetencji stawiając zadania podległym jednostkom organizacyjnym lub zlecając zadania obronne innym jednostkom organizacyjnym państwa.



Rys.1.2. Ideowy schemat systemu kierowania obronnością państwa (wariant)

Organa kierowania odpowiadające za realizację zadań obronnych, powiązane informacyjnie i pozostające w ustanowionych prawnie relacjach kompetencyjnych wraz ze swoim aparatem wykonawczym (administracyjnym, sztabowym, organizacyjnym) oraz niezbędną infrastrukturą tworzą podsystem kierowania obronnością.

W procesie kierowania obronnością uczestniczą organy władzy ustawodawczej, wykonawczej i organy samorządu terytorialnego. Podstawowe funkcje w tym zakresie określa konstytucja oraz ustawy. Do najważniejszych należy zaliczyć:

- ustalanie zadań obronnych, zasad ich wykonywania oraz wykonawców poprzez opracowanie i wydawanie aktów normatywno-prawnych;
- działalność organizatorska w zakresie przygotowań obronnych, obejmująca podejmowanie decyzji oraz sprawowanie nadzoru i kontroli

Prawidłowe spełnianie tych funkcji warunkuje stan prawny w państwie, precyzyjny podział kompetencji oraz przydzielone na obronność środki finansowe. Dotychczas obowiązujący stan prawny (przed wejściem w życie nowej konstytucji) określał, że najważniejszymi organami

JAWNE
Zastrzeżone

odpowiedzialnymi za organizację, nadzór oraz kontrolę procesu przygotowań obronnych są: Rada Ministrów i Komitet Obrony Kraju (KOK).

W świetle nowej Konstytucji, w związku z tym, że zapewnienie bezpieczeństwa zewnętrznego i wewnętrznego państwa należy do Rady Ministrów, na niej spoczywa ciężar organizowania przygotowań obronnych państwa, natomiast zgodnie z ustaleniami ustawy o powszechnym obowiązku obrony głównym organizatorem tych przygotowań jest Komitet Obrony Kraju. Powoduje to określone rozbieżności kompetencyjne.

W ramach kierowania obronnością w czasie pokoju na szczególną uwagę zasługuje organizacja kierowania i dowodzenia siłami zbrojnymi. Szczególnie ważne w tej dziedzinie było przyjęcie ustawy o urzędzie MON, która uporządkowała wiele różnie interpretowanych kwestii.

Ustawa ta wnosi nowe elementy także do koncepcji organizacji wojennego systemu kierowania państwem. W zakresie kierowania obronnością w czasie kryzysu i wojny usytuowanie i rola organów kierujących obronnością nie ulegnie zasadniczym zmianom, za wyjątkiem szczegółowych zakresów kompetencji. Najbardziej zaangażowanymi organami w procesie kierowania obronnością będą: prezydent RP, Rada Ministrów, prezes Rady Ministrów oraz ministrowie: obrony narodowej, spraw zagranicznych, spraw wewnętrznych i administracji, a także naczelny dowódca sił zbrojnych (zgodnie z zapisem zawartym w nowej konstytucji). Działalność pozostałych organów kierujących obronnością różnić się będzie jedynie zakresem i rozmiarami.

W celu zapewnienia skuteczności działań organów wykonawczych państwa w zakresie obronności proponuje się powołanie organu państwowego (o charakterze doradczym), na posiedzeniach którego mogłyby być podejmowane najważniejsze decyzje strategiczne. Organ ten to Gabinet Wojenny (proponowana jest również nazwa - Komitet Obrony Państwa) powoływany przez prezydenta z chwilą wprowadzenia stanu wojennego.

W czasie pokoju, zgodnie z zasadą cywilnej i demokratycznej kontroli nad armią, całością sił zbrojnych, łącznie z żołnierzami i jednostkami organizacyjnymi wydzielonymi do struktur sojuszniczych, kieruje minister obrony narodowej przy pomocy Ministerstwa Obrony Narodowej. Zasadniczym organem planowania strategicznego sił zbrojnych jest Sztab Generalny WP.

Dowództwa Rodzajów Sił Zbrojnych dowodzą w pełni wszystkimi podległymi wojskami, ponosząc odpowiedzialność za całokształt pokojowej działalności podległych wojsk oraz za przygotowanie ich do działań w czasie kryzysu i wojny. Współpracują z dowództwami

JAWNE
Zastrzeżone

sojuszniczymi, w których podporządkowanie wydzielają swoje wojska, a po ich wydzieleniu kierują procesem ich wszechstronnego zabezpieczenia.

W razie zaistnienia polityczno-militarnych sytuacji kryzysowych, stwarzających pośrednie zagrożenia dla bezpieczeństwa Polski, nie będą wprowadzane nadzwyczajne zmiany w ogólnych zasadach kierowania obronnością, a jedynie uruchomione zostaną dodatkowe środki i procedury kierowania reagowaniem kryzysowym. Kierowanie siłami zbrojnymi w czasie kryzysu odbywa się według zasad kierowania pokojowego. Wojskami wydzielonymi do międzynarodowych zgrupowań, wykonujących zadania w ramach reagowania kryzysowego, dowodzą operacyjnie dowódcy tych zgrupowań.

Szczególne rozwiązania wprowadza się na potrzeby kierowania działaniami wojennymi. W warunkach wojennych, jeśli Sejm nie może się zebrać na posiedzenie, funkcję organu ustawodawczego sprawuje prezydent Rzeczpospolitej Polskiej. Na wniosek Rady Ministrów wydaje on rozporządzenia z mocą ustawy, w tym zwłaszcza dotyczące prowadzenia działań wojennych. Prezes Rady Ministrów zapewnia realizację polityki Rady Ministrów w zakresie obrony państwa, określając sposoby jej wykonania. Na czas wojny uruchamia się Centralne Stanowisko Kierowania Obronnością Państwa, obejmujące stanowiska prezydenta Rzeczpospolitej Polskiej, prezesa Rady Ministrów i wyznaczonych przez niego członków Rady Ministrów.

W czasie wojny siłami zbrojnymi dowodzi naczelny dowódca Sił Zbrojnych RP, mianowany przez prezydenta RP na wniosek prezesa Rady Ministrów. Dla zapewnienia bezkolizyjnego rozwijania sił zbrojnych RP oraz kierowania nimi w czasie wojny utworzony zostaje Wojenny System Dowodzenia. Jest on organizowany w czasie pokoju i rozwijany w razie zewnętrznego zagrożenia bezpieczeństwa państwa i wojny. Powinien on zapewnić sprawne wdrażanie decyzji władz państwa i dowodzenie Siłami Zbrojnymi RP w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i wojny, umożliwiając odpowiednie współdziałanie z wojskami sojuszniczymi. Proces dowodzenia odbywa się w systemie narodowym i sojuszniczym. System narodowy zapewnia pełne dowodzenie siłami nie wydzielonymi do struktur NATO oraz dowodzenie pozaoperacyjne wojskami wydzielonymi do zgrupowań sojuszniczych. Po przekazaniu wojsk operacyjnych dowództwom sojuszniczym dowództwo narodowe nadal odpowiada za szkolenie rezerw oraz uzupełnienie i wsparcie logistyczne przekazanych wojsk, a także zapewnia warunki do przyjęcia sił wzmocnienia na terytorium kraju. Naczelny dowódca sił zbrojnych dowodzi w pełni siłami zbrojnymi

JAWNE
Zastrzeżone

pozostającymi w narodowym podporządkowaniu. Całością wojsk wydzielonych do sił zbrojnych NATO dowodzą operacyjnie wielonarodowe dowództwa sojusznicze, na których decyzje władz polskich mogą wpływać poprzez polityczno-wojskowe organa kierowania NATO.

Podsystem militarny - Siły Zbrojne RP

Siły Zbrojne RP są podstawowym elementem systemu obronności państwa. Służą obronie niepodległości Rzeczpospolitej Polskiej i niepodzielności jej terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jej granic. W ramach tej funkcji wykonują zadania wynikające ze strategii obronności Rzeczpospolitej Polskiej, skonkretyzowane w polityczno-strategicznej dyrektywie obronnej i w stosownych narodowych i sojuszniczych planach operacyjnych. Działając w narodowym systemie obronności i w systemie sojuszniczym, Siły Zbrojne RP są przygotowane do wykonywania trzech rodzajów zadań strategicznych: zadań obronnych w razie wojny (odparcie bezpośredniej agresji na terytorium Polski lub udział w odparciu agresji na inne państwo sojusznicze), zadań reagowania kryzysowego (także w ramach misji organizacji międzynarodowych) oraz zadań stabilizacyjnych i prewencyjnych w czasie pokoju, ponadto są one gotowe do udziału w reagowaniu na zagrożenia pozamilitarne. Miejsce i rolę sił zbrojnych w systemie obronności wyznaczają stojące przed nimi zadania, dostosowane do charakteru i skali zagrożeń. Realizują je 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.

W sytuacji sporów, napięć i konfliktów wojennych, które mogą wystąpić w bezpośrednim otoczeniu Polski, a stwarzających bezpośrednie 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

JAWNE
Zastrzeżone

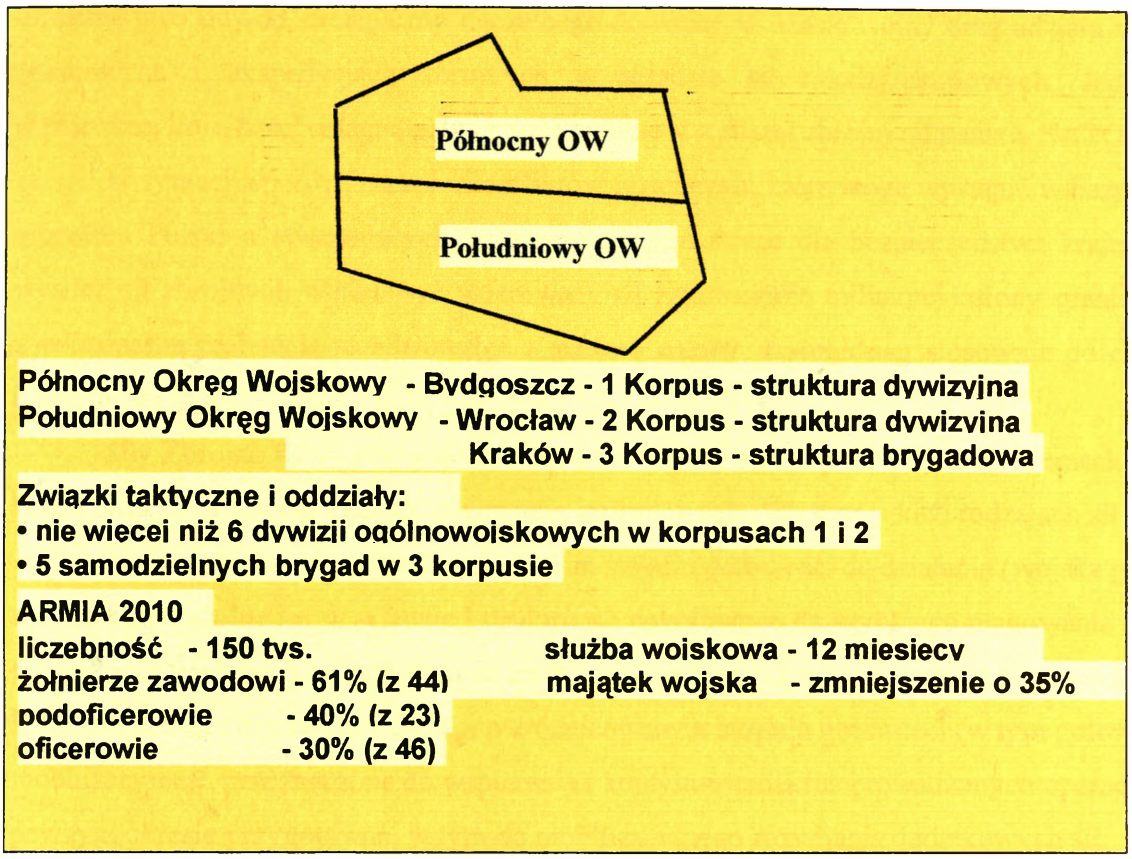
zgrupowania przeciwnika, odzyskania zajętego terytorium, a w razie potrzeby przeprowadzenie działań na jego terytorium.

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.

Uwzględniając przyszłe wymagania operacyjne i strategiczne, główny wysiłek w kształtowaniu modelu Sił Zbrojnych RP skupia się na ich jakości. Oznacza to przede wszystkim konieczność priorytetowego traktowania problemów przyspieszenia tempa modernizacji technicznej, pełnej realizacji procesu szkolenia, w tym stałego podnoszenia kwalifikacji kadr sił zbrojnych zgodnie z wymogami współdziałania sojuszniczego oraz poprawy warunków życia i służby żołnierzy. Potencjał Sił Zbrojnych RP w czasie pokoju będzie utrzymywany na poziomie umożliwiającym skuteczne i elastyczne reagowanie na zmiany sytuacji militarnej w otoczeniu Polski. Będzie on gwarantował realizację zadań osłonowych i natychmiastowe podjęcie działań obronnych w razie zagrożenia bezpieczeństwa państwa i sojuszu, a także stały udział w międzynarodowych operacjach pokojowych i reagowania kryzysowego. Jednocześnie powinien zapewnić możliwość mobilizacyjnego rozwinięcia Sił Zbrojnych RP, stosownie do potrzeb czasu zagrożenia i wojny.

Nowa treść zadań strategicznych i operacyjnych Wojska Polskiego RP oraz zmienione warunki ich realizacji stymulują istotne zmiany w siłach zbrojnych. Trwają intensywne prace nad nowym modelem wojska. Równocześnie ze zmniejszeniem jego liczebności następują sukcesywne przeobrażenia strukturalne, przesunięcia dyslokacyjne, modernizacja techniczna. Wariant przyjęty w 1998 r. przedstawia rys. 1.3.

Stosownie do umów międzynarodowych, zmieniających się potrzeb operacyjno-strategicznych oraz możliwości ekonomicznych kraju przyjęto tj. pod koniec 2000 r. zmniejszenie liczebności Wojska Polskiego do 150 tysięcy żołnierzy. Wojsko Polskie składa się z trzech rodzajów sił zbrojnych. Przewiduje się stopniowo doprowadzenie do bardziej równomiernego rozmieszczenia na obszarze kraju. Nadzwyczaj trudnym zadaniem jest modernizacja techniczna sił zbrojnych oznaczająca konieczność radykalnego zredukowania podstawowych środków walki z równoczesną reorientacją techniczną.



Rys.1.3. Struktura wojsk lądowych (wariant)

Jako priorytet traktujemy modernizację systemów dowodzenia, rozpoznania i WRE oraz łączności - będącej podstawowym warunkiem osiągania zdolności współdziałania w ramach systemu wspólnego bezpieczeństwa.

Jednym ze strategicznych kierunków przebudowy Wojska Polskiego jest sukcesywne przekształcanie wojsk lądowych w wojska powietrzno-lądowe. Jest to możliwe do osiągnięcia przez wprowadzenie do sił zbrojnych śmigłowców i tworzenie oddziałów powietrzno szturmowych i w przyszłości powietrzno-zmechanizowanych. Będą to awangardowe jednostki, składające się na aeromobilne zgrupowanie operacyjne, o pełnym ukompletowaniu, najwyższym stopniu gotowości i zdolności bojowej, o dużym stopniu uzawodowienia.

Siły te przeznaczone będą do natychmiastowego działania w każdym miejscu i na każdym kierunku, samodzielnego przeciwstawienia się niespodziewanym lokalnym zagrożeniom, działania jako odwód strategiczny naczelnego dowódcy w czasie wojny oraz udziału w misjach pokojowych i ekspedycjach zbrojnych w składzie sił międzynarodowych. Jednostki te w pierwszej kolejności osiągną pełną kompatybilność z siłami zbrojnymi państw NATO.

W sytuacji sporów, napięć i konfliktów wojennych, które mogą wystąpić w bezpośrednim otoczeniu Polski a stwarzających bezpośrednie zagrożenie dla bezpieczeństwa kraju, główny wysiłek sił zbrojnych winien być skierowany na zapewnienie militarnej osłony granic państwa z jednoczesną realizacją przedsięwzięć z zakresu osłony strategicznej stosownie do charakteru i stopnia zagrożeń.

Siły Zbrojne RP są przygotowywane zarówno do wykonywania zadań w ramach obrony kolektywnej NATO, jak i zadań reagowania kryzysowego. We wszystkich rodzajach sił zbrojnych utrzymywane są wojska o wysokim stopniu gotowości do działania (wojska gotowości operacyjnej), zdolne już w składzie i strukturach pokojowych do szybkiego reagowania na każdy rodzaj zagrożenia, w tym zwłaszcza do natychmiastowego odparcia agresji na terytorium Rzeczpospolitej Polskiej oraz wojska o zróżnicowanym stopniu gotowości (w tym gotowości mobilizacyjnej), przeznaczone do wspierania i kontynuowania już prowadzonych operacji po pewnym okresie przygotowań, w tym do mobilizacyjnego rozwijania dodatkowych sił, niezbędnych do prowadzenia operacji w razie wojny na dużą skalę.

Podsystem pozamilitarny – pozamilitarne ogniwa obronne

Podsystem pozamilitarny przeznaczony jest do tworzenia niezbędnych warunków przygotowania i działania sił zbrojnych oraz funkcjonowania pozostałych struktur państwa, a także zapewnienia ochrony oraz materialnych i duchowych warunków przetrwania narodu w czasie kryzysu i wojny.

Do podstawowych funkcji pozamilitarnych ogniw obronnych należą:

- ochrona ludności i struktur państwa w warunkach zagrożenia bezpieczeństwa państwa (kryzysu) i wojny;
- zapewnienie materialnych, informacyjnych i duchowych podstaw egzystencji ludności w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa (kryzysu) i wojny;
- zasilanie zasobami ludzkimi i materiałowymi Sił Zbrojnych RP oraz pozamilitarne wsparcie wojsk własnych i sojuszniczych, prowadzących operacje na terytorium Polski.

Wśród ogniw pozamilitarnych występują ogniwa informacyjne, ochronne i gospodarcze. W sensie organizacyjnym funkcjonują one w ramach resortowych i terytorialnych systemów obronności. Zgodnie z powinnościami konstytucyjnymi zadania obronne spoczywają na wszystkich ogniwach systemu obronnego, jak również na wszelkich organizacjach: politycznych, gospodarczych, społecznych. Podstawą siły obronnej kraju jest świadomość obronna każdego obywatela. Miejsce i rolę poszczególnych ogniw pozamilitarnych w systemie obronności państwa wyznaczają stojące przed nim zadania na rzecz sił zbrojnych i obronności.

Najważniejsze zadania obronne realizują polityczne, gospodarcze i administracyjne struktury państwowe. Dotyczy to w szczególności polityki zagranicznej, wywiadu, produkcji i zakupu uzbrojenia oraz sprzętu wojskowego, ochrony wewnętrznej ludności i struktur państwa, w tym obrony cywilnej oraz powszechnej edukacji społeczeństwa (Rys.1.4.).

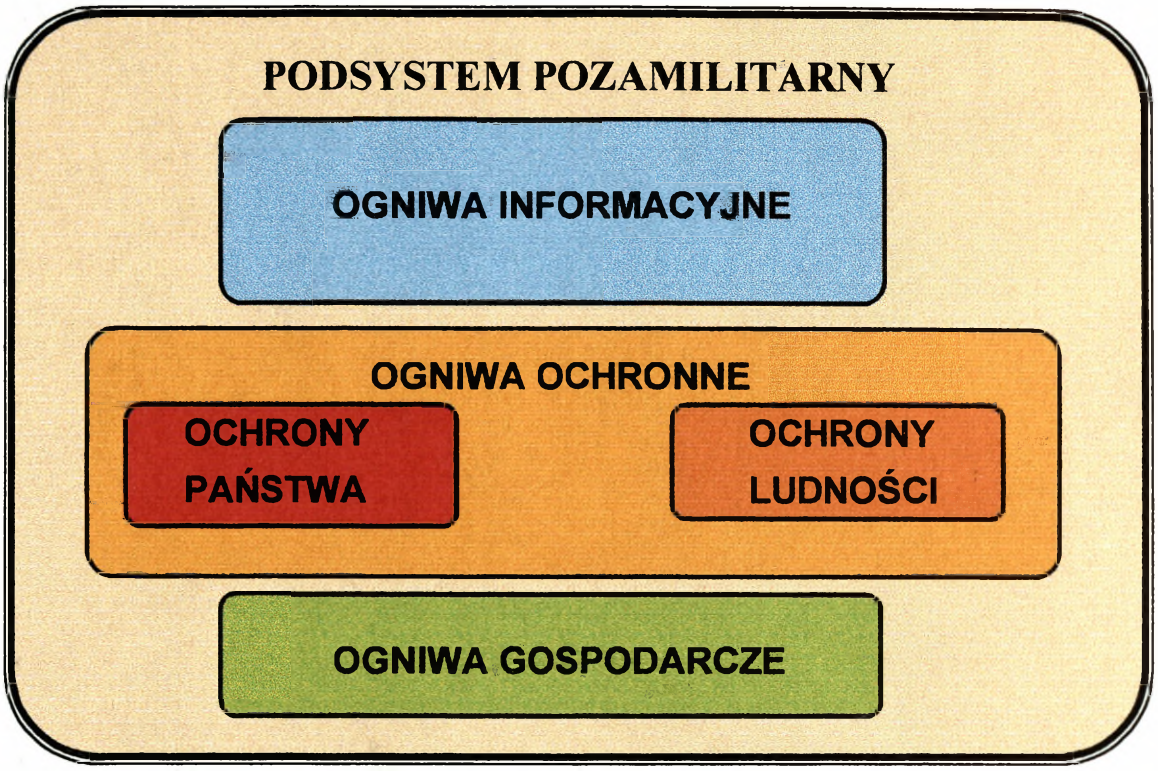
Główne zadania:

- ogniwa informacyjne - utrzymanie pozycji Polski jako suwerennego podmiotu w społeczności międzynarodowej oraz umacnianie jedności narodu, patriotyczno-obronnych postaw i poczucia odpowiedzialności wszystkich obywateli za bezpieczeństwo kraju;
- ogniwa ochronne - zapewnienie warunków sprawnego funkcjonowania struktur państwa oraz ochronę ludności w warunkach kryzysu i wojny;
- ogniwa gospodarcze - zaspokajanie potrzeb systemu obronności państwa i ludności w warunkach kryzysu i wojny.

W razie kryzysu polityczno-militarnego w otoczeniu Polski, zagrażającego bezpieczeństwu państwa, główny wysiłek układu pozamilitarnego skierowany jest na: rozpoznanie sytuacji kryzysowych oraz ocenę ich wpływu na sytuację Polski, rozwiązywanie kryzysu środkami poza zbrojnymi, informowanie społeczeństwa o sytuacji i wynikających z niej zagrożeniach oraz na przeciwdziałanie im. Szczególne zadania w tym względzie spoczywają na resorcie spraw zagranicznych oraz takich ogniwach ochronnych, jak: resort spraw wewnętrznych i administracji, obrona cywilna, Urząd Ochrony Państwa, resort zdrowia i opieki społecznej czy resort ochrony środowiska, zasobów naturalnych i leśnictwa.

W razie lokalnej (ograniczonej) agresji ogniwa układu pozamilitarnego działają przede wszystkim na rzecz jak najszybszego rozstrzygnięcia konfliktu drogą polityczną oraz stworzenia organizacyjnych, informacyjnych i materiałowych warunków skutecznego prowadzenia działań zbrojnych oraz funkcjonowania struktur państwa i przetrwania ludności w czasie wojny.

JAWNE
Zastrzeżone



Rys. 1.4. Struktura podsystemu pozamilitarnego (wariant)

W czasie wojny powszechnej głównym zadaniem układu pozamilitarnego jest - po przejściu gospodarki narodowej z działalności pokojowej na wojenną - stworzenie warunków do skutecznego prowadzenia przez siły zbrojne działań wojennych.

Wyspecjalizowane służby - podległe ministrowi spraw wewnętrznych i administracji (takie jak: Urząd Ochrony Państwa, Policja, Straż Graniczna, Państwowa Straż Pożarna i inne formacje) - mają obowiązek zapobiegania, ujawniania i zwalczania przestępstw kryminalnych, w czasie pokoju oraz narastających w czasie klęsk, kryzysów i wojny.

Obrona Cywilna Kraju koordynuje działania wszystkich sił i środków służących ochronie życia i mienia ludności oraz dóbr kultury, w ramach systemu obronności państwa. Obronę Cywilną Kraju, zgodnie z postanowieniami międzynarodowego prawa wojennego zobowiązuje się do:

JAWNE
Zastrzeżone

- planowania przedsięwzięć w zakresie ochrony życia i zdrowia ludności, ochrony zakładów pracy, urządzeń użyteczności publicznej oraz dóbr kultury przed skutkami działań wojennych;
- organizowania wykrywania zagrożeń w powyższym zakresie;
- ostrzegania i alarmowania ludności oraz jej ewakuacji;
- przygotowania obiektów ochronnych;
- zaopatrywania ludności w sprzęt i środki ochrony indywidualnej;
- chronienia dóbr niezbędnych do przetrwania;
- organizowania akcji ratunkowych i likwidacji skażeń.

Podsystem pozamilitarny przeznaczony jest do tworzenia niezbędnych warunków przygotowania i działania sił zbrojnych oraz funkcjonowania pozostałych struktur państwa.

W nowych realiach obronnych przywiązuje się coraz większą wagę do roli układu pozamilitarnego w systemie obronności. Stąd struktura tego układu, podobnie jak sił zbrojnych, ulega dynamicznym przeobrażeniom. Jednocześnie w całokształcie przygotowań obronnych dostrzega się coraz częściej rolę i znaczenie przygotowań organizacyjno-mobilizacyjnych układu pozamilitarnego. Przygotowania te rzutują bezpośrednio na wykorzystanie potencjału ludzkiego i rzeczowego na potrzeby obrony, a w konsekwencji na sprawność operacyjną systemu obronności. Usytuowanie i przeznaczenie poszczególnych ogniw układu pozamilitarnego w całości systemu obronności wynika z przypisanych im zadań na rzecz obronności kraju, w tym także zasilania sił zbrojnych.

Stan i możliwości układu pozamilitarnego w znacznym stopniu uzależnione są od potencjału gospodarczego, a także z uwagi na wiodącą w procesie przygotowania państwa do obrony, od wiedzy obronnej kadr kierowniczych. Najważniejsze zadania obronne w czasie pokoju realizują polityczne, gospodarcze i administracyjne struktury państwowe.

Zakłada się, że zaspokajanie potrzeb sił zbrojnych i ludności w warunkach wojny wymaga podporządkowania gospodarki narodowej celom wojennym. Konieczne będzie czuwanie nad wielkością i asortymentem produkcji dóbr podstawowego użytku i dystrybucją tych dóbr. Wówczas szczególnego znaczenia nabierze funkcjonowanie administracyjnych struktur państwa oraz sprawność konwersji gospodarki na tory wojenne.

Układ pozamilitarny obejmuje ogniwa obronne, a w tym ochrony ludności i struktur państwa, gospodarcze i polityczne, które realizują określone zadania obronne. Jednakże z uwagi na brak ostatecznych ustaleń co do nowej struktury omawianego układu dla potrzeb przygotowań

JAWNE
Zastrzeżone

organizacyjno-mobilizacyjnych wyodrębniono następujące ogniwa obronne układu pozamilitarnego, a mianowicie:

- pozamilitarne ogniwa gospodarczo-obronne; w skład których wchodzą jednostki organizacyjne podległe ministrom, wojewodom i organom samorządu terytorialnego oraz podmioty gospodarcze objęte programem mobilizacji gospodarki;
- pozamilitarne ogniwa ochrony struktur państwa, które tworzą głównie wyspecjalizowane jednostki organizacyjne resortu spraw wewnętrznych i administracji;
- pozamilitarne ogniwa ochrony ludności wchodzące w struktury organizacyjno- funkcjonalne obrony cywilnej.

Pominięto tu ogniwa polityczno-obronne (polityczne i społeczne), a także niektóre organa (Trybunał Konstytucyjny, Najwyższą Izbę Kontroli, sądownictwo i prokuraturę). Nie ujmując bardzo ważnej roli, jaką spełniają te organa, instytucje i organizacje w systemie obronności państwa zauważa się, że nie są one reprezentatywne dla zobrazowania istoty przygotowań organizacyjno - mobilizacyjnych, jakie są prowadzone w pozostałych ogniwach układu pozamilitarnego tego systemu.

Pozamilitarne ogniwa gospodarczo-obronne

Ogniwa gospodarczo-obronne zapewniają niezbędny poziom produkcji i usług zorientowanych na cele obrony, jak również wykonywanie określonych zadań mobilizacyjnych. Tworzą warunki do optymalnego zaspokojenia materiałowych potrzeb państwa na czas wojny, w tym zasilania sił zbrojnych, ogniw ochrony struktur państwa i formacji obrony cywilnej. Ogniwa gospodarczo-obronne planują, gromadzą i utrzymują w tym celu rezerwy państwowe i specjalistyczne zgodnie z wymogami obronnymi. W czasie pokoju przygotowują i utrzymują zdolność organizmów gospodarczych do produkcji i świadczenia usług zapewniających osiągnięcie niezbędnego stopnia gotowości obronnej państwa. Ogniwa gospodarczo-obronne tworzą też niezbędne warunki do stopniowego zwiększania wysiłku w razie zagrożenia i wojny. Utrzymują i rozbudowują infrastrukturę techniczną, energetyczną, komunikacyjną i telekomunikacyjną. Proces włączania zasobów ekonomicznych państwa do realizacji przygotowań mobilizacyjnych uzasadnia konieczność ich programowania i planowania w ramach średniookresowego planu jakim jest program mobilizacji gospodarki. Podstawę jego opracowania stanowią potrzeby obronne zgłaszane przez uprawnione organa państwowe.

Program mobilizacji gospodarki dotyczy m.in. takich problemów, jak: produkcja przemysłowa, rolnictwo, skup, zaopatrzenie ludności, transport i łączność oraz służba zdrowia.

JAWNE
Zastrzeżone

Ważnym elementem tego programu są dostawy wojenne, realizowane przez ogniwa gospodarczo-obronne na rzecz sił zbrojnych w postaci dostaw podstawowych rodzajów uzbrojenia, amunicji oraz części zamiennych do uzbrojenia, a także usług w postaci remontów sprzętu wojskowego.

Nadzór i koordynację zadań obronnych realizowanych w ogniwach gospodarczo-obronnych, w tym określonych zadań na korzyść sił zbrojnych, sprawują ministrowie i wojewodowie. Organa te kierują ponadto całokształtem przedsięwzięć organizacyjno-mobilizacyjnych zapewniających warunki do wykonywania zadań gospodarczo-obronnych w resortach i województwach.

W razie podwyższania gotowości obronnej państwa kierować będą procesami osiągania gotowości przez podległe jednostki organizacyjne i nadzorowane podmioty gospodarcze do funkcjonowania w czasie wojny. Struktura i obszar działania ogniw gospodarczo-obronnych są specyficzne dla każdego z nich i nie podlegają podziałowi terytorialnemu sił zbrojnych na okręgi wojskowe i terytorialnemu podziałowi kraju.

Pozamilitarne ogniwa ochrony struktur państwa

Ogniwa ochrony struktur państwa tworzą organa centralne podporządkowane MSWiA wraz z podległymi jednostkami resortu spraw wewnętrznych i administracji, a więc Policja, Urząd Ochrony Państwa, Państwowa Straż Pożarna, Straż Graniczna. Przeznaczone są one do wykonywania zadań na rzecz ochrony struktur państwa. Ich struktura organizacyjna i obszar działania, z wyjątkiem Straży Granicznej i wojsk MSWiA, są dostosowane do podziału administracyjnego państwa. Centralnymi ogniwami ochrony struktur państwa są komendy główne: Policji, Państwowej Straży Pożarnej, Straży Granicznej oraz Szefostwo Urzędu Ochrony Państwa. Terenowym aparatem Policji i Państwowej Straży Pożarnej są komendy wojewódzkie, a Urzędu Ochrony Państwa - wojewódzkie delegatury lub delegatury UOP. Komendantom wojewódzkim Policji i Państwowej Straży Pożarnej podlegają komendanci miejskich, dzielnicowych i gminnych posterunków Policji oraz komendanci jednostek i pododdziałów Państwowej Straży Pożarnej.

Policja przeznaczona jest do zapewnienia bezpieczeństwa i porządku publicznego, a we współdziałaniu z Urzędem Ochrony Państwa do działań administracyjno-porządkowych zapewniających bezpieczeństwo i ochronę struktur państwa. Do jej zasadniczych zadań w czasie pokoju należy ochrona życia i zdrowia obywateli oraz mienia przed bezprawnymi zamachami naruszającymi te dobra, ochrona porządku wewnętrznego, zapobieganie popełnianiu przestępstw

i wykroczeń, wykrywanie ich i ściganie sprawców, a także udział w akcjach ratowniczych organizowanych podczas klęsk żywiołowych i nadzwyczajnych zagrożeń oraz przygotowanie stanów osobowych do wykonywania zadań obronnych na rzecz sił zbrojnych i obrony cywilnej.

Natomiast w okresie zagrożenia zewnętrznego przewiduje się, że jednostki organizacyjne Policji zabezpieczać będą mobilizacyjne i operacyjne rozwijanie wojsk, w tym rozwinięcie akcji kurierskiej oraz ochraniać trasy przegrupowania wojsk, a także zabezpieczać rozwijanie i funkcjonowanie systemu kierowania państwem, w tym głównie stanowisk kierowania władz naczelnych, centralnych i wojewódzkich. W celu realizacji tych zadań, w razie ogłoszenia mobilizacji lub wybuchu konfliktu zbrojnego przewiduje się sformowanie jednostek manewrowych Policji przeznaczonych głównie do: ochrony wydzielonych dróg manewru wojsk i ewakuacji ludności, zapewnienia porządku w rejonach zagrożenia i prowadzenia akcji ratunkowych oraz w rejonach stanowisk kierowania władz naczelnych, centralnych i wojewódzkich, a także na drogach rozśrodkowania i ewakuacji ludności, jak również udziału w zwalczaniu grup specjalnych, dywersyjnych i desantów powietrznych przeciwnika.

Urząd Ochrony Państwa powołany jest do prowadzenia i ochrony działalności kontrwywiadowczej, ze szczególnym uwzględnieniem rejonów stanowisk kierowania, ważnych dla obronności obiektów militarnych, gospodarczych i komunikacyjnych oraz instytucji narażonych na penetrację obcych służb wywiadowczych. Szefostwo Urzędu Ochrony Państwa, wojewódzkie delegatury i podległe im delegatury UOP wykonują, zadania związane z rozpoznawaniem zagrożeń oraz przeciwdziałaniem ich powstawaniu. Dla organów państwowych i dowództw wojskowych przygotowują niezbędne informacje i analizy dotyczące obronności i wojska, w tym zamiary przeciwnika, jego siły i środki, rejony, zadania grup specjalnych dywersyjnych i desantów powietrznych przeciwnika.

Zakres działań wykonywanych przez Urząd Ochrony Państwa i podległe mu delegatury realizowany jest zgodnie z ustawą o Urzędzie Ochrony Państwa i umową zawartą między resortem spraw wewnętrznych i administracji a resortem obrony narodowej. Urząd Ochrony Państwa ściśle współpracuje ze służbami specjalnymi, kontrwywiadem wojskowym i żandarmerią.

Straż Graniczna przeznaczona jest do ochrony granicy państwowej i realizuje ustawowe zadania w tym zakresie. W czasie pokoju Straż Graniczna podlega ministrowi spraw wewnętrznych i administracji. Po ogłoszeniu mobilizacji i w czasie wojny Straż Graniczna staje się częścią Sił Zbrojnych RP.

Państwowa Straż Pożarna przeznaczona jest do ochrony przeciwpożarowej i uczestniczy w tworzonym Krajowym Systemie Ratowniczo-Gaśniczym. Na okres zagrożenia i wojny PSP rozwija manewrowe jednostki przeciwpożarowe. W razie zagrożenia i w czasie wojny zabezpiecza pod względem przeciwpożarowym mobilizacyjne rozwijanie jednostek wojskowych, chroni opuszczone obiekty koszarowe, składy i inne wydzielone obiekty wojskowe. Do zadań PSP należy też osłona (pod względem przeciwpożarowym) ważnych obiektów infrastruktury obronnej kraju, zwalczanie pożarów w strefach zniszczeń wojennych oraz zabezpieczenie ewakuacji ludności. PSP współdziała w tym zakresie z Policją i obroną cywilną. Z uwagi na włączenie Państwowej Straży Pożarnej do Krajowego Systemu Ratowniczo-Gaśniczego staje się ona jednocześnie istotnym elementem ogniw ochrony ludności.

Pozamilitarne ogniwa ochrony ludności

Ochrona ludności jest konstytucyjnym obowiązkiem wszystkich organów władzy, administracji państwowej i samorządowej, a także obowiązkiem organizacji społecznych i podmiotów gospodarczych, mającym na celu zapewnienie warunków przetrwania i bytu ludności w warunkach różnorodnych zagrożeń. Ogniwa ochrony ludności przeznaczone są do ochrony ogółu społeczeństwa przed zagrożeniami, których źródłem mogą być w czasie pokoju klęski żywiołowe, katastrofy i skażenia, a w czasie wojny ponadto skutki działań zbrojnych. Ochronę cywilną, zgodnie z postanowieniami międzynarodowego prawa wojennego zobowiązuje się m.in. do: organizowania akcji ratunkowych i likwidacji skażeń, organizowania wykrywania zagrożeń, przygotowania obiektów ochronnych oraz zaopatrywania ludności w sprzęt i środki ochrony indywidualnej, a także planowania innych przedsięwzięć w zakresie ochrony życia i zdrowia ludności, ochrony zakładów pracy, urządzeń użyteczności publicznej oraz dóbr kultury przed skutkami działań wojennych. Wprawdzie wyżej wymienione przedsięwzięcia dotyczą ochrony cywilnej, w naszych warunkach praktycznie są one realizowane przez obronę cywilną. Natomiast koordynatorem działań, w ramach systemu obronnego państwa, wszystkich sił i środków służących ochronie życia i mienia ludności oraz dóbr kultury jest Urząd Obrony Cywilnej Kraju podległy ministrowi spraw wewnętrznych i administracji. Obronie Cywilnej Kraju zapewnia się warunki i możliwości sprawnego działania. W tym celu przygotowuje się i wyznacza personel kadrowy, tworzy odpowiednie warunki jego funkcjonowania oraz wyposaża w niezbędne materiały i środki. Organizuje się szkolenie w ogólnym systemie edukacji narodowej w ośrodkach wyspecjalizowanych, w terenowych jednostkach administracji państwowej, samorządu terytorialnego i zakładach pracy. Angażuje się w tym celu także środki

masowego przekazu. Obrona cywilna w czasie wojny zachowuje neutralność zbrojną. Jej zadaniem jest przygotowanie i realizacja działań niosących pomoc ludności, również na terenach czasowo zajętych przez nieprzyjaciela.

Województwa, powiaty i gminy stanowią jednostkę organizacyjną podziału administracyjnego kraju i z tego powodu spełniają kluczową rolę w funkcjonowaniu całego systemu obronności. Na jego obszarze integrowane są pod kierownictwem wojewodów wojewódzkie ogniwa ochrony państwa i ochrony ludności oraz wydzielone z resortów podmioty gospodarcze. Podsystem pozamilitarny spełnia dla podsystemów: kierowania obronnością państwa i militarnego rolę i funkcje bazy gospodarczo-obronnej i logistycznej oraz jest ich ostoją moralno-polityczną. Swoim działaniem obejmuje wszystkie dziedziny związane z gospodarką obronną państwa. Miejsce i rolę poszczególnych elementów pozamilitarnego systemu wyznaczają spełniane przez nich zadania na rzecz sił zbrojnych i obronności kraju.

1.2. Charakterystyka prawdopodobnych zagrożeń systemu obronności państwa

Pojęcia ogólne

Bezpieczeństwo narodowe, nazywane również bezpieczeństwem państwa, jest złożoną funkcją, obejmującą problematykę przeciwstawiania się wszelkim zagrożeniom dla istnienia oraz rozwoju narodu i państwa - zarówno zewnętrznym, jak i wewnętrznym. Obecnie w Europie jak również na świecie jednym ze szczególnie istotnych problemów jest kształtowanie relacji między systemami bezpieczeństwa narodowego i międzynarodowego. Wraz ze zmianami w sferze polityczno - gospodarczej i militarnej w ostatnich latach Polska dąży do zapewnienia sobie bezpieczeństwa w ramach euroatlantyckich struktur bezpieczeństwa międzynarodowego. Możliwe stany w stosunkach międzypaństwowych i międzynarodowych to: bezpieczeństwo, "zimny" pokój, kryzys, "zimna wojna", zagrożenie pozamilitarne, zagrożenie militarne, konflikt zbrojny, wojna.[2] Należy podkreślić, że wejście w struktury wspólnego, euroatlantyckiego bezpieczeństwa nie jest celem samym w sobie, jest ono jedynie etapem i jednym z zadań strategicznych na drodze do zapewnienia możliwości osiągnięcia celu nadrzędnego, jakim jest zagwarantowanie suwerenności i nienaruszalności terytorialnej oraz rozwoju ekonomicznego. W tym celu Rzeczpospolita Polska utrzymuje i doskonali swój system bezpieczeństwa, a w tym głównie system obronności państwa.

JAWNE
Zastrzeżone

Skład, struktura i zasady funkcjonowania systemu obronności w czasie pokoju i wojny uwarunkowane są szeregiem różnorodnych czynników, wśród których najistotniejsza jest ocena ewentualnych zagrożeń i wynikających z nich potrzeb obronnych, a także kierunku działań nakreślonych przez politykę bezpieczeństwa państwa. W literaturze system obronności państwa definiowany jest jako:

- zbiór wzajemnie powiązanych elementów (ludzi, organizacji i urządzeń) działających narzecz zachowania bezpieczeństwa i nienaruszalności terytorialnej kraju.[3]
- „zbiór powiązanych ze sobą ogniw aparatu państwowego (ludzi, organizacji, urządzeń) pełniących różne funkcje, działających pod kierownictwem władz zgodnie z doktryną obejmującą przygotowanie obronne kraju (lub w ramach ewentualnej koalicji)".[4]
- "skoordynowany wewnętrznie zbiór wzajemnie powiązanych elementów organizacyjnych, ludzkich i materiałowych, działających na rzecz osiągania i utrzymania w państwie stanu uznanego powszechnie za bezpieczny".

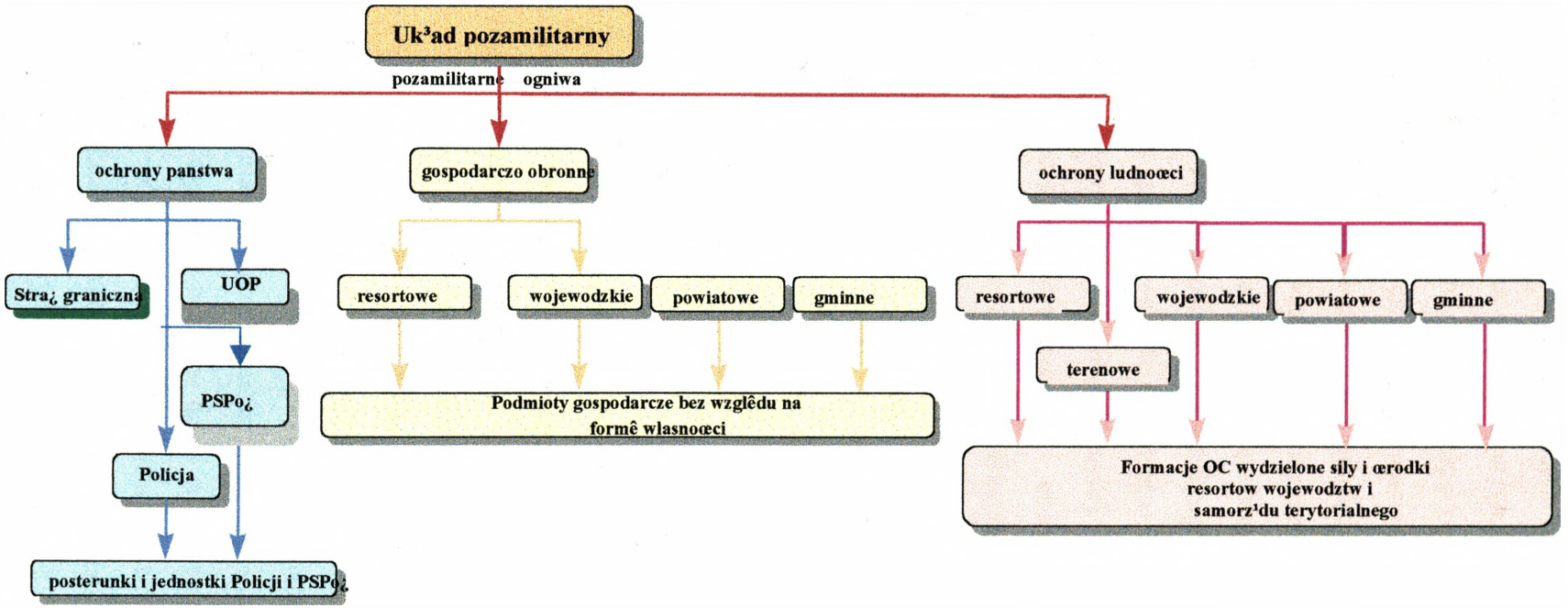
System obronności państwa, zdefiniowany w ramach pracy studyjnej[5] to: „zbiór wzajemnie powiązanych elementów - ludzi, organizacji, urządzeń - działających na rzecz bezpieczeństwa państwa", natomiast bezpieczeństwo państwa definiowane jest jako - "zdolność państwa do ochrony jego wartości przed zagrożeniami".

Przytoczona definicja rozszerza poprzednie i określa, że: "System obronności RP stanowią elementy potencjału obronnego własnego i ewentualnie sojuszniczego, połączone celem politycznym, zapewniającym historycznie uwarunkowaną suwerenność i niepodległość narodu polskiego, jego prawa do integralności terytorialnej i nienaruszalności granic państwa". Niekiedy definicja systemu związana jest z doktryną obronną przez stwierdzenie, że: "stanowi (on) podstawę sprawowania przez państwo funkcji obronnej i ma na celu przygotowanie - zgodnie z przyjętą doktryną obronną - całego społeczeństwa, gospodarki narodowej, obszaru kraju i sił zbrojnych do działania na rzecz bezpieczeństwa narodowego i nienaruszalności terytorialnej kraju, a także skutecznego zapobiegania lub przeciwstawienia się każdej agresji."[6]

---

[2] Opracowano na podstawie pracy n-b "KAPPA". AON Warszawa 1996 (załącznik 2)
[3] Balcerowicz B. Słownik podstawowych terminów dotyczących bezpieczeństwa państwa, AON Warszawa 1996
[4] Zubek J, Doktryny Bezpieczeństwa, AON 1992
[5] Praca zbiorowa "Perspektywiczny model systemu obronnego państwa. Kierunki. System pojęć" AON, Warszawa 1992.
[6] Komański A, Dworecki S, Piedziuk E, Perspektywiczny model systemu obronnego państwa. Kierunki, AON Warszawa 1993.

JAWNE
Zastrzeżone



Rys.1.5. Struktura podsystemu pozamilitarnego (wariant)

JAWNE

Zastrzeżone

JAWNE
Zastrzeżone

Generalnie rzecz ujmując wszystkie te definicje, w sposób bezpośredni lub bardziej opisowy, określają system obronności, w tym również system obronności RP, głównie jako:

- zbiór elementów szeroko rozumianego potencjału obronnego (sił, środków, organizacji itp.) realizujących określone cele i zadania na rzecz obronności kraju;
- powiązania i wzajemne zależności pomiędzy elementami tego zbioru;

Podstawowym warunkiem skutecznego działania w dziedzinie bezpieczeństwa i obronności jest jednolita interpretacja podstawowych pojęć i kategorii.

Bezpieczeństwo polityczne - obejmuje przygotowanie naczelnych organów władzy i administracji państwowej do przeciwstawienia się zagrożeniom politycznym państwa (zarówno wewnętrznym, jak i zewnętrznym). Bezpieczeństwo państwa obrazuje rys. 1.6.

Bezpieczeństwo cywilizacyjne - obejmuje przygotowanie gospodarki państwa do przeciwstawienia się zagrożeniom ekonomicznym. [7]

Obronność (czyli bezpieczeństwo obronne lub wojenne) - przygotowanie struktur państwa, zwłaszcza sił zbrojnych, do skutecznego przeciwstawienia się zagrożeniom wojennym.

Bezpieczeństwo społeczne (cywilizacyjne), w tym ekologiczne - obejmuje przygotowanie i utrzymywanie gotowości struktur państwa do przeciwstawienia się wszelkim zagrożeniom cywilizacyjnym, w tym ekologicznym oraz likwidacji skutków katastrof ekologicznych.

Bezpieczeństwo publiczne - obejmuje przygotowanie i utrzymywanie sił i środków do przeciwstawienia się wszelkim zagrożeniom struktur państwa, porządku publicznego, ochrony życia i zdrowia obywateli.

Rodzaje i właściwości zagrożeń wpływają bezpośrednio na charakter i treść bezpieczeństwa narodowego, a także i kategorii wobec niego pochodnych. [8] Najogólniej zagrożenia dzieli się na zewnętrzne i wewnętrzne (ze względu na ich źródło). W konsekwencji wyróżnia się bezpieczeństwo zewnętrzne i wewnętrzne. Zagrożenia wojenne i militarne wymagają głębszej analizy, zarówno ze względu na ich charakter, jak i niosące ze sobą skutki. Zagrożenia militarne dzieli się na realne i potencjalne. Zagrożenia wojenne są szczególnym rodzajem zagrożeń państwa, skierowane są bowiem w podstawy istnienia narodów i państw. Zagrożenia wojenne to zestaw różnorodnych zagrożeń występujących jednocześnie, wśród których główną rolę odgrywa zagrożenie militarne. Zagrożenie wojenne jest pojęciem szerszym niż zagrożenie militarne, ponieważ wojna, zwłaszcza wojna

---

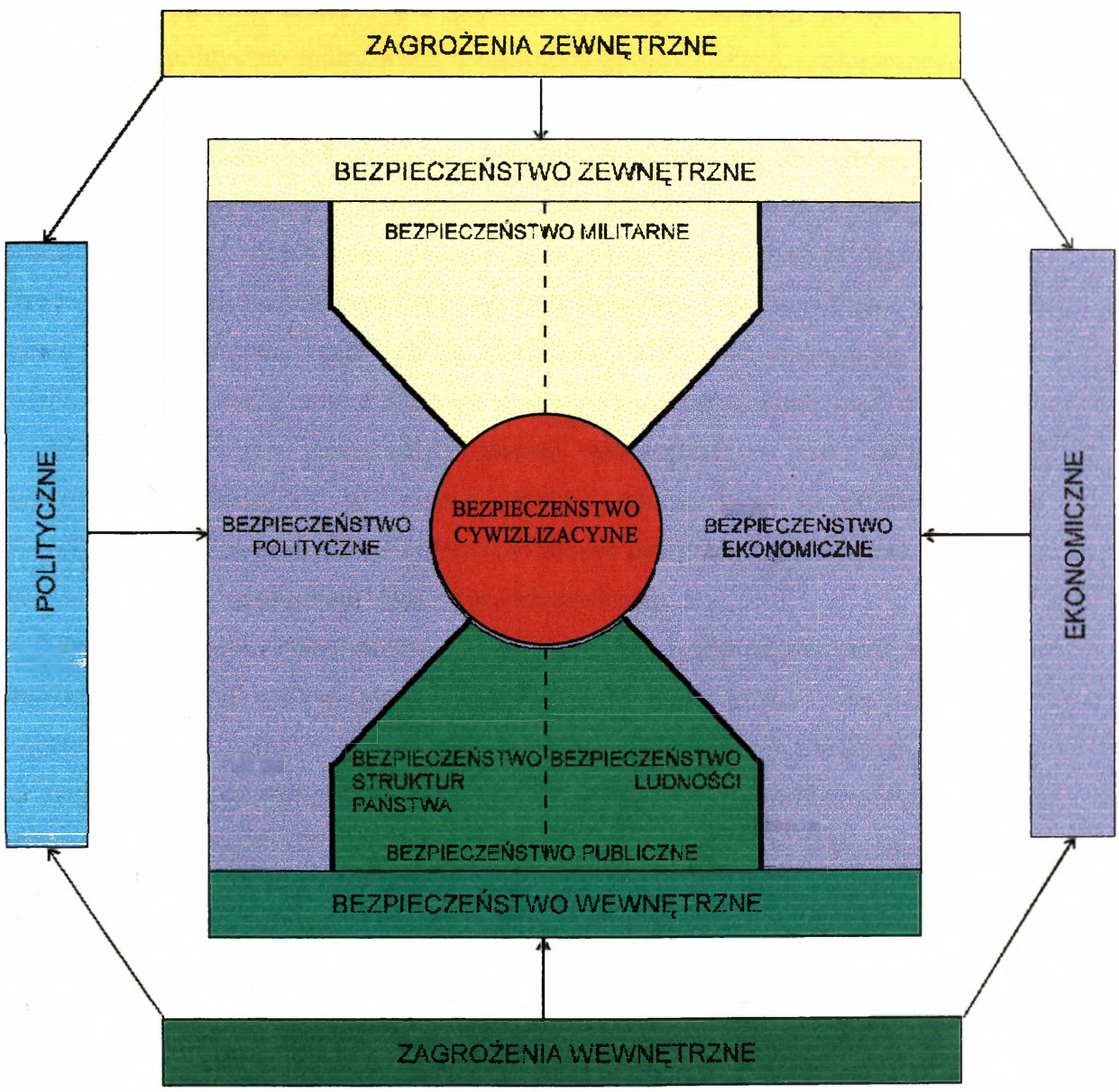
[7] Nożko K, Sztuka tworzenia przewagi w systemie obronnym RP. Bellona, Warszawa 1994.

[8] Koziej S., Wołkowicz F., Podstawowe założenia polityki bezpieczeństwa i strategii obronnej. AON. Warszawa 1998

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

współczesna, obejmuje nie tylko działania zbrojne, ale także różnorodne działania poza zbrojne (społeczne, ekonomiczne, informacyjne itp.). Groźba agresji nie należy wprawdzie do zagrożeń dnia dzisiejszego, ale nie może być też wykluczona. Specjalną odmianą zagrożeń wojennych, obecnie bardzo aktualną, są zagrożenia kryzysowe, będące następstwem kryzysu polityczno-militarnego w otoczeniu państwa, czyli w sytuacji, w której co prawda nie występuje groźba bezpośredniej agresji na dane państwo, ale która stwarza zagrożenia pośrednie.



Rys.1. 6. Bezpieczeństwo państwa[9] (wariant)

JAWNE

[9] Koziej S., Wołkowicz F., Podstawowe założenia polityki bezpieczeństwa i strategii obronnej. AON. Warszawa 1998

Zastrzeżone

JAWNE
Zastrzeżone

Obronność (obrona narodowa) jest szczególną dziedziną bezpieczeństwa narodowego, czyli taką funkcją państwa, która dotyczy przeciwstawiania się wszelkimi posiadanymi środkami (militarnymi i pozamilitarnymi) zagrożeniom wojennym, a przede wszystkim militarnym, stanowiącym sedno zagrożeń wojennych.

Kształtowanie obronności (obrony narodowej) odbywa się w ramach realizacji polityki, strategii i doktryny obronnej. Te trzy kategorie pojęciowe należą do podstawowych kategorii z zakresu obronności. Zarówno bezpieczeństwo państwa jako całość, jak i wszystkie jego dziedziny mają swoją politykę, strategię i doktrynę, co oznacza, że polityka i strategia bezpieczeństwa państwa składa się z polityki i strategii obronnej, polityki i strategii bezpieczeństwa: polityczno-społecznego, ekonomicznego, publicznego, ekologicznego itp.[10]

Obrona narodowa - w ujęciu funkcjonalnym - to zapobieganie i przeciwdziałanie zagrożeniom i ich skutkom. Zagrożenia utożsamia się z wieloma zjawiskami. Raz obok napięć społecznych wymienia się wojnę, innym razem wojna traktowana jest jako takie samo zagrożenie jak handel narkotykami. Wydaje się, że wiele zjawisk stanowi zagrożenie, lecz istotny jest stopień ich szkodliwości - wpływu na byt i rozwój społeczny. Z tego też względu w czasie pokoju, kryzysu i wojny istnieją zagrożenia podobne lub różniące się co do skali i rodzaju, przy czym wojna sama w sobie stanowi najwyższą formę zagrożenia.[11]

Polityka obronna (obronności, obrony narodowej) - jako część polityki bezpieczeństwa państwa - to zespół działań informacyjno - propagandowych, dyplomatycznych, ekonomicznych, militarnych i innych prowadzonych przez państwo w celu przeciwstawienia się zagrożeniom wojennym i ich skutkom.

Strategia obronna (obronności, obrony narodowej) - jest częścią polityki obronnej i jednocześnie częścią szerszej strategii bezpieczeństwa narodowego. Zajmuje się ona sposobami realizacji polityki obronnej. Jej istotą jest optymalizacja użycia sił i środków wydzielonych przez państwo do realizacji celów i zadań określonych przez politykę. Oznacza to stosowne korygowanie ustalonych celów, wydzielanych środków oraz przyjmowanych sposobów postępowania państwa w dziedzinie obronności.

Doktryna obronna (obronności, obrony narodowej) - stanowi polityczno-strategiczny zestaw obowiązujących w danym czasie celów obronnych oraz zasad i założeń ich osiągania, jest jednocześnie częścią szerszej doktryny bezpieczeństwa narodowego. Doktryna obronności - opublikowana w oficjalnych dokumentach państwowych zawiera w swej istocie strategiczną decyzję co do podstawowych zasad i założeń polityki obronnej, czyli co do

---

[10] Koziej S., Wołkowicz F., Podstawowe założenia polityki bezpieczeństwa i strategii obronnej. AON. Warszawa 1998

[11] Kitler W. Obrona narodowa. Konieczność nowego podejścia. Zeszyty Naukowe.AON. Warszawa 1997

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

możliwości przeciwdziałania zagrożeniom wojennym, w tym zagrożeniom kryzysowym. W tej sytuacji problematyka reagowania kryzysowego staje się podstawowym składnikiem współczesnych koncepcji doktrynalnych w dziedzinie obronności. Dalszym skonkretyzowaniem i uszczegółowieniem strategii i doktryny obronnej jest strategia i doktryna militarna. Ich wyróżniającą cechą jest rodzaj środka obronnego, jakim są siły zbrojne.

Strategia militarna zajmuje się sposobami przygotowania i użycia sił zbrojnych do realizacji zadań obronnych. Odpowiednio - doktryna militarna - stanowi obowiązującą koncepcję strategiczną przygotowania (utrzymywania) i użycia sił zbrojnych.

Systemem obronności państwa nazywamy całość sił i środków, jakie państwo wydziela do realizacji zadań obronnych. Są to zarówno siły i środki militarne (siły zbrojne), jak i pozamilitarne (cywilne).

Gotowość obronna państwa - to stan systemu obronności określający zdolność tego systemu do planowego i zorganizowanego działania na wypadek zagrożenia bezpieczeństwa kraju i w czasie wojny. Według innej definicji gotowość obronna państwa - to taki stan przygotowania wszystkich elementów jego systemu obronności, który zapewnia bezpieczeństwo i rozwój państwa w każdym okresie jego funkcjonowania.[12] Gotowość obronna może być: stała, podwyższona, wzmożona i pełna.

1. Gotowość obronna podsystemu kierowania obronnością państwa obejmuje:
- centralne, resortowe i wojewódzkie stanowiska kierowania;
- przechodzenie na wojenny system kierowania obronnością państwa.
2. Gotowość bojowa sił zbrojnych obejmuje:
- wojska operacyjne;
- jednostki OT.
3. Gotowość obronna ogniw pozamilitarnych obejmuje:
- siły ochrony państwa;
- siły gospodarczo-obronne;
- siły obrony cywilnej.

Przygotowania obronne jest to całość przedsięwzięć, jakie prowadzone są w państwie w czasie pokoju, aby przygotować system obronny do realizacji zadań w wypadku zagrożenia i wojny. W odniesieniu do podstawowych pojęć i kategorii bezpieczeństwa państwa można było ustalić następującą systematykę.

---

[12] J. Zubek, J. Wojnarowski, Przygotowanie i prowadzenie wojny obronnej przez Polskę po 2000 roku, praca n-b "KAPPA", AON, Warszawa 1996

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

1. *Bezpieczeństwo narodowe (państwa)* - jako przeciwstawienie się wszelkim zagrożeniom przy użyciu wszystkich posiadanych przez państwo sił i środków.
2. *Obronność* – jako przeciwstawienie się zagrożeniom wojennym, w tym również kryzysowym, przy użyciu wszystkich (militarnych i pozamilitarnych) sił i środków, jakie państwo wydziela do realizacji tych zadań.
3. *Bezpieczeństwo militarne* - jako przeciwstawienie się zagrożeniom militarnym przy użyciu sił zbrojnych.

Relacje i zależności między bezpieczeństwem państwa a obronnością są hierarchicznie zależne, natomiast między polityką i strategią występują bardzo wyraźne wzajemne uwarunkowania.

Źródła oraz charakter wyzwań i zagrożeń

Bezpieczeństwo narodowe i jego zagrożenia mają obecnie charakter nie tylko militarny. We współczesnym świecie znacznie zmniejszyło się prawdopodobieństwo wybuchu wojny powszechnej. Nie oznacza to jednak całkowitego uwolnienia się od konfliktów. Konflikty zbrojne nadal stanowią zagrożenie, ale o znacznie mniejszej skali i innym charakterze. Skutki takich konfliktów przenoszone się bezpośrednio na sąsiadujące państwa, wywołując kryzys natury politycznej, militarnej, ekonomicznej, społecznej itp.

Równie niebezpieczne dla funkcjonowania państwa są zagrożenia spowodowane działaniami żywiołów oraz zachowaniem ludzi. W ustawodawstwie niektórych państw określa się je jako nadzwyczajne zagrożenia wewnętrzne, do których zalicza się: zagrożenia ustroju konstytucyjnego, zagrożenia bezpieczeństwa i porządku publicznego, klęski żywiołowe, nieszczęśliwe wypadki o znamionach klęski żywiołowej. Przyczyny powstawania zagrożeń przedstawiono na rys.1.7.

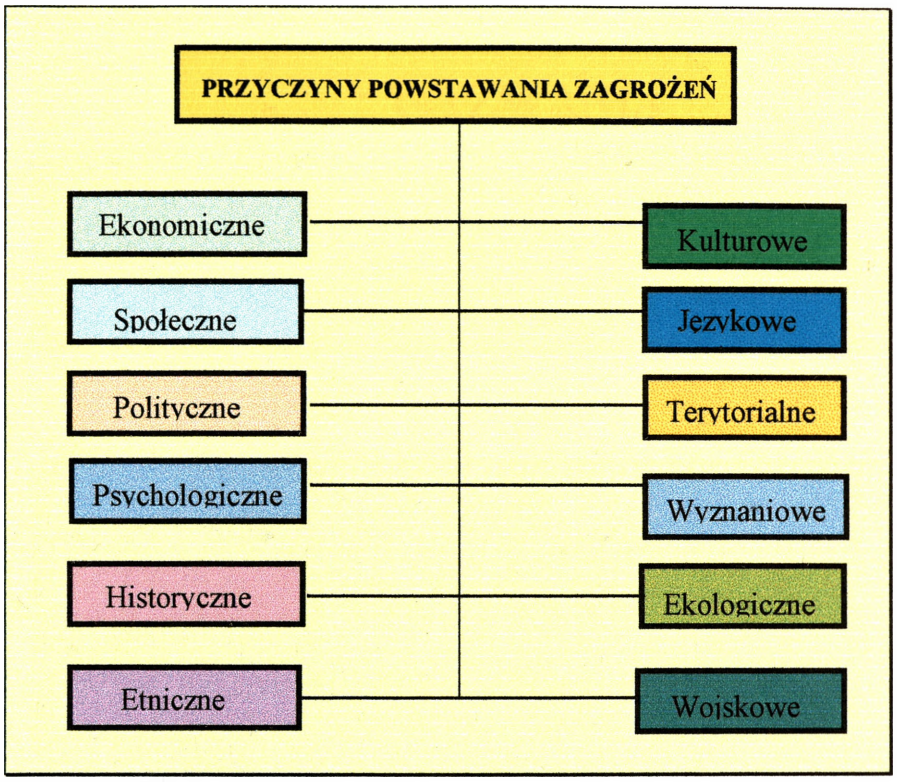
W Polsce przyjęto umownie wyróżniać dwa podstawowe rodzaje zagrożeń, jako najbardziej rzutujące na bezpieczeństwo państwa:

1. polityczno-militarne;
2. pozamilitarne, w skład których wchodzą:
   - zagrożenia ustroju konstytucyjnego;
   - zagrożenie ładu i porządku publicznego;
   - nadzwyczajne zagrożenia środowiska (kryzysy polityczno-cywilizacyjne).

Polska nie traktuje nikogo jako wroga, celowo przygotowującego się do agresji na nasze terytorium, ani też nie deklaruje się być przeciwnikiem jakiegokolwiek państwa. Bierze jednak pod uwagę istniejące obiektywnie, niezależne od woli politycznej i intencji innych państw i narodów potencjalne źródła zagrożeń w bliższym i dalszym otoczeniu strategicznym,

JAWNE
Zastrzeżone

w stosunku do których opracowuje stosowne koncepcje i plany przeciwdziałania oraz utrzymuje niezbędny do ich realizacji potencjał obronny. Polska, jako państwo graniczne NATO może być obiektem oddziaływań różnorakich zagrożeń nie tylko skierowanych przeciwko niej bezpośrednio, ale także przeciwko innym państwom Sojuszu usytuowanym w głębi strategicznej (Rys. 1.8.). W ocenie warunków swej obronności Polska bierze pod



Rys.1.7. Przyczyny powstawania zagrożeń[13] (wariant)

uwagę zarówno polityczno-militarne wyzwania czasu pokojowego, jak i zewnętrzne zagrożenia kryzysowe oraz zagrożenia wojenne (wśród nich groźba wojny lokalnej i powszechnej). Do podstawowych wyzwań polityczno-militarnych czasu pokoju należą:

- ponoszenie niezbędnych wysiłków na utrzymanie odpowiedniego, jakościowego i ilościowego poziomu potencjału obronnego, tak aby minimalizować groźbę szantażu politycznego, zapobiegać redukcji pozycji międzynarodowej państwa oraz zapewniać realne wsparcie dyplomacji w bieżących zabiegach o skuteczną realizację ważnych interesów Polski na arenie międzynarodowej;

[13] Dworecki S., "Od konfliktu do wojny", BUWIK, Warszawa 1996.

JAWNE
Zastrzeżone

Rys.1.8. Wyzwania i zagrożenia (wariant)

JAWNE
Zastrzeżone

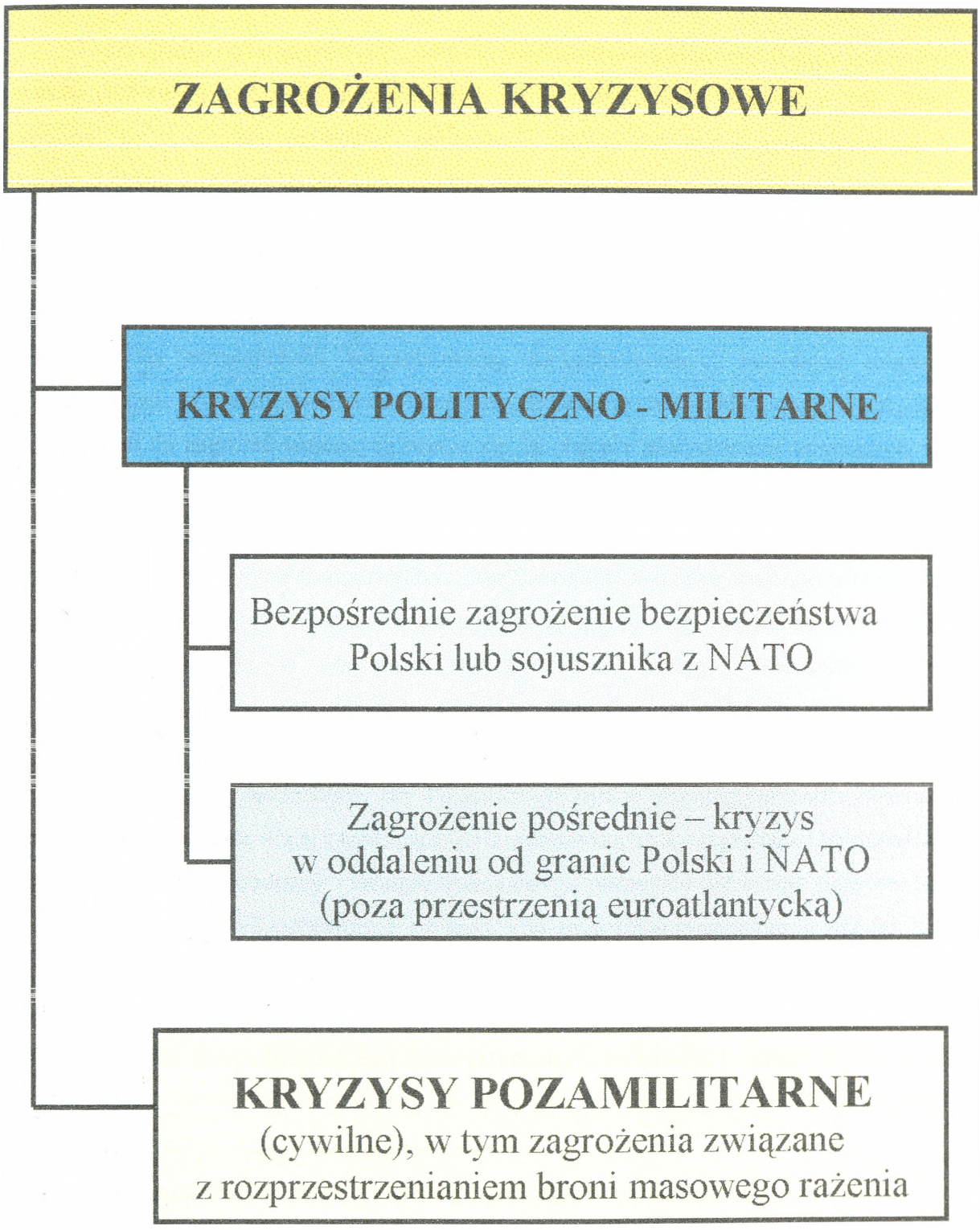
- wnoszenie istotnego wkładu w umacnianie instytucji i organizacji międzynarodowych działających w sferze obronnej, w tym w dziedzinie kontroli zbrojeń, rozbrojenia oraz budowy zaufania, a także ponoszenia kosztów kontynuowania udziału Polski w międzynarodowych operacjach pokojowych;
- przełamywanie uprzedzeń i kształtowanie dobrosąsiedzkich stosunków w sferze militarnej z państwami bliższego i dalszego otoczenia.

Szczególne znaczenie mają wyzwania związane z koniecznością ponoszenia wysiłków na rzecz utrwalania i rozwinięcia uzyskanych w wyniku członkostwa w NATO korzystnych, zewnętrznych uwarunkowań obronności państwa. Wymagać to będzie systematycznego zapewnienia stosownego do potencjału Polski, wkładu w system obrony tak, aby wzmacniać siły i wiarygodność obronną Sojuszu oraz wiarygodność Polski. Wyzwaniem jest również ponoszenie kosztów kontynuowania udziału Polski w międzynarodowych operacjach pokojowych. W okresie pokoju mogą wystąpić również wyzwania wiążące się z zagrożeniami ponad narodowymi takimi jak: niekontrolowane rozprzestrzenianie broni masowego rażenia (nuklearnej, biologicznej, chemicznej), zagrożenia dla życia polskich obywateli oraz bezpieczeństwa polskich obiektów państwowych znajdujących się poza granicami RP, następstwa katastrof naturalnych oraz ekologicznych, terroryzm. W odpowiedzi na te zagrożenia i wyzwania państwo będzie zmuszone wykorzystać swój potencjał obronny.

Po zakończeniu „zimnej wojny" głównym niebezpieczeństwem dla stabilności międzynarodowej stały się zagrożenia kryzysowe. Mogą one mieć charakter wewnątrzpaństwowy, jak i międzypaństwowy. Ich oddziaływanie na bezpieczeństwo Polski będzie się przejawiało bezpośrednio -jeśli tego rodzaju kryzysy i konflikty będą miały miejsce w bezpośrednim otoczeniu naszego państwa lub pośrednio - jeśli wystąpią one z dala od naszych granic. Źródłem tego rodzaju zjawisk mogą być napięcia polityczne, ekonomiczne, etniczne, religijne, czy też spory graniczne (Rys. 1.9.)

Kryzys o charakterze bezpośredniego zagrożenia bezpieczeństwa Polski lub jej sojuszników może mieć charakter ukrytej lub jawnej groźby użycia przemocy. Może on zmierzać do wymuszenia określonych ustępstw (rewizja granic, zmiany terytorialne, zaspokojenie celowo wygórowanych żądań grup etnicznych i wyznaniowych). Działania takie polegać mogą na prowokowaniu zbrojnych wystąpień państwa w obronie swojej racji stanu. Jedną z metod osiągnięcia zakładanych celów może być destabilizacja sytuacji wewnętrznej. Odmowa spełnienia żądań, roszczeń lub innych warunków, brak woli uzyskania satysfakcjonującego porozumienia może w konsekwencji doprowadzić do bezpośredniego konfliktu militarnego.

JAWNE
Zastrzeżone



Rys. 1.9. Zagrożenia kryzysowe (wariant)

JAWNE
Zastrzeżone

Wnioski

W przypadku wystąpienia kryzysów w bezpośrednim otoczeniu, Polska może być narażona zarówno na oddziaływania militarne, jak i pozamilitarne. Pierwsze z nich mogą przejawiać się w postaci: prowokacji militarnych, incydentów granicznych, przypadków naruszania granicy przez zbrojne ugrupowania, naruszania polskiej przestrzeni powietrznej i polskich wód terytorialnych, prowadzenia w bliskości polskiej granicy działań zbrojnych, przenikania lub działania na polskim terytorium grup terrorystycznych lub sabotażowo-dywersyjnych. Oddziaływania pozamilitarne w takiej sytuacji mogą mieć charakter: rozszerzenia się przestępczości zorganizowanej, niekontrolowanych masowych migracji ludności, skażeń promieniotwórczych, chemicznych lub zakażeń epidemiologicznych, itp. W odniesieniu do zagrożeń wojennych ocenia się, że obecnie zdecydowanie zmniejszyła się groźba wybuchu wojny globalnej i konfliktu ogólnoeuropejskiego. Nie można jednak wykluczyć pojawienia się takiej ewentualności w odleglejszej perspektywie czasowej. W rezultacie porozumień rozbrojeniowych poziom uzbrojenia konwencjonalnego w otoczeniu Polski uniemożliwia przeprowadzenie z zaskoczenia agresji na dużą skalę. Zagrożenie takie mogłoby być wykryte ze znacznym wyprzedzeniem. Dlatego ewentualna agresja z zaskoczenia może mieć głównie wymiar lokalny. Odnosi się to także do groźby agresji na któregokolwiek naszego sojusznika z NATO.

Jest zatem mało prawdopodobne, aby Polska mogła być w nieodległym czasie obiektem agresji militarnej na dużą skalę, zagrażającej jej suwerenności oraz integralności terytorialnej, a także wymagającej mobilizacji i zaangażowania całego potencjału obronnego państwa. Nie można jednak wykluczyć odtworzenia się tego typu zagrożenia wojennego w strategicznie dalszej przyszłości. Większe natomiast jest obecnie prawdopodobieństwo niespodziewanego wystąpienia zagrożenia o małej skali, lokalnego naruszenia terytorium Rzeczypospolitej Polskiej lub wręcz przypadkowego incydentu granicznego, do którego mogłoby dojść w razie niebezpiecznego rozwoju sytuacji w bezpośrednim otoczeniu strategicznym Polski. Agresja zbrojna zależnie od jej skali może przybrać formy:

- kampanii zaczepnej na pełną skalę w wymiarze lądowym, powietrznym i morskim;
- ograniczonej operacji zaczepnej na jednym kierunku;
- uderzeń rozproszonych (na kilku kierunkach) o ograniczonym rozmachu;
- działań grup dywersyjno-rozpoznawczych (nieklasycznych uderzeń) na wybranych kierunkach, rajdów grup zbrojnych o różnym składzie i wyposażeniu, aktów dywersji i innych niekonwencjonalnych działań bojowych.

Zastrzeżone

Z większym prawdopodobieństwem można przewidywać wystąpienie konfliktu lokalnego bądź regionalnego w otoczeniu Polski. Może on być wynikiem trudności w transformacji systemowej w niektórych państwach naszego regionu. Zagrożeniem dla Polski, nawet gdyby znalazła się poza bezpośrednią strefą konfliktu, byłoby przeniesienie działań militarnych lub ich skutków na nasze terytorium. Konflikty tego rodzaju charakteryzować się mogą stosunkowo krótkim czasem przygotowań oraz zmienną intensywnością od pierwszych dni działań zbrojnych. Pozbawione kontroli i ograniczeń politycznych konflikty lokalne mogą prowadzić do eskalacji, angażowania innych państw i przekształcenia się w konflikt regionalny. Celem starć zbrojnych zwaśnionych stron może być opanowanie spornego terytorium lub wymuszenie ustępstw na płaszczyźnie politycznej czy też ekonomicznej. W razie objęcia Polski takim konfliktem należy się liczyć z możliwością selektywnych uderzeń lotniczych i rakietowych oraz aktów terroru na całym terytorium państwa, a nawet zajęcia jego części.

Niebezpieczeństwo konfliktów regionalnych i lokalnych potęgują zagrożenia pozamilitame. Ich znaczenie, zasięg oraz rodzaj wykazują tendencje wzrostową przybierając rozmiar regionalny, a nawet kontynentalny. Narastającym objawom degradacji społecznej w niektórych państwach objętych transformacją ustrojową towarzyszą zjawiska patologii, tworzenia sprzyjających warunków do rozwoju międzynarodowej przestępczości zorganizowanej, obejmującej swoim zasięgiem całe regiony. Najbardziej niebezpieczną formą zagrożenia wynikającą z międzynarodowej aktywności przestępczej staje się terroryzm przybierający różne oblicza i zakładający różne cele. Następstwem działań przestępczości międzynarodowej stają się także zorganizowany przemyt, korupcja struktur władzy, handel narkotykami oraz potencjalne skażenie środowiska mogące wystąpić na skutek nielegalnego obrotu materiałami rozszczepianymi, chemicznymi lub biologicznymi.

Polska w coraz większym stopniu narażona będzie na problemy związane z rozprzestrzenianiem technologii podwójnego zastosowania, broni masowego rażenia i środków jej przenoszenia. Problemy te będą występować zarówno w okresie pokoju w aspekcie położenia geograficznego kraju, który stanowi obszar tranzytowy przy nielegalnym obrocie technologiami i materiałami służącymi do produkcji BMR, jak też w okresie kryzysu i wojny, gdy BMR może być użyta przez potencjalnego agresora na dowolnym obszarze państwa. Ważnym czynnikiem kształtującym bezpieczeństwo militarne Polski będzie również postęp technologiczny w dziedzinie zbrojeń.

Zastrzeżone

JAWNE
Zastrzeżone

2. KIEROWANIE OBRONNOŚCIĄ PAŃSTWA - STAN AKTUALNY

2.1. Rola, miejsce i zadania podsystemu kierowania obronnością państwa

W celu zapewnienia możliwości przeciwstawiania się zagrożeniom wojennym, zgodnie z celami i zadaniami obrony, Polska utrzymuje na czas pokoju oraz rozwija na czas kryzysu i wojny system obronności państwa. Jednym z jego głównych elementów jest podsystem kierowania obronnością.

Podsystem kierowania obronnością (obroną narodową) przeznaczony jest do formułowania celów i zadań oraz planowania, organizowania i koordynowania działań wszystkich struktur państwowych w ramach przygotowania i utrzymywania na odpowiednim poziomie potencjału obronnego państwa w czasie pokoju oraz sprawnego rozwijania i skutecznego wykorzystywania tego potencjału w okresach zewnętrznego zagrożenia kryzysowego i wojny. System kierowania obronnością tworzą organa władzy oraz administracji rządowej i samorządowej, a także ośrodki kierowania gospodarką, z przypisanymi im ustawowo kompetencjami. W procesie kierowania obronnością uczestniczą organa władzy ustawodawczej, wykonawczej i organa samorządu terytorialnego. Podstawowe funkcje w tym zakresie określa konstytucja oraz ustawy. Do najważniejszych należy zaliczyć:

- ustalanie zadań obronnych, zasad ich wykonywania oraz wykonawców poprzez opracowanie i wydawanie aktów normatywno-prawnych;
- działalność organizatorska w zakresie przygotowań obronnych, obejmująca podejmowanie decyzji oraz sprawowanie nadzoru i kontroli.
- podział kompetencji oraz przydzielone na obronność środki finansowe.

We współczesnych warunkach Prawidłowe spełnianie tych funkcji warunkuje stan prawny w państwie, precyzyjny szczególne znaczenie ma podsystem kierowania reagowaniem kryzysowym. Jego zbudowanie jest jednym z ważniejszych zadań rządowych.

2.2. Charakterystyka wybranych elementów podsystemu kierowania

Podstawowym atrybutem suwerenności Rzeczpospolitej Polskiej jest posiadanie własnego potencjału obronnego. Potencjał ten opiera się na utrzymywanym w czasie pokoju i rozwijanym na okres stanów zagrożenia państwa systemie obronności.

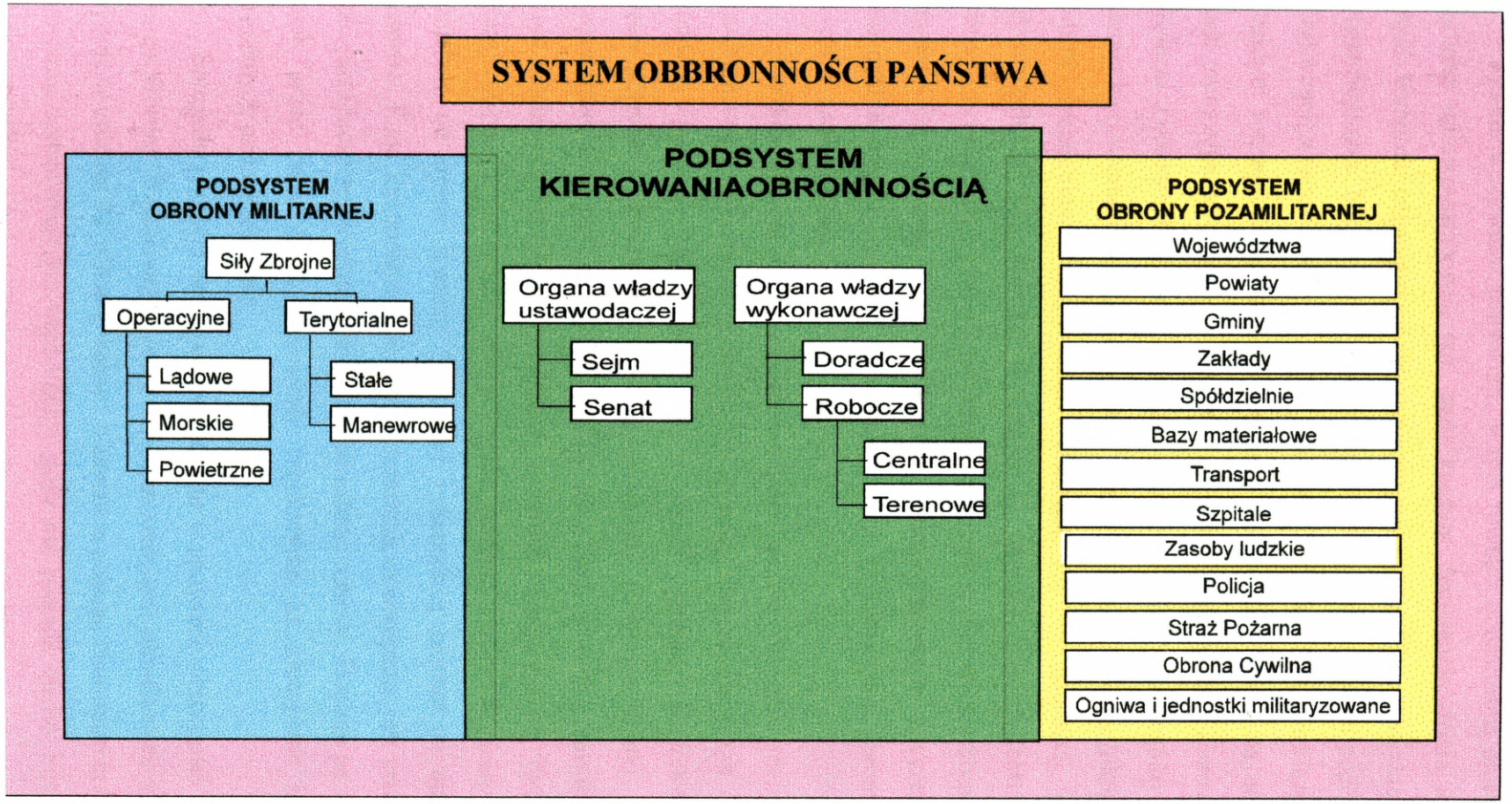
JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Podział elementów zbioru systemu na trzy podstawowe podsystemy (elementy) nie budzi kontrowersji i u większości autorów jest podobny. Wszystkie elementy systemu obronności państwa są przyporządkowane poszczególnym podsystemom - głównie zaś podsystemowi obrony militarnej i pozamilitarnej. Złożoność działania systemu obronności, a zwłaszcza wspólne wykonywanie niektórych zadań obronnych, powoduje, że systemy te w pewnych warunkach przenikają się wzajemnie. Szczególną rolę pełni podsystem kierowania obronnością państwa, który integruje działanie pozostałych podsystemów. Jednocześnie wybrane główne elementy podsystemu militarnego i pozamilitarnego są elementami podsystemu kierowania obronnością kraju. Podsystem kierowania obronnością, rozumiany jako uporządkowana integralna całość, której elementami są sprzężone ze sobą informacyjnie organa i techniczne środki kierowania oraz dowodzenia, jest częścią systemu obronności państwa, który przedstawiono na rys. 2.1. Strukturę podmiotową podsystemu 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 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. Ściśle z tym związany jest wybór odpowiedniej strategii obronnej, co w konsekwencji wiąże się z wielkością potencjału obronnego państwa utrzymywanego w czasie pokoju.

W kierowaniu obronnością obowiązują określone zasady. Jedną z nich jest zasada niezmienności struktur organów kierowania. Dąży się, aby kierowanie obronnością państwa w okresie wojny opierało się na tej samej strukturze organów władzy i administracji rządowej, co w czasie pokoju. Zasada jednoosobowego podejmowania decyzji i ponoszenia za nie odpowiedzialności szczególnie ważna jest w okresie kryzysu i wojny, gdzie przede wszystkim potrzebne jest zachowanie tajemnicy, skrócenie czasu podejmowania decyzji i szybkie jej realizowanie. Powyższe nie może prowadzić do wniosku, że udział organów kolegialnych w podejmowaniu decyzji jest zbędny.

JAWNE
Zastrzeżone



Rys. 2.1. Elementy systemu obronności państwa

JAWNE

Zastrzeżone

JAWNE
Zastrzeżone

System kierowania państwem, w tym również obronnością opiera się w większości na strukturze liniowo-sztabowej, tzn. przy każdym decydencie działa komórka organizacyjna (zespół komórek organizacyjnych) wykonująca czynności o charakterze przygotowawczym i organizacyjnym. Nie zwalnia to jednak decydenta od osobistego podejmowania decyzji i od konsekwencji z tego wynikających. W kierowaniu obronnością obowiązują podobne zasady jak w każdym rodzaju kierowania. 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 uchwalanych przez Radę Ministrów oraz w dotychczas obowiązujących uchwałach Komitetu Obrony Kraju. Zgodnie z postanowieniami zawartymi w wyżej wymienionych aktach poszczególne organa sprawują określone funkcje w kierowaniu obronnością Rzeczpospolitej Polskiej w czasie pokoju.

Parlament jest organem stanowiącym prawo, w tym również prawo dotyczące bezpieczeństwa i obronności państwa. W głównej mierze, decyduje o wielkości potencjału obronnego państwa utrzymywanego w czasie pokoju. Wszelkie decyzje dotyczące bezpieczeństwa i obronności państwa powodują określone skutki głównie ekonomiczne i gospodarcze, a nieraz także polityczne i inne. Stąd, w tych sprawach, szczególnie w czas 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.Zgodnie z postanowieniami określonymi w Konstytucji RP Sejm decyduje w imieniu RP o stanie wojny i o zawarciu pokoju. Natomiast parlament bezpośrednio w kierowaniu obronnością nie uczestniczy, gdyż nie posiada on jak i jego komisje uprawnień wykonawczych.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Prezydent Rzeczypospolitej Polskiej i Rada Ministrów – jako organy sprawujące władzę wykonawczą, są naczelnymi organami kierowania obronnością i wykonują swoje zadania w tym zakresie na podstawie Konstytucji RP. Zgodnie z Konstytucją, prezydent stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium. Jest on najwyższym zwierzchnikiem Sił Zbrojnych Rzeczpospolitej Polskiej. Jego organem doradczym w zakresie bezpieczeństwa wewnętrznego i zewnętrznego jest Rada Bezpieczeństwa Narodowego. Rada Ministrów prowadzi politykę wewnętrzną i zagraniczną Rzeczpospolitej Polskiej, zapewnia jej bezpieczeństwo wewnętrzne i zewnętrzne oraz sprawuje ogólne kierownictwo w dziedzinie obronności.

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 kieruje obronnością w czasie pokoju, współdziałając z prezydentem Rzeczpospolitej Polskiej w ramach prowadzenia polityki wewnętrznej i zagranicznej. Organem opiniodawczo-doradczym Rady Ministrów w tym zakresie jest Komitet Spraw Obronnych Rady Ministrów. W razie konieczności realizacji zadań szczególnych, wynikających bądź to z potrzeb wyłącznie narodowych, bądź też wykonywanych w ramach NATO lub innych organizacji międzynarodowych, mogą być wprowadzane dodatkowe procedury i tworzone doraźne struktury operacyjne (komitety, zespoły, komisje, pełnomocnicy, itp.).

Minister Obrony Narodowej kieruje resortem obrony narodowej, w tym przede wszystkim całokształtem działalności Sił Zbrojnych Rzeczpospolitej Polskiej. Przygotowuje projekty założeń obronnych państwa oraz sprawuje ogólne kierownictwo w sprawach wykonywania powszechnego obowiązku obrony. Koordynuje i sprawuje ogólny nadzór, w zakresie powierzonym przez Radę Ministrów, nad realizacją zadań obronnych przez organa administracji publicznej, samorządy, instytucje, podmioty gospodarcze (przedsiębiorców) i inne jednostki organizacyjne.

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

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

użycia sił zbrojnych, a także za ich gotowość bojową i mobilizacyjną. Do obowiązków szefa Sztabu Generalnego należy również współuczestniczenie w opracowywaniu 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 dotychczas szczeblem równorzędnym dowództw rodzajów sił zbrojnych były 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 rolę i miejsce w hierarchii dowodzenia siłami zbrojnymi.

System dowodzenia siłami zbrojnymi Polski, członka Paktu Północnoatlantyckiego, wymaga usprawnienia i dostosowania do standardów w nim przyjmowanych. Wiąże się to również z wydzielaniem wojsk operacyjnych do wielonarodowych związków operacyjnych podporządkowanych dowództwu NATO. Wydzielane wojska powinny zatem posiadać 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.

Wojewoda 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 porządku publicznego, a także zapobiegania klęskom żywiołowym oraz usuwania ich skutków. Wojewodzie jako szefowi Obrony Cywilnej Województwa bezpośrednio podporządkowany jest Wojewódzki Inspektorat Obrony Cywilnej. Podsystem

JAWNE
Zastrzeżone

kierowania obronnością państwa obejmuje ośrodki decyzyjne, mające ściśle określone uprawnienia i zadania w dziedzinie obronności, są to:

- parlament (Sejm i Senat);
- urząd prezydenta;
- urząd premiera;
- urząd ministra obrony;
- dowódca sił zbrojnych.

W niektórych opracowaniach do podsystemu kierowania obronnością państwa zalicza się:

- organa samorządu terytorialnego;
- kierowników podległych i nadzorowanych jednostek organizacyjnych wykonujących zadania obronne.

W literaturze przedmiotu podsystem kierowania obronnością kraju jest wielokrotnie nazywany podsystemem koordynacji polityki bezpieczeństwa państwa. Wynika to niewątpliwie z racji spełnianych przez niego funkcji. Do elementów tego systemu wliczane są więc często wybrane komórki ww. organów, bezpośrednio uczestniczące w procesie kierowania, takie jak.:

- komisje obrony narodowej - sejmowa i senacka;
- Biuro Bezpieczeństwa Narodowego;
- Rada Bezpieczeństwa Narodowego;
- Rada Ministrów;
- Komitet Spraw Obronnych Rady Ministrów itp.

Reasumując, zbiór elementów systemu kierowania obronnością państwa ograniczony jest:

- organami naczelnej władzy państwowej - od góry:
  - ustawodawczej;
  - wykonawczej;
  - sądowniczej (poglądy autorów)
- przedstawicielami władzy wykonawczej - od dołu na poziomie:
  - poszczególnych ministerstw;
  - dowódcy sił zbrojnych;
  - wojewodów;
  - starostów;
  - burmistrzów;

– kierowników ważniejszych jednostek organizacyjnych wykonujących zadania obronne.

Sprawność systemu kierowania obronnością państwa zależy od jednoznaczności zakresu obowiązków i odpowiedzialności jego poszczególnych ogniw i osób funkcyjnych. Ogólny schemat systemu kierowania obronnością przedstawiono na rys. 2.2.

Podstawowym zadaniem systemu dowodzenia siłami zbrojnymi jest zapewnienie ciągłości, operatywności i skrytości kierowania. Spełnienie tych zadań jest uwarunkowane wcześniejszym przygotowaniem i w odpowiednim czasie rozwinięciem infrastruktury technicznej systemu, którą stanowi sieć, odpowiednio wyposażonych w zautomatyzowane podsystemy wspomagania procesów kierowania, stanowisk dowodzenia oraz łączący je podsystem łączności. Struktura organizacyjna systemu ma typowy charakter hierarchiczny (liniowo - sztabowy); na jej czele znajduje się urząd prezydenta - zwierzchnika sił zbrojnych. Strukturę systemu kierowania siłami zbrojnymi w różnych stanach przedstawiono na rysunkach 2.3, 2.4, 2.5. a strukturę wojennego systemu dowodzenia na rys. 2.6. W rozwiązaniach proponowanych przez niektórych autorów, przewiduje się istnienie strategicznego szczebla dowodzenia o strukturze hierarchicznej, który jednocześnie stanowi organiczny element systemu kierowania obronnością państwa. W ramach wojennego systemu dowodzenia prezydentowi bezpośrednio podlega naczelny dowódca SZ RP, który z kolei poprzez struktury Sztabu Generalnego dowodzi okręgami wojskowymi rodzajami wojskDokonywana obecnie zmiana organizacji sił zbrojnych, a zwłaszcza powołanie Dowództwa Wojsk Lądowych, wpłynęło na zmianę struktury dowodzenia wojskami. Wariantowa koncepcja systemu dowodzenia została przedstawiona w pracy "Perspektywiczny model systemu obronnego państwa" pk. Kraj. Wojenny system dowodzenia przewiduje trzy szczeble dowodzenia SZ:

- strategiczny, z jednym organem dowodzenia naczelnego wodza - Sztabem Generalnym SZ;
- operacyjny, z organami dowodzenia rodzajów sił zbrojnych i okręgów wojskowych;
- taktyczny, z organami dowodzenia związków taktycznych, oddziałów i pododdziałów.

Kierowanie w okresie kryzysu

Konflikty zbrojne nie dotyczą tylko i wyłącznie zwaśnionych stron. Skutki konfliktów o różnym charakterze przenoszą się bezpośrednio na sąsiadujące państwa, a nieraz na inne państwa znacznie oddalone od rejonu konfliktu, wywołując kryzysy natury politycznej, militarnej, ekonomicznej, gospodarczej, społecznej itp.

Ogólny termin "kryzys" ma wiele znaczeń i bywa często uzywany w języku potocznym, w publicystyce, a także w badaniach naukowych w rozmaitych kontekstach. W trzech

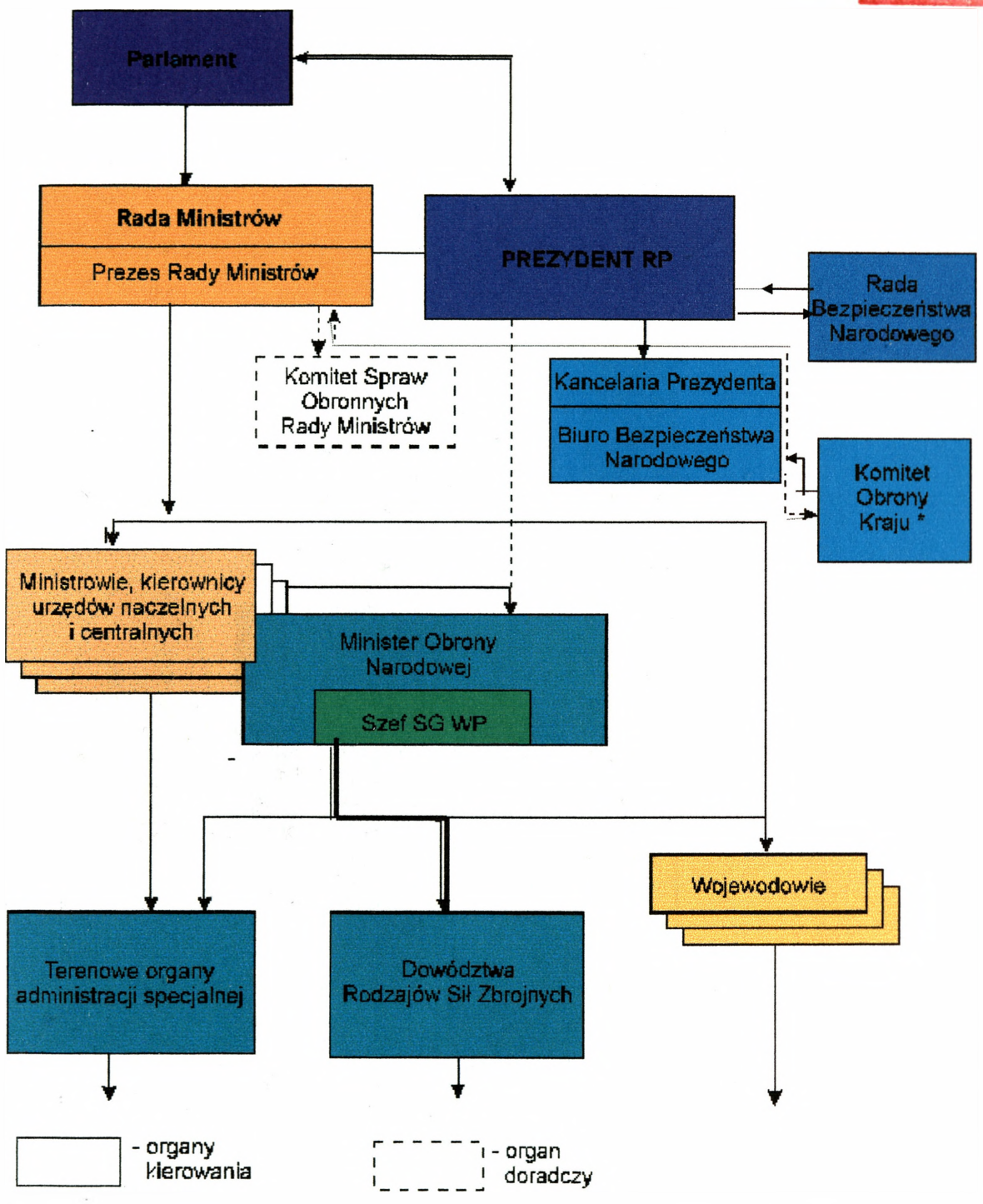
JAWNE
Zastrzeżone

dziedzinach jest jednak kryzys najczęściej przedmiotem rozważań, a mianowicie: ekonomii, polityce i socjologii. Od kilkunastu lat kryzys jest przedmiotem szczególnego zainteresowania strategii obronnej, traktowany w sposób interdyscyplinarny, z uwzględnieniem aspektów związanych z użyciem środków wojskowych i konsekwencji, jakie ono niesie dla bytu i rozwoju społeczeństwa (państwa). Termin "kryzys polityczno-militarny" wiąże się z wieloma zróżnicowanymi sferami życia społeczeństwa i państwa. Z tego względu powinien być ujmowany jako szczególna postać kryzysu politycznego. Kryzys polityczno-militarny jest kryzysem politycznym i jednocześnie konfliktem zbrojnym, realizowanym na poziomie niższym niż wojna. "Szczególne działania władz politycznych" w okresie kryzysu - to całokształt środków polityki o charakterze walki, zastosowanych przez władze polityczne celem jego rozwiązania, licząc od momentu sformułowania żądań strony przeciwnej, których państwo nie może lub nie chce spełnić, aż do zakończenia sporu. Obejmować one mogą cały repertuar środków polityk, stosowanych w okresie pokoju, ale znaczna ich część bezpośrednio służy niszczeniu lub wyeliminowaniu przeciwnika jako strony konfliktu.

Wspólną cechą środków polityki stosowanych w kryzysie jest łączenie w pewną całość elementów walki zbrojnej i niezbrojnej. To samo czyni strona przeciwnika. Taka sytuacja nadaje funkcjonowaniu państwa zazwyczaj, choć nie zawsze, formę stanu wyjątkowego. Wspólną cechą środków polityki stosowanych w kryzysie jest łączenie w pewną całość elementów walki zbrojnej i niezbrojnej. To samo czyni strona przeciwnika. Taka sytuacja nadaje funkcjonowaniu państwa zazwyczaj, choć nie zawsze, formę stanu wyjątkowego.[14] Początkiem konfliktu społecznego w skali makro jest moment oficjalnego wyartykułowania żądań strony przeciwnej, których państwo nie chce lub nie może spełnić. Początkiem zaś kryzysu jest moment rozpoczęcia działań jawnie wrogich wobec państwa, nie koniecznie od razu walki zbrojnej. Ta ostatnia zwykle jest odpowiedzią na reakcje władzy politycznej w związku z wrogimi działaniami drugiej strony.

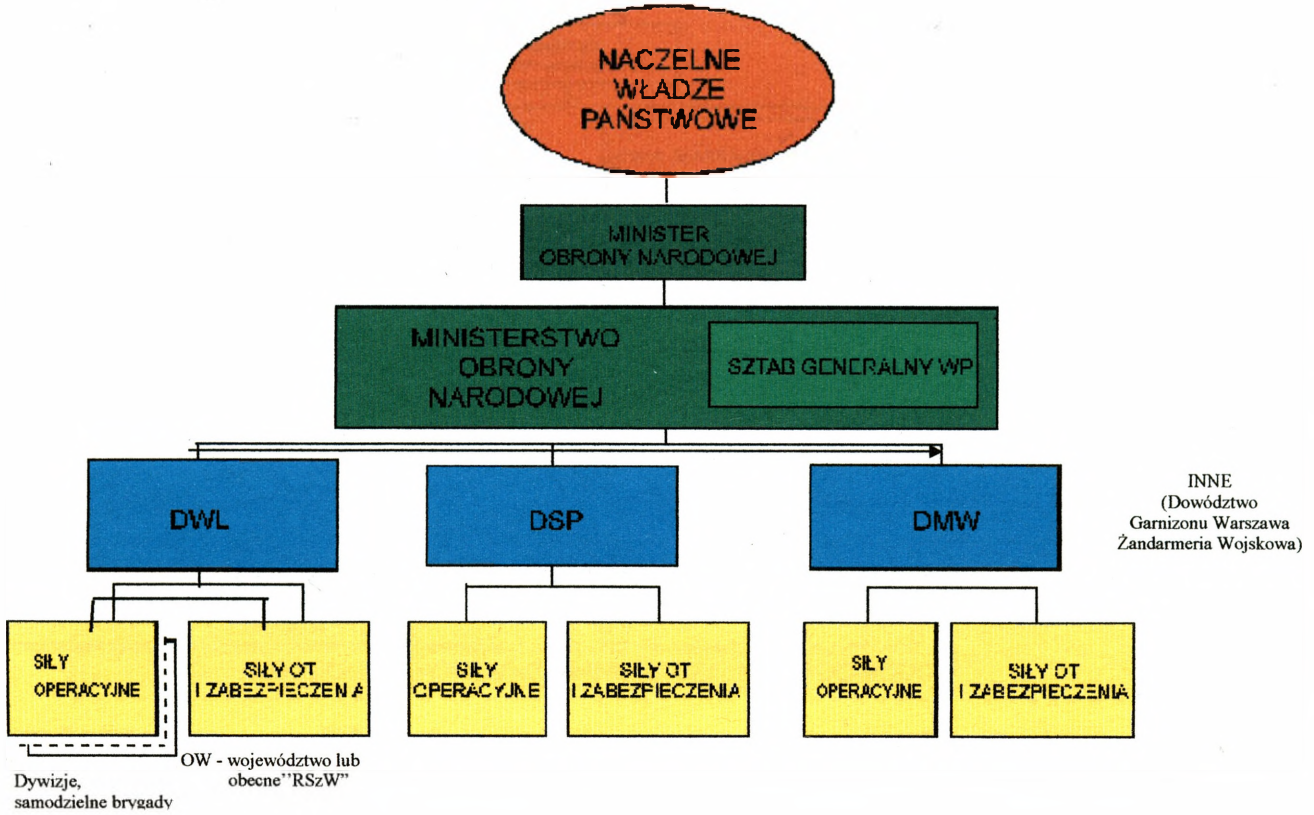
[14] Zgodnie z definicją kryzysu, państwa koalicji antyirackiej zaangażowane w konflikcie zbrojnym z Irakiem znalazły się w sytuacji kryzysowej, chociaż w większości z nich nie było potrzeby wprowadzania stanu wyjątkowego. Dotyczyło to także Polski.

JAWNE
Zastrzeżone



* Dotychczas funkcjonuje. Nowa Konstytucja nie uwzględnia KOK.

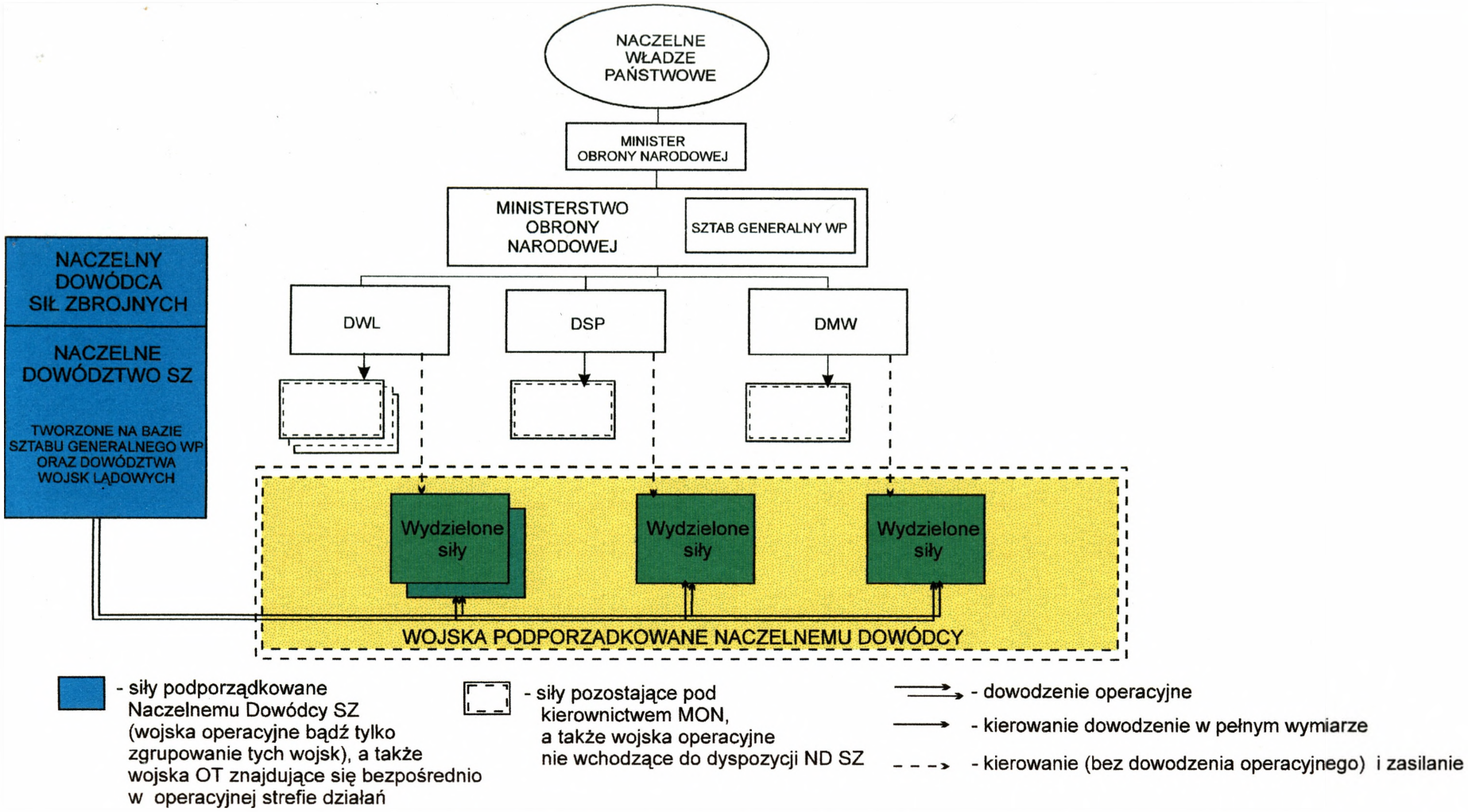
Rys. 2.2. Ogólna struktura systemu kierowania obronnością państwa (wariant)



Rys. 2.3. Struktura systemu kierowania siłami zbrojnymi w czasie pokoju (wariant)

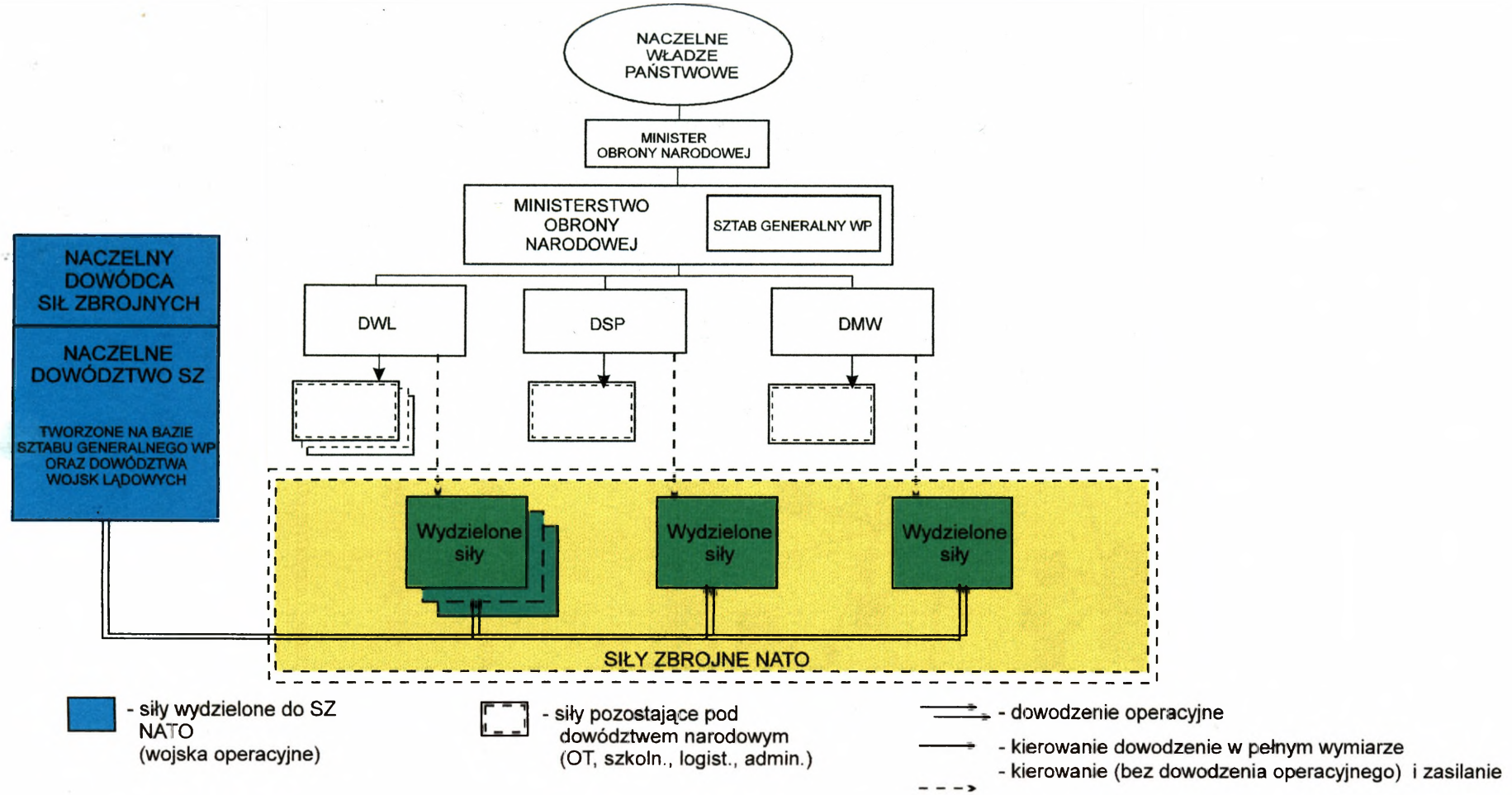
JAWNE

Zastrzeżone



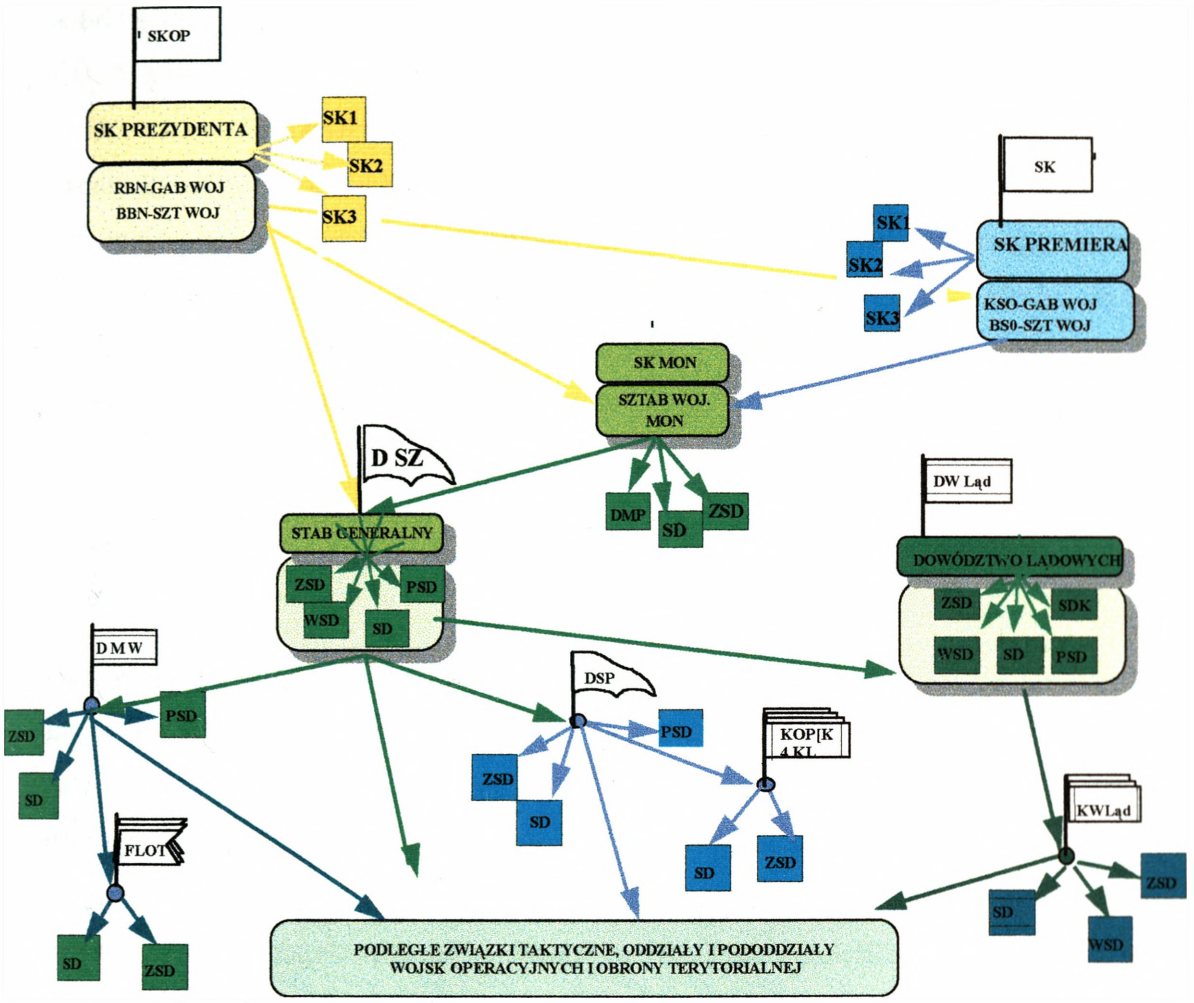
Rys. 2.4. Struktura systemu kierowania siłami zbrojnymi w czasie stnów nadzwyczajnych (wariant przejściowy)

JAWNE
Zastrzeżone



Rys. 2.5. Struktura systemu kierowania siłami zbrojnymi w czasie wojny (wariant uwzględniający struktury NATO)

JAWNE
Zastrzeżone



Rys. 2.6. Struktura wojennego systemu dowodzenia (wariant)

Konflikt społeczny w skali makro kończy się:

- zgodą państwa na żądania drugiej strony;
- kompromisem, czyli wzajemnymi ustępstwami stron konfliktu, tj. z jednej strony ograniczeniem żądań, z drugiej zaś zgoda na ich spełnienie w takiej ograniczonej formie;
- wyeliminowanie strony przeciwnej za pomocą walki.

Trzeba podkreślić iż, zakończenie konfliktu społecznego, którego składową była walka zbrojna, nie jest możliwe bez jej zaprzestania. Kryzys kończy się w tych samych okolicznościach

co konflikt społeczny, a także w wypadku przejścia państwa do wojny, czyli rozszerzenia przez nie arsenału środków (do wymiaru całości lub przeważającej części posiadanych sił).[15]

Tak samo niebezpiecznymi dla funkcjonowania państwa są zagrożenia spowodowane działaniami żywiołów oraz zachowaniem ludzi. W ustawodawstwie niektórych państw określa się je jako nadzwyczajne zagrożenia wewnętrzne do których zalicza się: zagrożenia ustroju konstytucyjnego, zagrożenia bezpieczeństwa i porządku publicznego, klęski żywiołowe, nieszczęśliwe wypadki o znamionach klęski żywiołowej.

Niebezpieczne sytuacje w otoczeniu państwa o różnym charakterze (politycznym, militarnym, społecznym, ekonomicznym, ekologicznym itp.) tworzą sytuacje kryzysowe.

W warunkach Polski przyjęto umownie wyróżniać dwa podstawowe rodzaje zagrożeń jako najbardziej rzutujące na bezpieczeństwo państwa:

1) polityczno-militarne;

2) pozamilitarne, w skład których wchodzą:

- zagrożenie ustroju konstytucyjnego,
- zagrożenie ładu i porządku publicznego,
- nadzwyczajne zagrożenie środowiska (kryzysy przyrodniczo-cywilizacyjne).

Zainteresowanie się problematyką kryzysów znalazło odzwierciedlenie w koncepcjach i doktrynach bezpieczeństwa większości państw, w tym Rzeczpospolitej Polskiej. Duże znaczenie przywiązuje się głównie pierwszemu etapowi 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.[16] Żeby 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 art. 230 i 232, gdzie mówi się o środkach nadzwyczajnych w razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli i porządku publicznego lub w celu zapobieżenia skutkom

---

[15] Wróblewski R., Jendraszczak E. Przygotowanie i prowadzenie wojny obronnej przez Polskę po 2000 roku. Praca n-b "Kappa". AON. Warszawa 1996

[16] Tarasiuk B, Czarniecki A, Suwiński W. Kierowanie obronnością państwa w czasie pokoju, kryzysu i wojny. AON, DSO MON Warszawa 1998

JAWNE
Zastrzeżone

katastrof naturalnych i technicznych. 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.

Dotychczas w Polsce nie było zorganizowanego systemu kierowania reagowaniem kryzysowym. Opracowaniem systemu reagowania na zagrożenia kryzysami pozamilitarnymi zajmuje się stały zespół KSORM ds. kryzysowych. Według założeń przewiduje się, że reagowanie na tego rodzaju kryzysy organizowane byłoby przede wszystkim na szczeblu lokalnym, a dopiero w razie potrzeby angażowane byłyby wyższe szczeble administracji państwowej. Siły i środki do przeciwdziałania skutkom kryzysów pozamilitarnych są w większości podporządkowane lub nadzorowane przez ministra spraw wewnętrznych i administracji (Policja, Państwowa Straż Pożarna, Służba Graniczna, Obrona Cywilna), toteż zakłada się, że Stanowisko Kierowania Reagowaniem Kryzysowym ds. kryzysów pozamilitarnych będzie usytuowane w tym resorcie. Będzie ono 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 będzie, aby Stanowisko Kierowania Reagowaniem Kryzysowym ds. kryzysów polityczno-militarnych organizowane było 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. Zakłada się, że na Stanowisku Kierowania Reagowaniem Kryzysowym ds. kryzysów polityczno-militarnych MON (Strukturę Stanowiska Kierowania Reagowaniem Kryzysowym przedstawiono na schemacie 2.7.) będą realizowane następujące zadania:

- zbieranie i opracowanie informacji o sytuacjach politycznych i militarnych;
- diagnozowanie i prognozowanie rozwoju procesów polityczno-militarnych;
- ostrzeganie o symptomach zjawisk zagrażających bezpieczeństwu państwa;
- modelowanie sytuacji kryzysowych oraz weryfikacja planów obronnych;

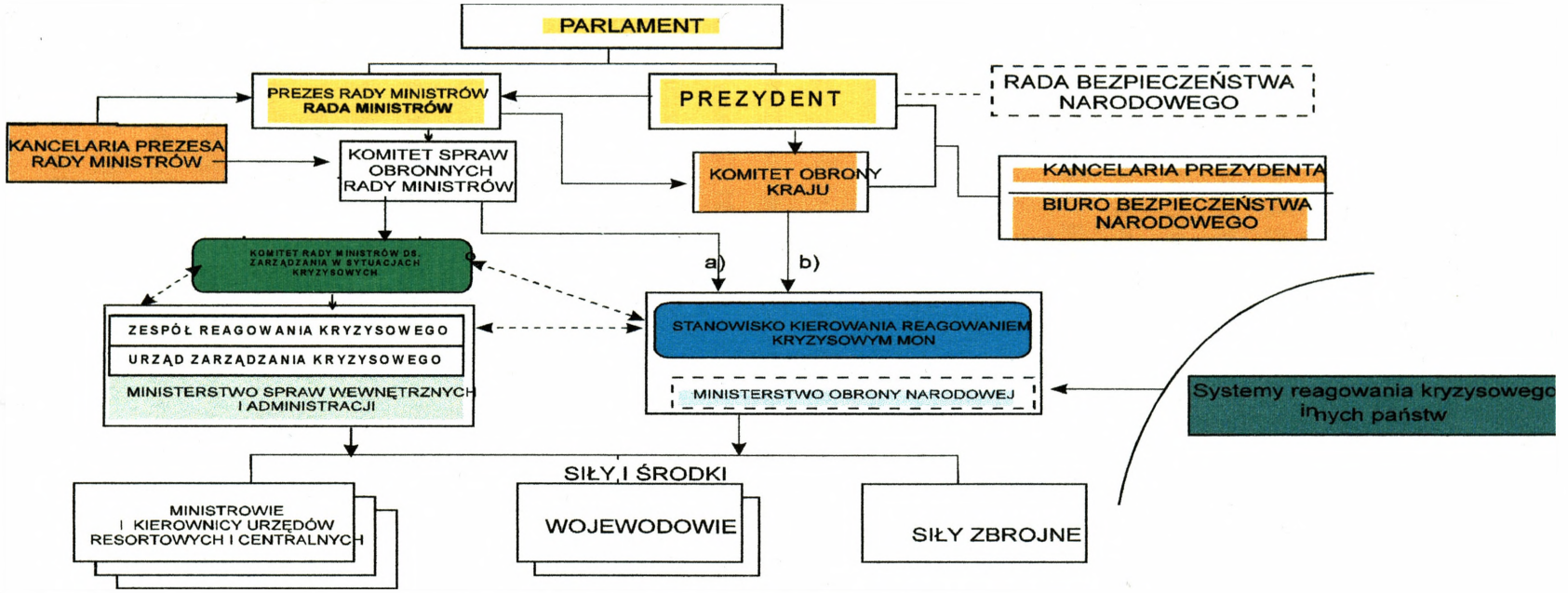
JAWNE
Zastrzeżone

- określanie celów i sposobów działania w sytuacjach narastania zagrożenia bezpieczeństwa państwa;
- opracowanie propozycji użycia sił i środków systemu obronności;
- określenie potrzeb wszechstronnego zabezpieczenia wydzielonych do działań sił zbrojnych;
- opracowywanie i przekazywanie zadań wykonawcom;
- nadzorowanie przygotowań i koordynowanie działań wydzielonych sił i środków do likwidacji kryzysu.

Analizując zadania realizowane przez centrum nasuwa się zasadnicze pytanie - kto będzie dostarczał wiarygodnych informacji? Z doświadczenia wiemy, że wiarygodność informacji trzeba potwierdzić, inaczej mówiąc powinny być one uzyskiwane z kilku źródeł.

Dysponentem takich informacji jest minister spraw zagranicznych, który otrzymuje je bezpośrednio z polskich ambasad, konsulatów i innych placówek dyplomatycznych akredytowanych za granicą. Źródłem informacji dla ministra spraw zagranicznych będą również placówki dyplomatyczne akredytowane w Polsce. Istotne informacje posiada także minister obrony narodowej bezpośrednio z polskich attachatów wojskowych akredytowanych za granicą i kontaktów z attache wojskowymi akredytowanymi w Polsce. Źródłem informacji dla ministra obrony narodowej są również ustawowo podległe Wojskowe Służby Informacyjne. Kolejnym dysponentem informacji jest szef Urzędu Ochrony Państwa, posiadający wyspecjalizowane w tej dziedzinie służby.

Wiarygodne informacje są podstawą prawidłowego działania Stanowiska Kierowania Reagowaniem Kryzysowym MON, warunkują one prowadzenie rzetelnych ocen, analiz i prognoz, co w konsekwencji umożliwia podejmowanie właściwych decyzji. Stanowisko Kierowania Reagowaniem Kryzysowym będzie funkcjonowało głównie dla potrzeb najwyższych organów państwowych. Stąd logicznym będzie, aby w jego strukturze byli przedstawiciele nie tylko ministra obrony narodowej, ale również ministra spraw zagranicznych i szefa urzędu ochrony państwa. Strukturę Stanowiska Kierowania Reagowaniem Kryzysowym MON odzwierciedla schemat, jedną z prawdopodobnych wersji. Struktura ta nie jest ostatecznie ustalona. Jednakże już w etapie koncepcyjno - organizacyjnym można określić, że stałym elementem stanowiska funkcjonującym na co dzień powinien być ośrodek operacyjno-informacyjny i ośrodek analityczno-prognostyczny.



Rys. 2.7. System kierowania reagowaniem kryzysowym[17] (wariant)

JAWNE

17 Tarasiuk B, Czarniecki A, Suwiński W. Kierowanie obronnością państwa w czasie pokoju, kryzysu i wojny. AON, DSO MON, Warszawa 1998

Zastrzeżone

JAWNE
Zastrzeżone

Pozostałe elementy stanowiska powoływane byłyby w wypadku realnego zagrożenia bezpieczeństwa państwa. Utworzone w MON centrum reagowania na kryzysy polityczno-militarne dostarczałoby także informacji organom naczelnym niezbędnych do podejmowania określonych decyzji politycznych i militarnych.

2.3. Procesy i zależności między elementami systemu kierowania

Kierowanie obronnością państwa sprawują wszystkie organa władzy i administracji publicznej stosownie do kompetencji i zadań obronnych przypisanych im w Konstytucji i innych ustawach. Ich wspólnym celem jest przygotowanie i utrzymanie na odpowiednim poziomie potencjału obronnego państwa w czasie pokoju oraz sprawne rozwinięcie i skuteczne wykorzystanie tego potencjału w przypadku zagrożenia bezpieczeństwa państwa i w okresie wojny.

Konstytucja z 2 kwietnia 1997r. nie ustanawia organu, który byłby właściwy w zakresie bezpieczeństwa państwa. Przyjęto natomiast rozwiązanie podziału kompetencji i zadań w tym zakresie, zarówno na Prezydenta RP jak i na Radę Ministrów. Mianowicie Konstytucja określając funkcje ustrojowe prezydenta Rzeczypospolitej Polskiej stwierdza, że prezydent "stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności jego terytorium" (art. 126 ust. 2). Natomiast inny przepis Konstytucji (art. 146 ust. 4 pkt. 8 i 11) stanowi, że Rada Ministrów, w zakresie i na zasadach określonych w Konstytucji i ustawach "zapewnia bezpieczeństwo zewnętrzne państwa", a także "sprawuje ogólne kierownictwo w dziedzinie obronności kraju oraz określa corocznie liczbę obywateli powoływanych do czynnej służby wojskowej".

Doświadczenia, szczególnie z okresu międzywojennego dowodzą, że dla zapewnienia sprawnego koordynowania całokształtem problematyki bezpieczeństwa państwa potrzebny jest jeden centralny ośrodek koordynacyjny. Obecnie funkcje takiego organu spełnia Komitet Obrony Kraju, w którego skład wchodzą najwyżsi przedstawiciele państwa władzy ustawodawczej, a także przedstawiciele rządu, włącznie z premierem i ministrami mającymi wpływ na zdolność obronną i stan bezpieczeństwa państwa.

Pojawiają się poglądy, że Rada Bezpieczeństwa Narodowego mogłaby pełnić rolę koordynacyjną. Jednak przepisy Konstytucji wyraźnie stanowią, że jest ona organem doradczym prezydenta Rzeczypospolitej w zakresie wewnętrznego i zewnętrznego bezpieczeństwa państwa (art. 135). Sama funkcja doradcza organu daje uprawnienia dla Rady jedynie do wyrażania opinii prezydentowi i rekomendowania sposobów rozwiązywania przez

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

niego problemów. Nie pozostawia jednak wątpliwości, że organ ten nie może mieć uprawnień stanowiących. Za rady jakich udzielaliby jej członkowie nie ponosiliby żadnej odpowiedzialności i nie byłyby one również w żadnym stopniu obowiązujące dla prezydenta.

Także Rada Gabinetowa, zwoływana przez prezydenta RP w sprawach szczególnej wagi (tworzy ją Rada Ministrów obradująca pod przewodnictwem Prezydenta RP), nie może spełniać funkcji koordynacyjnej, ponieważ nie przysługują jej kompetencje Rady Ministrów (art. 141). Zważywszy, że Konstytucja przyznaje zarówno prezydentowi Rzeczypospolitej Polskiej jak i Radzie Ministrów kompetencje w zakresie kierowania i odpowiedzialności za bezpieczeństwo i obronność kraju, rodzi się pytanie w jaki sposób trzeba będzie rozstrzygać wszelkie kontrowersje w zakresie tego kierowania i kto mógłby podejmować decyzje, które obowiązywałyby tak prezydenta jak i rząd?

Całokształt kierowania obronnością państwa (w tym dowodzenia siłami zbrojnymi) jest procesem informacyjno-decyzyjnym. System informacyjny sprzęga w jedną spójną całość wszystkie pozostałe elementy składowe systemu kierowania obronnością państwa. Obejmuje siły i środki zdobywania, przetwarzania i przesyłania informacji we własnym systemie obronnym oraz informacyjnego oddziaływania na przeciwnika. Najistotniejszym elementem kierowania i dowodzenia jest decydowanie o najwłaściwszym wykorzystaniu ludzi, broni i sprzętu. Aby sprostać temu zadaniu niezbędne jest zdobywanie, przetwarzanie i przesyłanie informacji, podejmowanie na ich podstawie odpowiednich decyzji, przekazywanie ich wykonawcom oraz zapewnienie warunków ich realizacji.[18]

Integralną część procesu kierowania i dowodzenia stanowią procesy informacyjne, realizowane w obszarze jego funkcjonowania. Podstawowym zadaniem systemu informacyjnego jest obsługa informacyjna zgodna z wymaganiami narzuconymi przez jego użytkowników. Przytoczone określenia wskazują, że bazą systemu informacyjnego jest przede wszystkim system łączności. Dlatego też skuteczność systemu kierowania i zarządzania państwem, sterowania gospodarką narodową, dowodzenia siłami zbrojnymi oraz funkcjonowania organów bezpieczeństwa publicznego jest uzależniona od niezawodnie i efektywnie funkcjonującego systemu łączności państwa. Zdolność wykonywania stojących przed nim zadań zależy między innymi od stanu rozbudowy infrastruktury na obszarze kraju, sprawności organizacyjno-technicznej, przepustowości i niezawodności; szczególnego znaczenia nabierają one w okresie stanów nadzwyczajnych.[19]

---

[18] Kulczycki R., Piedziuk E., Perspektywiczny model kierowania obronnością RP do opracowania koncepcji systemów łączności w SOP, AON, Warszawa 1994

[19] Piedziuk E., Połowniak A., System obronny państwa - struktury organizacyjne dowództw i sztabów oraz organów zarządzania. AON. Warszawa 1996

Zastrzeżone

JAWNE

Zastrzeżone

Należy podkreślić, że obecnie istniejący system obronności państwa nie jest systemem w pełnym znaczeniu tego słowa. Wprawdzie mamy w tym systemie elementy, jednak nie są one dostatecznie powiązane relacjami, zwłaszcza informacyjnymi. A przecież o tym, czy istnieje system decydują właśnie relacje. Relacje informacyjne to nie tylko określone wiadomości, ale także przyjęte normy i procedury działania. scalające funkcjonowanie poszczególnych elementów systemu. Niedostatki tu wymienione dotyczą zwłaszcza podsystemu kierowania obronnością państwa i podsystemu pozamilitarnego. Przykładem jest brak dotąd w Polsce narodowego systemu zarządzania w sytuacjach kryzysowych "crisis management", opartego na normach i procedurach skutecznego działania różnych instytucji państwa w ramach jego systemu obronnego. Model systemu obronności państwa i relacje informacyjne w nim występujące przedstawiono na rys. 2.8.

W centrum uwagi strategów wojskowych pozostają stale takie problemy, jak:

- zdobywanie informacji za pomocą urządzeń elektronicznych;
- zapewnienie ciągłości kierowania państwem i dowodzenia siłami zbrojnymi; zabezpieczenie funkcjonowania systemów sterowania uzbrojeniem;
- utrudnianie pracy i zakłócanie funkcjonowania systemów kierowania państwem i dowodzenia siłami zbrojnymi przeciwnika.

Wynika z tego szerokie spektrum zadań szczegółowych:

1. Zbieranie informacji (poprzez system rozpoznania i odbiór meldunków od podległych struktur organizacyjnych):
   - sytuacji międzynarodowej,
   - przygotowaniach militarnych państw ościennych,
   - aktualnych możliwościach obronnych kraju,
   - rozwoju sytuacji wojennej,
   - stanie rezerw, zapasów i możliwościach odtwarzania gospodarki.
2. Przetwarzanie informacji poprzez odpowiednie kalkulacje, analizy i obliczenia (ręczne, półautomatyczne lub automatyczne):
   - analiza sytuacji międzynarodowej, wojennej i gospodarczej,
   - planowanie obronne i wojskowe,
   - przygotowanie meldunków do nadrzędnych struktur organizacyjnych;
   - przygotowanie dyrektyw, zarządzeń, rozkazów i innych danych do podległych i współdziałających struktur organizacyjnych.
3. Przekazywanie dyrektyw, zarządzeń, rozkazów i innych danych do nadrzędnych, współdziałających i podległych struktur organizacyjnych.

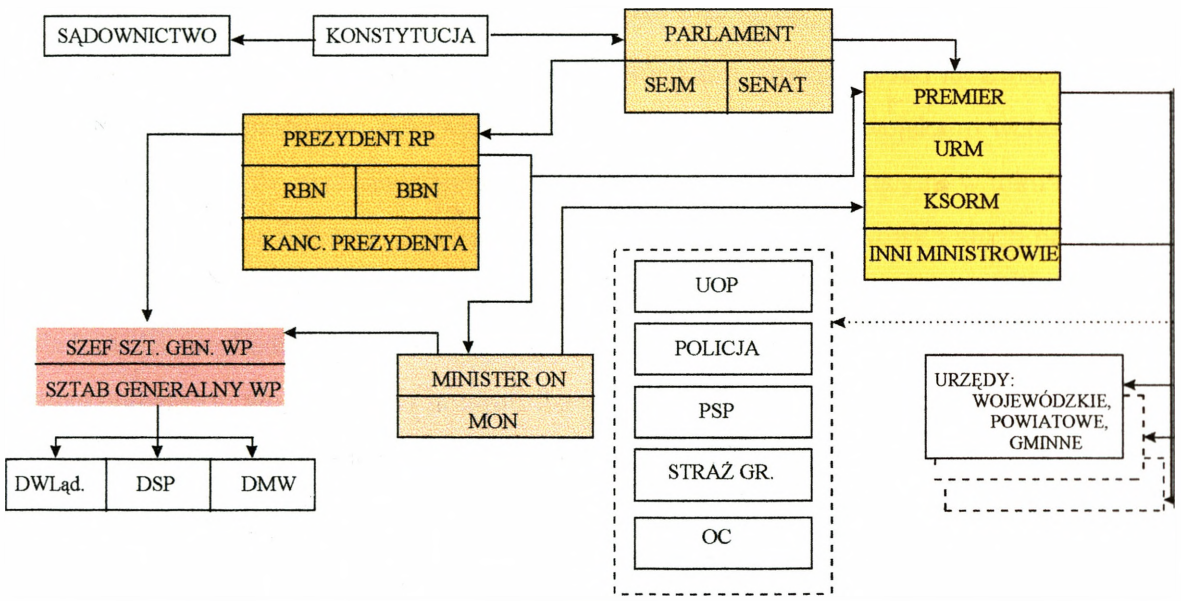
JAWNE

Zastrzeżone

JAWNE
Zastrzeżone

W stanach nadzwyczajnych realizowane będą następujące zadania:

- zbieranie i opracowywanie informacji o sytuacjach politycznych i militarnych;
- diagnozowanie i prognozowanie rozwoju procesów polityczno- militarnych;
- ostrzeganie o symptomach zjawisk zagrażających bezpieczeństwu państwa;
- modelowanie sytuacji kryzysowych oraz weryfikacja planów obronnych;
- określanie celów i sposobów działania w sytuacjach narastania bezpieczeństwa państwa;
- opracowanie propozycji użycia sił i środków systemu obronności;
- określenie potrzeb wszechstronnego zabezpieczenia wydzielonych do działań sił zbrojnych;
- opracowywanie i przekazywanie zadań wykonawcom;
- nadzorowanie przygotowań i koordynowanie działań wydzielonych sił i środków do likwidacji kryzysu.



Rys. 2.8. Relacje informacyjne wstępujące w modelu systemu obronności państwa (wariant)

Niezwykle dynamiczny rozwój technologiczny pozwolił na utworzenie multimedialnych systemów usług informacyjnych, opartych na połączeniu możliwości transmisyjnych z najnowszą generacją technik komputerowych. Usługi takie dostarczają użytkownikom informacji w dowolnej formie i dowolnym czasie.

Prawie wszystkie państwa na świecie korzystają, z możliwości najszybszego uzyskania wiarygodnych informacji o innych. Służą one kierownictwom politycznym i wyższym sztabom wojskowym do dokonywania bieżących ocen sytuacji polityczno - wojskowej i podejmowania decyzji.

JAWNE
Zastrzeżone

Dynamiczny rozwój techniki rozszerzył znacznie obszary, w których mogą być prowadzone działania zbrojne, wzrosła ich aktywność i szybkość. Dlatego potrzeba skracania czasu reagowania politycznego i wojskowego wymaga ciągle nowych środków uzyskiwania, transmisji i opracowania informacji oraz systemów kierowania państwem i siłami zbrojnymi.

Podstawą realizacji sprawnego przekazywania i przetwarzania informacji jest odpowiednio funkcjonująca łączność i środki informatyki.

2.4. Ocena aktualnego systemu kierowania obronnością

Łączność jest podstawowym środkiem kierowania obronnością państwa i dowodzenia siłami zbrojnymi. Bez niej organa kierownicze państwa, dowódcy, sztaby nie mają możliwości nieprzerwanego kierowania systemem obronności państwa i dowodzenia wojskami.

Charakter prawdopodobnych działań organów kierowniczych oraz potrzeby w zakresie kierowania obronnością państwa i dowodzenia wojskami stawiają przed łącznością określone zadania. W celu sprawnego kierowania obronnością i dowodzenia wojskami wchodzącymi do nakazanych rejonów, przechodzącymi do działań bojowych lub będącymi w toku tych działań organa kierownicze państwa, dowódca, sztab, szefowie rodzajów wojsk i służb powinni stale znać położenie i stan podległych wojsk, posiadać dane o przeciwniku i szereg innych wiadomości niezbędnych do podjęcia decyzji. Powinna również istnieć możliwość stawiania zadań podległym wojskom oraz kontroli ich wykonania.

Przygotowanie obszaru kraju do obrony, w aspekcie potrzeb łączności, powinno obejmować przedsięwzięcia o charakterze organizacyjnym, technicznym i inwestycyjnym w sieci telekomunikacyjnej użytku publicznego, a w tym także w wojskowej stacjonarnej sieci łączności - stosownie do potrzeb wynikających z planów obronności państwa i operacyjnego użycia sił zbrojnych.

Celem przygotowania obszaru kraju do obrony pod względem łączności jest przygotowanie, zwłaszcza w czasie pokoju, systemu łączności państwa do zapewnienia sprawnego kierowania obronnością i dowodzenia wojskami w okresie zagrożenia wojennego i wojny, przez wcześniejsze przystosowanie jego elementów składowych takich jak węzły i linie telekomunikacyjne, do przewidywanych potrzeb i wymagań systemu kierowania i dowodzenia oraz zapewnienie:

- zdolności do wydzielenia cyfrowych strumieni grupowych (łączy telekomunikacyjnych) z sieci telekomunikacyjnej państwa nowym elementom systemu kierowania i dowodzenia w różnych rejonach działań wojsk;
- niezawodności i elastyczności oraz możliwości odtwarzania naruszonych elementów infrastruktury telekomunikacyjnej;
- odporności na uszkodzenia, zniszczenia środków i urządzeń łączności;
- osiągnięcia przez oddziały, pododdziały dowodzenia i łączności gotowości bojowej oraz wyprzedzające rozwinięcie ich w ramach operacyjnego rozwinięcia sił zbrojnych;
- łączności organom kierowania i dowodzenia operacyjnym przygotowaniem obszaru kraju do obrony.

Zakres wykorzystania wojsk łączności do realizacji zadań łączności w czasie przygotowania obszaru kraju do obrony jest różny w poszczególnych jego okresach: od niewielkiego, w okresie osiągania wyższych stanów gotowości bojowej, do pełnego, po osiągnięciu przez ZO i ZT rejonu działań.

Do zadań łączności realizowanych w trakcie obrony państwa należy zaliczyć:

- zapewnienie organom kierowniczym państwa, dowódcom, sztabom, szefom rodzajów sił zbrojnych możliwości ciągłego kierowania i dowodzenia podległymi wojskami, to jest łączności kierowania i dowodzenia. Łączność kierowania i dowodzenia powinna zapewnić terminowe przekazywanie dyrektyw, rozkazów i zarządzeń podległym instytucjom, organom kierowniczym oraz wojskom i otrzymywanie od nich meldunków i sprawozdań o przebiegu i realizacji otrzymanych zadań;
- skoordynowanie wysiłku sąsiednich związków, oddziałów i pododdziałów, różnych rodzajów wojsk i sił zbrojnych.

Dlatego też organa kierownicze, dowódcy i sztaby współdziałających wojsk powinni systematycznie informować się wzajemnie o położeniu, uzgadniać działanie podległych wojsk według zadań i sposobów ich wykonania, a także według obiektów, rubieży i czasu.

Zapewnienie możliwości wymiany informacji między współdziałającymi sztabami i wojskami, dowództwami oraz władzami administracji państwowej i obrony cywilnej jest zapewnienie łączności współdziałania:

- przekazywanie w czasie działań obronnych, w trybie natychmiastowym sygnałów powiadamiania, ostrzegania i alarmowania wojsk i ludności, a więc zapewnienie terminowego obiegu sygnałów uprzedzających ludność i wojska o bezpośrednim zagrożeniu oraz użyciu przez przeciwnika broni masowego rażenia, o przeciwniku

powietrznym i o skażeniach, to jest zapewnienie łączności powiadamiania, ostrzegania i alarmowania;

- wszechstronne i nieprzerwane zabezpieczenie logistyczne, które możliwe jest tylko przy operatywnym i ciągłym dowodzeniu jednostkami logistycznymi, a zatem zapewnienie kierowania, dowodzenia jednostkami i obiektami logistycznymi oraz kierowania wsparciem logistycznym walczących wojsk, to jest zapewnienie łączności logistyce wojskowej.

System łączności działa w niezwykle złożonych warunkach, powinien więc spełnić szereg wymagań, do których między innymi należy zaliczyć: gotowość bojową, przepustowość, mobilność, trwałość oraz bezpieczeństwo.

Systemy łączności są systemami złożonymi, w skład których wchodzi część stacjonarna i polowa (mobilna); są systemami dynamicznymi, zmieniającymi się w czasie i przestrzeni. Działają w określonym otoczeniu, które oddziaływują na nie, a więc są systemami otwartymi. Charakteryzują się także odpowiednimi wskaźnikami (wyróżnikami) w określonym przedziale czasowym oraz celami działania. Systemy łączności zaliczane są do klasy tzw. wielkich systemów i mają następujące właściwości:

- wielofunkcyjność, wynikającą z potrzeby gromadzenia, przetwarzania i przesyłania wielu rodzajów informacji, świadczenia różnorodnych usług w zakresie łączności (np. telefonicznych, telefaksowych, telegraficznych, transmisji danych, fotofonicznych, pocztowych itp.);
- złożoność struktury organizacyjnej i sposoby działania;
- różnorodność tworzących je podsystemów i elementów oraz ścisłe ich powiązania i wzajemne zależności;
- prawdopodobny charakter procesów funkcjonowania systemów, podyktowany ciągłą zmianą parametrów i warunków ich działania oraz losowy charakter strumieni informacji;
- konieczność kierowania nimi, zabezpieczenie oraz wsparcie ich działania.

Systemy łączności spełniają zasadniczą rolę w procesie przekazywania informacji, toteż bez niezawodnego ich funkcjonowania trudno sobie wyobrazić prawidłowe kierowanie państwem i dowodzenie wojskami. Aby zmniejszyć, a w miarę możliwości wyeliminować, skutki destrukcyjnego oddziaływania przeciwnika w działaniach obronnych, prowadzonych na obszarze kraju, należy realizować różnorodne przedsięwzięcia organizacyjno-techniczne.

Jednym z zasadniczych elementów zapewniania sprawnego kierowania i dowodzenia SZ RP jest niezawodne funkcjonowanie systemu łączności a zdolność realizowania powyższych zadań będzie zależeć od infrastruktury systemu łączności na obszarze kraju.

JAWNE
Zastrzeżone

2.5. Stany nadzwyczajne w kontekście prawdopodobnych zagrożeń

Stan wojenny

Stan wojenny traktowany jako instytucja prawna oznacza, że jego wprowadzenie nie jest równoznaczne z rozpoczęciem rzeczywistych działań wojennych polegających na użyciu siły zbrojnej wobec państwa nieprzyjacielskiego. Tak rozumiany, stan wojenny trwa od chwili wypowiedzenia wojny lub faktycznego rozpoczęcia działań zbrojnych (wojennych) do czasu ustania działań wojennych, a w sensie formalno-prawnym do momentu podpisania traktatu pokojowego.

Stan wojenny z punktu widzenia prawa międzynarodowego, oznacza taką sytuację miedzy dwoma lub więcej państwami, która zgodnie z III Konwencją Haską z 18 października 1907r. (dotyczącą rozpoczęcia kroków nieprzyjacielskich) powoduje między innymi następujące skutki prawno-międzynarodowe :

a) możliwość prowadzenia przeciwko sobie wszelkich nie zabronionych normami prawa międzynarodowego akcji militarnych;
b) przerwanie stosunków dyplomatycznych i konsularnych;
c) ograniczenie praw obywateli państwa nieprzyjacielskiego na terytorium drugiego państwa (nadzór policyjny bądź internowanie, a nawet możliwość wydalenia ich z kraju) oraz konfiskatę własności obywateli państwa nieprzyjacielskiego i samego państwa (poprzez konfiskatę, sekwestr lub inne ograniczenia w prawie do dysponowania rzeczami);
d) zawieszenie lub wygaśnięcie umów między państwami wojującymi;
e) obowiązywanie umów i porozumień zawartych specjalnie na wypadek wojny;
f) możność powstania między państwami pozostającymi w konflikcie zbrojnym a państwami neutralnymi specjalnych stosunków polegających na tym, że te ostatnie mogą stać się tzw. mocarstwami opiekuńczymi.

W naszym systemie prawnym, w razie zewnętrznego zagrożenia państwa, zbrojnej napaści lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, zgodnie z obowiązującą nową Konstytucją prezydent na wniosek Rady Ministrów może wydać rozporządzenie o stanie wojennym podlegające zatwierdzeniu przez Sejm. Należy podkreślić, iż nasze przepisy konstytucyjne nie przewidują możliwości wypowiedzenia wojny, ale tylko wydanie postanowienia o stanie wojennym. Taka konstrukcja prawna współbrzmi z naszą doktryną obronną.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Stan wojenny, jak powszechnie wiadomo, będąc stanem rzeczywistego pozostawania jednego państwa w konflikcie z innym państwem ma głębokie skutki prawne, tak w zakresie prawa międzynarodowego, jak i wewnętrznego (państwowego). Jeśli idzie o wymiar wewnątrzpaństwowy owych skutków, to przejawiają się one z reguły w ograniczeniu podstawowych praw i wolności obywatelskich oraz zwiększeniem obywatelskich obowiązków. Gdy zaś idzie o organizację i funkcjonowanie struktur państwa , to może się to wyrażać w przekazaniu danemu naczelnemu organowi państwowemu szerokich uprawnień podyktowanych warunkami wojennymi.

Analizując przepisy konstytucyjne trzeba też odnotować zawarte tam pojęcie „stanu wojennego". W art.134, ust. 3. Nowej Konstytucji stanowi się, że „prezydent na czas wojny mianuje i zwalnia naczelnego dowódcę". Słuszny jest pogląd zgodnie z którym sformułowanie to nie oznacza, że nie można wyznaczyć naczelnego dowódcy jeszcze przed rozpoczęciem działań wojennych. Odnosi się ona tylko do okresu czasu, w którym naczelny dowódca miałby możliwość wykonywania swoich zadań dowódczych.

Stan wyjątkowy

Analizując instytucję stanu wyjątkowego należy odwołać się przede wszystkim do odpowiednich uregulowań konstytucyjnych. W art. 230, ust.1. Nowej Konstytucji stanowi się: „W razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, prezydent może wprowadzić stan wyjątkowy na części lub całym terytorium Rzeczypospolitej Polskiej, a także ogłosić częściową lub powszechną mobilizację". Z powyższego wynika, ze wprowadzenie stanu wyjątkowego uzależnione jest od kilku warunków materialnych. Są to warunki konieczne.

Konstytucja wskazuje tylko na jeden naczelny organ państwowy – prezydenta,- który może wprowadzić stan wyjątkowy. Żaden inny organ państwa nie może podjąć tej decyzji w jego zastępstwie. Logiczne jest spostrzeżenie, że przy różnorodnych zagrożeniach państwo stara się im zapobiegać (taka jest jego istota). W tym celu podejmuje ono określone kroki, polegające przede wszystkim na ograniczeniach praw i wolności obywatelskich na określonym terenie, na którym wprowadzono stan wyjątkowy bądź na obszarze całego kraju. Zarazem zwiększa się zakres zadań i uprawnień organów administracyjnych, wojskowych i policyjnych. Po to aby podejmowały skuteczne przedsięwzięcia przeciwko zagrożeniom państwa. Istota tego rodzaju stanu wyjątkowego polega na tym, że prawodawca dopuszcza możliwość szeregu ograniczeń praw i wolności obywateli jak np. zakaz strajków, akcji protestacyjnych, zwoływania zgromadzeń, ograniczenie swobody przemieszczania się, wprowadzenie godziny policyjnej itp.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Stan klęski żywiołowej

Wśród stanów nadzwyczajnych państwa wyróżniamy również stan klęski żywiołowej. Wprawdzie nie jest on powiązany z działaniami wojennymi, z zagrożeniem konstytucyjnego ustroju państwa, to jednak zamysł całościowego ujęcia problematyki stanów nadzwyczajnych nakazuje jego uwzględnianie. Stan klęski żywiołowej może wprowadzić Rada Ministrów na czas określony, nie dłuższy niż 30 dni, na części lub całym terytorium Państwa, w celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych i ich usunięcia.

Przytoczona norma konstytucyjna wskazuje na dwie przyczyny będące podstawą wprowadzenia stanu klęski żywiołowej. Określa też górną granicę czasookresu jego trwania do 30 dni. Natomiast przedłużenie tego stanu może nastąpić jedynie za zgodą Sejmu.
Gdy chodzi o stan klęski żywiołowej, to wprowadza się:

- po pierwsze - na całym terytorium państwa w przypadku wystąpienia na znacznym obszarze kraju zdarzeń żywiołowych zagrażających życiu większej liczby osób albo mieniu znacznych rozmiarów lub mogących wywołać istotne zakłócenia w gospodarce narodowej, które wymagają podjęcia szczególnych środków ochrony zasadniczych interesów państwa i obywateli;
- po drugie - na części terytorium kraju (w określonych jednostkach zasadniczego, terytorialnego podziału kraju) jeżeli ww. zdarzenia miały miejsce.

Ustawodawca określa też środki jakie należy podjąć dla zwalczania tych zagrożeń. Zakłada między innymi możliwości wprowadzenia obowiązku wykonania przez określone podmioty (osoby fizyczne i prawne) świadczeń osobistych i rzeczowych. Zasięg terytorialny obowiązywania stanu klęski żywiołowej może być zróżnicowany.

Ogólna ocena uregulowań prawnych o stanach nadzwyczajnych nie wypada pozytywnie. Niektóre przepisy są nazbyt represyjne, chociaż wiemy, że będą skutecznie przeciwdziałać zagrożeniom bezpieczeństwa państwa.

Wnioski

Wojnę określa się jako stan walki orężnej między państwami, albo jako przeciwstawienie stanu pokoju. Określenia te, które w przeszłości stanowiły podstawę podziału prawa międzynarodowego na dwie dziedziny, prawo wojny i pokoju nie odpowiadają jednak współczesnym tendencjom zmierzającym do objęcia przepisami prawa działań o charakterze zbrojnym, także wówczas gdy państwa z różnych przyczyn nie uważają tych działań za wojenne. Dlatego coraz częściej ma zastosowanie szersze określenie „konflikt zbrojny". Istotne znaczenie ma podział konfliktów zbrojnych na konflikty międzynarodowe

JAWNE Zastrzeżone

JAWNE
Zastrzeżone

i konflikty nie mające charakteru międzynarodowego. Zakres zobowiązań w odniesieniu do pierwszej kategorii konfliktów jest znacznie szerszy aniżeli w odniesieniu do drugiej kategorii.

Należy jednak pamiętać, że w świetle doświadczeń naszej epoki linie podziału na konflikty międzynarodowe i nie mające charakteru międzynarodowego nie są wyraźne, często bowiem konflikt początkowo jak najbardziej wewnętrzny na skutek interwencji z zewnątrz nie zawsze zresztą w formie wyłącznie oddziałów ekspedycyjnych, ale przez pomoc ekspertów i dostawy broni nabiera charakteru międzynarodowego. Pojęciem o zasięgu szerszym niż wojna i konflikt zbrojny jest „użycie siły". Obejmuje ono bowiem nie tylko przypadki, w których ma miejsce starcie się ze sobą sił zbrojnych dwóch lub więcej przeciwników, ale także akcje zbrojne, które nie napotykają zbrojnego oporu, jak to ma miejsce często przy interwencjach zbrojnych, demonstracjach o charakterze wojennym i inne. Aspekt wewnętrznych uwarunkowań legislacyjno – prawnych, zagadnienia wojny analizowano na tle naszej doktryny obronnej. Punktem wyjścia dociekań badawczych była teza, że RP jako demokratyczne państwo prawne nie ma żadnych agresywnych zamiarów względem otoczenia międzynarodowego.

Podstawowym celem polityki naszego kraju jest zapewnienie jego obronności i bezpieczeństwa wewnętrznego, co stanowi warunek wstępny jego harmonijnego rozwoju w wymiarze społecznym i gospodarczym. W praktyce polityka ta wyraża się w dążeniu do utrzymania suwerenności państwa i nienaruszalności jego granic, w rozwijaniu jego potencjału obronnego zdolnego do przeciwdziałania niebezpieczeństwa ewentualnej agresji. Zapewnienie obronności i bezpieczeństwa wewnętrznego państwa dokonuje się poprzez stosowanie prawnie usankcjonowanych środków i metod adekwatnych do zaistniałej sytuacji zewnętrznej i wewnętrznej.

Stosunki międzynarodowe mogą cechować się wzajemnym zrozumieniem, partnerską współpracą i wolą poszukiwania consensusu. Daje to możliwość pokojowego i bezpiecznego rozwoju narodu. Brak dobrej woli do negocjacji i określenia warunków porozumienia może doprowadzić do zaostrzenia różnych form wzajemnych oskarżeń, której skutkiem może być stan zagrożenia bezpieczeństwa państwa, a nawet agresja zbrojna. Zagrożeniem dla bezpieczeństwa państwa, narodu będzie ograniczenie lub utrata warunków jego bytu i rozwoju bądź utrata, naruszenie jego suwerenności i integralności terytorialnej. Zagrożenia mogą być militarne i pozamilitarne.

Kierowanie systemem obronności państwa uznano powszechnie za szczególną formę zarządzania i stanowiącą zespół czynności związanych z racjonalnym wykorzystaniem

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

potencjału ludzkiego, gospodarczego i środków walki na potrzeby obrony kraju przed agresją zbrojną. Kierowanie systemem obronności, a także przygotowaniami do obrony państwa odbywa się w systemie organizacyjno - funkcjonalnym obejmującym: organa władzy, administrację rządową i samorządową z ich ustawowymi kompetencjami, jak również infrastrukturą gospodarczą. Najbardziej newralgicznym okresem w kierowaniu państwem jest przechodzenie z pokojowego na wojenny system kierowania. Dlatego też przyjmuje się zasadę dokonywania jak najmniejszych zmian w kierowaniu państwem obowiązujących w czasie pokoju. W celu zapewnienia sprawnego funkcjonowania najwyższych organów władzy, administracji państwa i sił zbrojnych w czasie przechodzenia ze stanu pokojowego na wojenny już w czasie pokoju tworzy się odpowiednie struktury organizacyjne, których zadaniem jest zapewnienie utrzymania ciągłości kierowania oraz sprawnego przejścia gospodarki i sił zbrojnych ze struktury pokojowej na wojenną. W wielu krajach o rozwiniętych demokracjach struktury są takie same lub zbliżone. System kierowania obronnością państwa, obok podsystemu militarnego i pozamilitarnego jest jednym z zasadniczych elementów systemu obronności. Jego rola polega na informacyjnym sprzężeniu tych elementów w jednolitą sprawnie funkcjonującą całość. O jego efektywności decyduje nie tylko właściwy dobór ludzi na kierownicze funkcje, jego struktura gospodarcza, a przede wszystkim infrastruktura telekomunikacyjna i informatyczna.

Podstawowym elementem systemu kierowania i zarządzania państwem, sterowania gospodarką narodową, dowodzenia siłami zbrojnymi oraz funkcjonowania organów bezpieczeństwa publicznego jest niezawodnie działający system łączności państwa. Zdolność wykonania stojących przed nim zadań zależy między innymi od stanu rozbudowy infrastruktury systemu łączności na obszarze całego kraju, jego sprawności organizacyjno - technicznej, przepustowości i niezawodności. Natomiast szczególne znaczenie przypada łączności w okresie zagrożenia bezpieczeństwa państwa oraz w czasie stanów nadzwyczajnych.

Systemy łączności wykorzystywane w okresie stanów nadzwyczajnych i w trakcie obrony są projektowane już w czasie pokoju a następnie modyfikowane zgodnie z planami operacyjnymi. Muszą one spełniać szereg wymagań. Do podstawowych zalicza się wymagania w zakresie wymiany informacji w systemie kierowania i dowodzenia wojskami oraz wymagania stawiane systemowi łączności. Proces wymiany informacji w systemach kierowania i dowodzenia najpełniej charakteryzuje jakość łączności wyrażająca się spełnieniem wymagań w zakresie terminowości, wierności i skrytości łączności.

JAWNE
Zastrzeżone

3. .SYSTEMY KIEROWANIA OBRONNOŚCIĄ W WYBRANYCH PAŃSTWACH NATO

3.1. Kierowanie obronnością w wybranych państwach NATO

Nowoczesne społeczeństwo jest coraz bardziej uzależnione od zastosowań systemów telekomunikacyjnych i informatycznych. Zależność ta została uznana, zarówno przez państwa członkowskie NATO, jak i pozostałe kraje. Głównym celem, jaki postawiono przed władzami, jest stworzenie możliwości wykorzystania potencjału teleinformatycznego na poziomie krajowym i międzynarodowym zapewniając ciągłość działania łączności na rzecz wsparcia najważniejszych funkcji społeczeństwa w czasie sytuacji kryzysowych i wojny. W związku z ogromnym znaczeniem systemu teleinformatycznego operatorzy publiczni i dostawcy usług powinni posiadać dobrze przygotowane struktury, procedury zarządzania i mechanizmy na potrzeby działania i odtwarzania swoich sieci, jak również usług w sytuacjach szczególnych zagrożeń. W okresie kryzysu może jednak zaistnieć sytuacja, gdy NATO potrzebuje pomocy z zakresu dostępnych cywilnych systemów teleinformatycznych, ze względu na pilne potrzeby operacyjne. Może również zaistnieć sytuacja odwrotna, kiedy kraj lub kraje członkowskie mogą zwrócić się o pomoc do NATO. W tych okolicznościach konieczne jest posiadanie możliwości współpracy w zakresie konsultacji i uzyskania pomocy.

W ramach tych ogólnych celów, Komitet Planowania Łączności Cywilnej (CCPC) odpowiada za sprawy łączności cywilnej stosownie do ustaleń planowania zagrożeń cywilnych NATO. Planowanie łączności cywilnej musi być nastawione na zachowanie ciągłości świadczenia usług telekomunikacyjnych na potrzeby polityki, gospodarki i obronności. W tym ujęciu łączność cywilna rozumiana jest jako ogół potencjału systemów teleinformatycznych wraz z usługami przez nie świadczonymi, za wyjątkiem systemów militarnych.

W celu określenia gotowości łączności cywilnej do świadczenia usług na rzecz obronności i bezpieczeństwa państwa wyróżnia się dwa zasadnicze składniki:

- opiniowanie stanu istniejącego pod względem przydatności na potrzeby sytuacji kryzysowych i wojny;
- koordynacja i opracowanie w czasie pokoju sposobu wykorzystania sił i środków w celu zapewnienia ciągłości świadczenia usług telekomunikacyjnych w czasie kryzysu i wojny zarówno na potrzeby militarne jak i cywilne.

Obecnie w większości krajów zachodnich, struktura własności operatorów uległa zmianie, są to głównie prywatne spółki akcyjne. Zmiany te skutecznie rozdzieliły regulacje i nadzór, za

które odpowiedzialność ponosi w dalszym ciągu władza krajowa. Zmiany te mają natomiast pozytywny wpływ na rozwój technologiczny, który przynosi wiele zaawansowanych metod rozwoju sieci i przekazu informacji przy jednoczesnej minimalizacji kosztów. Trend globalizacji jest wynikiem konsolidacji międzynarodowego rynku telekomunikacyjnego.

Nowoczesną globalną służbę telekomunikacyjną można scharakteryzować następująco:

- dostęp do dowolnej usługi nie zależy od miejsca geograficznego, zabezpiecza globalne/regionalne usługi;
- system ma zdolność przełączeniową dla dostawców telekomunikacji, zarówno w skali światowej, jak i regionalnej, zabezpiecza globalne/regionalne infrastruktury i potencjału;
- system zapewnia abonentowi końcowemu fizyczne połączenie z globalną siecią szkieletową;
- system zapewnia usługi dodatkowe dla poszczególnych segmentów rynku telekomunikacyjnego;
- system integruje segmenty rynku abonentów co zapewnia duży obszar działalności w celu dostawy rozwiązań biznesowych.

Globalizacja na rynku telekomunikacji prowadzi do wzrostu liczby fizycznych połączeń pomiędzy dostawcami telekomunikacyjnymi. Wynika z tego wniosek , że informacje będą przesyłane przez różne sieci, co pociągnie to za sobą takie skutki, jak zagrożenie dla bezpieczeństwa, szczególnie tam gdzie usługi/sieci są dostarczane i zarządzane przez kraje spoza NATO. Większość krajów dysponuje połączeniami telekomunikacyjnymi pomiędzy władzami rządowymi, wojskowymi i cywilnymi a ważnymi użytkownikami za pomocą publicznej sieci telekomunikacyjnej, takiej jak publiczna komutowana sieć telefoniczna. Połączenia te są traktowane jako podstawowe i są niezbędne w celu zwiększenia ilości połączeń, gdy usługi telekomunikacyjne będą ograniczone z uwagi na uszkodzenia zatory lub usterki. Większość krajów dysponuje krajowymi planami preferencji. które umożliwiają funkcjonowanie tego istotnego ruchu krajowego. Stosuje się szereg metod poprawy realizacji połączeń dla ważnych użytkowników, takich jak:

- ograniczanie dostępu dla nieważnych użytkowników;
- rezerwowanie obwodów;
- zapewnienie zwiększonej pojemności (metoda ekspansywna);
- zapewnienie bezpośredniego dostępu centrów przełączających;
- wprowadzenie sterowania kodów docelowych.

Zgodnie z dokumentem NATO AC/121-D/713 określone są następujące obszary które powinny wchodzić w skład systemu teleinformatycznego na potrzeby kierowania państwem w okresie stanów nadzwyczajnych:

- część wojskowa;
- obrona cywilna / obrona terytorialna;
- cele dyplomatyczne i cele rządowe;
- cele bezpieczeństwa państwa, w tym cło i imigracja;
- usługi w sytuacjach kryzysowych władz lokalnych, w tym policji, służb przeciwpożarowych, itp.
- służby publiczne, w tym wodociągowe, energetyczne, itp.
- usługi medyczne;
- ratownictwo powietrzne i morskie;
- gałęzie przemysłu ważne dla podtrzymania wysiłku wojennego;
- transport wewnętrzny i międzynarodowy;
- usługi meteorologiczne;
- usługi radiowe i prasa.

Patrząc w przyszłość możemy zauważyć że systemy teleinformatyczne nowej generacji oferują wiele nowych dodatkowych możliwości dających duże korzyści operacyjne. Nowymi rodzajami usług są:

- poczta elektroniczna;
- dostęp do rozległych sieci komputerowych.

Większość krajów dysponuje krajowymi planami preferencji, które umożliwiają funkcjonowanie tego istotnego ruchu krajowego. Jednakże, sprawą znaczącej wagi dla NATO jest wsparcie krajów członkowskich w czasie kryzysu, co wiąże się z zapewnieniem interoperacyjności umożliwiającej łączność pomiędzy ważnymi użytkownikami w jednym kraju a jego korespondentami w innym.

Wiele istniejących krajowych programów preferencji cywilnych przeznaczona jest do uruchomienia w sytuacjach szczególnych, lecz mogą miejsce sytuacje, w których może wystąpić możliwość uruchomienia międzynarodowego programu preferencji w kraju, w którym wydaje się być to zbędne. Przykładem tego może być sytuacja, gdy tworzy się intensywny ruch międzynarodowy do odległego kraju znajdującego się w stanie kryzysu. Stąd międzynarodowe i krajowe programy powinny być niezależne ale kompatybilne.

JAWNE
Zastrzeżone

3.1.1. Kierowanie obronnością w USA

Zgodnie z Konstytucją Stanów Zjednoczonych Ameryki Północnej i ustawą o bezpieczeństwie państwa za obronność i bezpieczeństwo kraju odpowiada prezydent, który w dziedzinie kierowania obronnością, posiada duże uprawnienia. Ma prawo wydawać dekrety i zarządzenia w sprawach obronnych, w tym również wojskowych. Za zgodą Kongresu mianuje i odwołuje ministra obrony, jest najwyższym zwierzchnikiem sił zbrojnych, a w okresie wojny przysługują mu uprawnienia naczelnego dowódcy sił zbrojnych. Zgodnie z ustaleniami Kongresu, zawartymi w rezolucji *War Powers Resolution* prezydent ma prawo użycia sił zbrojnych, ale tylko w następujących wypadkach:

- po wypowiedzeniu wojny przez Kongres;
- na mocy specjalnej ustawy Kongresu upoważniającej prezydenta do użycia sił zbrojnych;
- mocą własnej decyzji w razie bezpośredniego zagrożenia bezpieczeństwa państwa, zarówno na jego terytorium, jak i w posiadłościach zamorskich oraz w wypadku ataku na siły zbrojne Stanów Zjednoczonych bez względu na miejsce ich dyslokacji.

Ministerstwo Obrony (Department of Defence) jest organem wykonawczym prezydenta odpowiedzialnym za realizację wszystkich przedsięwzięć dotyczących polityki zbrojeniowej i obronności kraju. Ministrowi obrony podlegają bezpośrednio Rada ds. Polityki Rozwoju Sił Zbrojnych, Komitet Szefów Sztabów, ministerstwa trzech rodzajów sił zbrojnych (lądowych, powietrznych, morskich) oraz wyspecjalizowane instytucje agencji centralnych. Rada ds. Polityki Rozwoju Sił Zbrojnych jest głównym organem doradczym ministra obrony w sprawach polityki wojskowej, koordynatorem planów mobilizacyjnych, ustalania perspektywicznych kierunków rozwoju sił zbrojnych na poszczególnych teatrach wojny.

Komitet Szefów Sztabów (spełnia rolę Sztabu Generalnego) jest wojskowym organem doradczym prezydenta, Rady Bezpieczeństwa Narodowego i ministra obrony.

Do obowiązków Komitetu Szefów Sztabów należy:

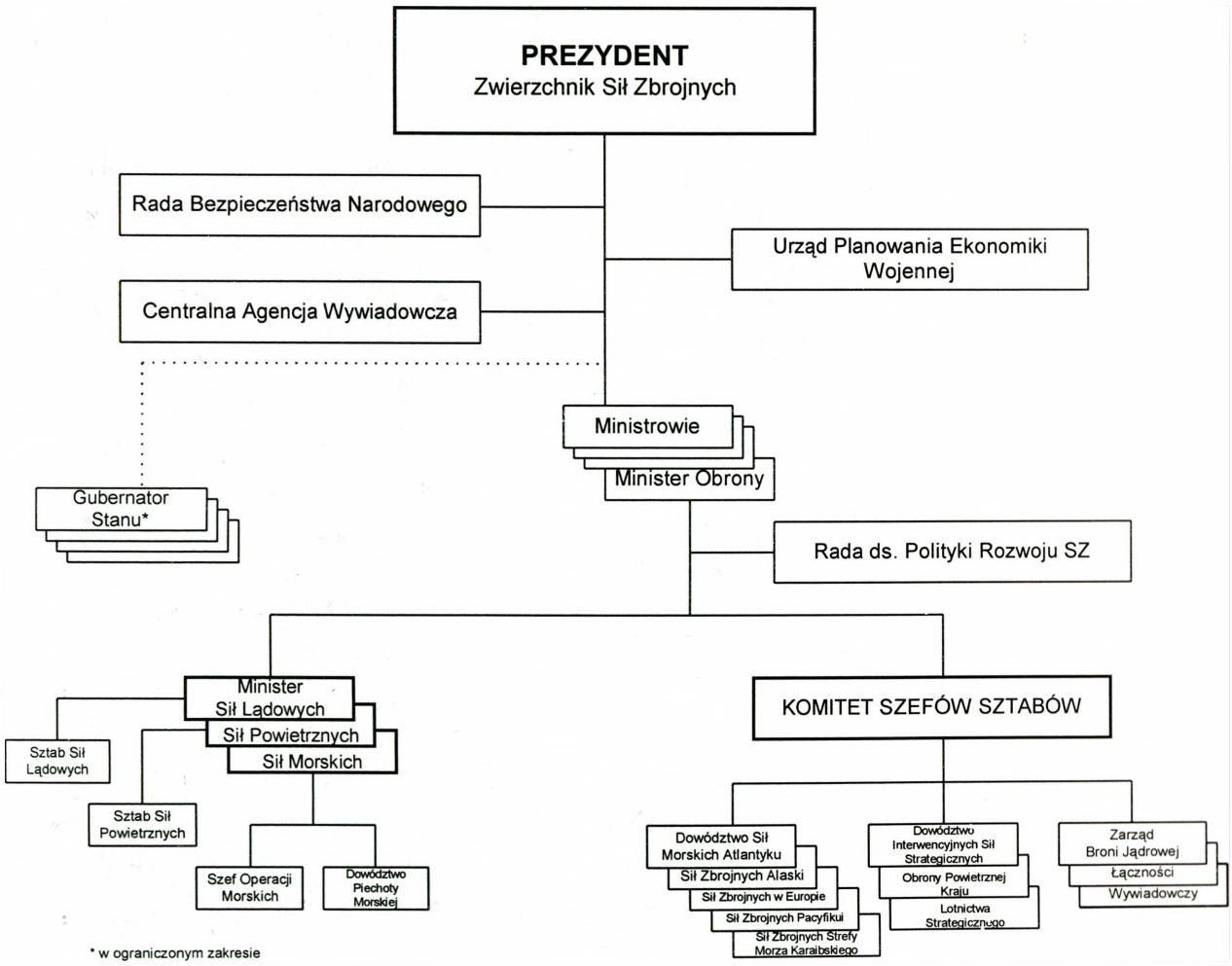
- przygotowanie planów strategiczno-operacyjnych sił zbrojnych;
- kierowanie operacjami na poszczególnych teatrach wojny.

Rada Bezpieczeństwa Narodowego jest organem doradczym prezydenta w sprawach bezpieczeństwa i zabezpieczenia interesów Stanów Zjednoczonych. Stałymi członkami rady są: przewodniczący rady–doradca prezydenta ds. bezpieczeństwa narodowego, sekretarz stanu, minister obrony, przewodniczący Komitetu Szefów Sztabów, minister skarbu, dyrektor Centralnej Agencji Wywiadowczej. Ministrowie realizują politykę obronną państwa, w ramach posiadanych kompetencji oraz stosownie do ustaleń prezydenta.

JAWNE
Zastrzeżone

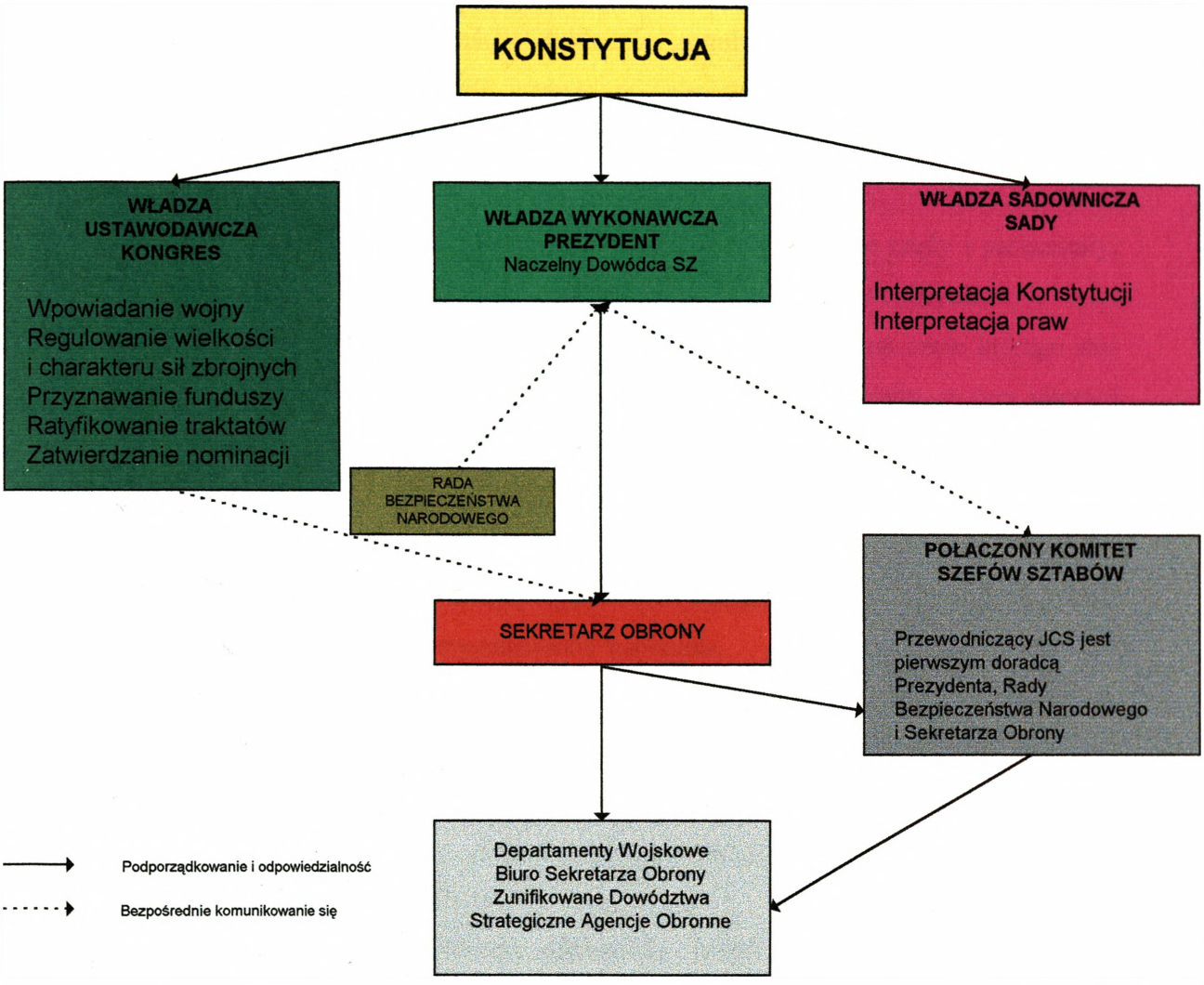
Gubernatorzy stanów posiadają duże uprawnienia władcze, nie dotyczą one obrony państwa i spraw zagranicznych. Gubernator, na obszarze stanu decyduje o środkach nadzwyczajnych w celu przeciwdziałania lub usunięcia skutków spowodowanych klęskami żywiołowymi (cyklony, powodzie, susze itp.), a także w celu przywrócenia bezpieczeństwa i porządku publicznego. Jemu podlega Policja stanowa, dowodzi również Gwardią Narodową.

STRUKTURA KIEROWANIA OBRONNOŚCIA USA



Rys.3.1. Kolejne szczeble decyzyjne w strukturze kierowania obronnością USA. (wariant)

JAWNE
Zastrzeżone



Rys. 3.2. Podział kompetencji dotyczący systemu obronności USA wynikający z konstytucji. (wariant)

Na rysunkach 3.1. i 3.2. przedstawiono struktury decyzyjne i kompetencyjne systemu obronności USA wynikające z konstytucji.

Kongres jako parlament Stanów Zjednoczonych bezpośrednio nie uczestniczy w kierowaniu państwem, w tym również obronnością. Ustanawia natomiast ustawy w tej dziedzinie, ma prawo wypowiedzenia wojny, uchwalenia specjalnej ustawy upoważniającej prezydenta do użycia sił zbrojnych, wyraża zgodę na mianowanie i odwołanie ministra obrony przez prezydenta.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

3.1.2. Kierowanie obronnością w Republice Federalnej Niemiec

Sprawy związane z obronnością dokładnie reguluje Ustawa Zasadnicza RFN (odpowiednik naszej konstytucji). W ustawie tej określono również organizację oraz kompetencje władzy ustawodawczej i wykonawczej Republiki Federalnej Niemiec na okres wojny.

Kraje wchodzące w skład RFN posiadają autonomię m.in. własne rządy i parlamenty, jednakże sprawy polityki zagranicznej obrony są w gestii tylko władz centralnych.

W czasie pokoju władzę wykonawczą sprawuje rząd federalny, na czele którego stoi kanclerz federalny. Kanclerz federalny określa wytyczne polityki dla rządu, w tym również polityki obronnej, za co ponosi odpowiedzialność przed parlamentem. Formalnie głową państwa jest Prezydent Federalny, faktycznie pełni on w zasadzie funkcje honorowe i reprezentacyjne.

Organem wyspecjalizowanym w sprawach obronności jest Federalna Rada Bezpieczeństwa obradująca pod przewodnictwem kanclerza.

W skład Rady wchodzą – ministrowie: obrony, spraw wewnętrznych, spraw zagranicznych, gospodarki i finansów oraz generalny inspektor Bundeswehry. Federalna Rada Bezpieczeństwa dokonuje analizy i oceny węzłowych problemów dotyczących sił zbrojnych, przygotowań obronnych państwa, wypracowuje koncepcje i projekty decyzji, które zatwierdzane są przez rząd lub kanclerza.

Minister obrony (osoba cywilna) odpowiada przed parlamentem i kanclerzem federalnym za realizację celów i założeń polityki wojskowej oraz za uzbrojenie, wyszkolenie i stan gotowości sił zbrojnych. W czasie pokoju pełni on funkcję dowódcy sił zbrojnych.

Organem wykonawczym ministra obrony jest Ministerstwo Obrony, w skład którego wchodzą sztaby: organizacyjny, planowania i informacyjno-prasowy. W składzie Ministerstwa Obrony funkcjonują trzy piony: wojskowy, administracyjno-prawny i zbrojeniowy.

Pion wojskowy jest zasadniczym pionem ministerstwa. Na jego czele stoi generalny inspektor Bundeswehery, który przed ministrem obrony odpowiada za wypracowanie i realizację ogólnej koncepcji rozwoju sił zbrojnych. Jest on jednocześnie, jako najwyższy rangą wojskowy, doradcą wojskowym ministra obrony, rządu i kanclerza. Skład pionu wojskowego: sztab sił zbrojnych, sztaby rodzajów sił zbrojnych, inspektor służby medyczno-sanitarnej. Ponadto w Ministerstwie Obrony, do rozwiązania szczególnie istotnych spraw, powołuje się doraźnie organ roboczy tzw. Konferencję Szefów Oddziałów.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Zgodnie z Ustawą Zasadniczą RFN wszelkie uprawnienia ustawodawcze i kontrolne przysługują obu izbom parlamentu niemieckiego (Bundestag i Bundesrat). Organem parlamentu wyspecjalizowanym w sprawach obronności jest Komisja Obrony, natomiast do sprawowania kontroli nad siłami zbrojnymi powoływany jest organ pomocniczy parlamentu – pełnomocnik wojskowy parlamentu federalnego.

Z chwilą ogłoszenia stanu napięcia lub stanu obrony na bazie parlamentu federalnego tworzy się Komisję Wspólną, w skład wchodzi 33 posłów z Bundestagu, 11 członków z Bundesratu. Komisja Wspólna przejmuje wszelkie uprawnienia ustawodawcze i kontrolne przysługujące obu izbom parlamentu w czasie pokoju, a także posiada uprawnienia do wyboru nowego kanclerza federalnego.

Federalna Rada Bezpieczeństwa zostaje przekształcona w Gabinet Wojenny, jako organ kanclerza do spraw kierowania państwem i dowodzenia siłami zbrojnymi. Skład Gabinetu Wojennego jest identyczny jak Federalnej Rady Bezpieczeństwa. Grupy doradcze Ministerstwa Obrony i pozostałych ministerstw federalnych, delegowane do Gabinetu Wojennego tworzą sztab roboczy spełniający rolę organów wykonawczych w sektorze wojskowym i cywilnym. Kanclerz federalny przejmuje naczelne dowództwo nad siłami zbrojnymi.

Dokonuje się zmian strukturalnych w Ministerstwie Obrony. Z wydzielonych elementów Ministerstwa Obrony i Sztabów Sił Zbrojnych tworzy się grupę doradczą, której pracami kieruje minister obrony. Jest to najbardziej rozbudowany element Gabinetu Wojennego, większy pod względem liczebnym od grupy doradczej sektora cywilnego. Jest też zasadniczym organem roboczym gabinetu, zdolnym do przejęcia procesu kierowania państwem i realizacji wszystkich zadań z tym związanych.

W składzie grupy doradczej ministerstwa znajduje się Operacyjny Sztab Kierowania Siłami Zbrojnymi bezpośrednio podporządkowany generalnemu inspektorowi Bundeswehry. Sztab ten tworzony jest na bazie grup operacyjnych Sztabu Sił Zbrojnych, Sztabów Rodzajów Sił Zbrojnych i Inspektoratu Służby Medyczno-Sanitarnej. Jego pracami kieruje szef Sztabu Sił Zbrojnych.

Grupa doradcza Ministerstwa Obrony przygotowuje niezbędne dane do podejmowania decyzji wojskowych przez kierownictwo polityczne państwa i jest odpowiedzialna za wprowadzenie ich w życie.

Referaty i oddziały Ministerstwa Obrony, które nie weszły w skład tworzonych organów czasu wojny, realizują zadania związane z mobilizacyjnym rozwinięciem wojsk, szkoleniem rezerw, zabezpieczeniem logistycznym jednostek Bundeswehry wydzielanych do

JAWNE
Zastrzeżone

składu Połączonych Sił Zbrojnych Paktu Północnoatlantyckiego. Wiele instytucji i urzędów ulega rozwiązaniu, a ich stany osobowe, zgodnie z planami mobilizacyjnymi, przechodzą do jednostek mobilizowanych.

W okresie wojny na szczeblu federalnym i krajów związkowych tworzy się Sztaby Kierowania Obroną Cywilną, a na szczeblu obwodów, powiatów lub miast wydzielonych – Sztaby Obrony Cywilnej. W ich skład wchodzą przedstawiciele obrony cywilnej poszczególnych resortów danego szczebla administracyjnego.

W okręgach wojskowych tworzy się Komitety Koordynacyjne kierowane przez dowódców okręgów i ministrów spraw wewnętrznych, w skład których wchodzi sekretariat i grupy robocze. Członkami tych grup są przedstawiciele ministerstw krajów związkowych, przedstawiciele dowództw okręgów wojskowych i jednostek wojskowych państw NATO stacjonujących na terenie danego okręgu. Komitet Koordynacyjny zajmuje się planowaniem i koordynacją wspólnych działań instytucji cywilnych i wojskowych w stanie napięcia i okresie wojny.

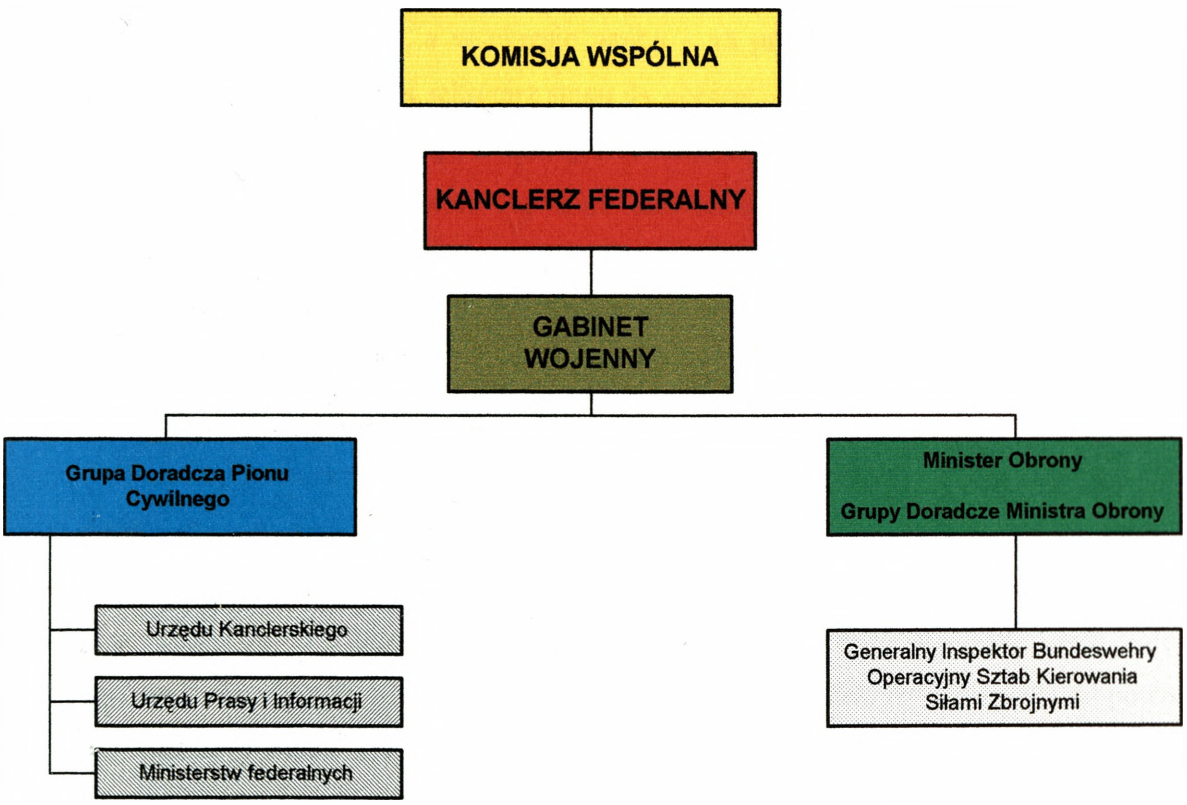
Planuje się utworzenie analogicznych organów koordynujących na szczeblu obwodowych i rejonowych dowództw obrony. Kompleksowo prowadzone są przedsięwzięcia związane z utworzeniem jednolitej struktury organów koordynujących w krajach związkowych i okręgach, co pozwoli ustalić strefy odpowiedzialności i zwiększyć efektywność wykorzystania organów obrony cywilnej na rzecz sił zbrojnych.

Dowodzenie Siłami Zbrojnymi RFN oraz sektorem cywilnym w stanie napięcia i wojny jest realizowane z wcześniej przygotowanych i rozwiniętych stanowisk dowodzenia i kierowania okresu wojny. Stanowiska te przejmują dowodzenie z chwilą ogłoszenia alarmu zwykłego.

W ustawodawstwie niemieckim wyróżnia się nadzwyczajne zagrożenia wewnętrzne, do których zalicza się zagrożenie ustroju konstytucyjnego, zagrożenie bezpieczeństwa i porządku publicznego, klęski żywiołowe, nieszczęśliwe wypadki o znamionach klęski żywiołowej, itp.

Według Ustawy Zasadniczej RFN likwidacja skutków wymienionych zagrożeń należy do obowiązków rządów krajów związkowych. Przy rządach tych krajów może być powoływany Sztab Kryzysowy, do zadań którego należy kierowanie likwidacją następstw kryzysowychW wypadku, gdy możliwości kraju związkowego są niewystarczające do likwidacji określonych następstw kryzysowych rząd tego kraju *...może zażądać pomocy sił policyjnych innych krajów związkowych, sił i urządzeń administracyjnych innych instytucji, jak również Federalnej Straży Granicznej i sił zbrojnych.*

W tym celu na szczeblu federalnym w Urzędzie Kanclerskim tworzy się Sztab Kryzysowy. W skład sztabu wchodzą ministrowie: spraw wewnętrznych, obrony, spraw zagranicznych, komunikacji, łączności, kierownik urzędu pracy i informacji oraz zależnie od potrzeb inni przedstawiciele rządu i instytucji centralnych. Wówczas rząd federalny uprawniony jest wydawać rządom krajowym polecenia oddania do dyspozycji innych krajów sił policyjnych, sił i urządzeń administracyjnych innych instytucji, jak również użycia federalnej straży granicznej i sił zbrojnych. Struktura władz państwowych RFN na okres wojny przedstawia rysunek 3.3.



Rys.3.3. Struktura władz państwowych RFN na okres wojny (wariant)

System telekomunikacyjny na potrzeby kierowania obronnością i bezpieczeństwem państwa jest systemem częściowo wydzielonym z krajowej infrastruktury telekomunikacyjnej. W części wojskowej jest to system całkowicie wydzielony, fizycznie odseparowany od systemu transmisyjnego operatorów komercyjnych. Dysponujący własnym systemem zarządzania i nadzoru.

3.1.3. Kierowanie obronnością w Wielkiej Brytanii

Zgodnie z ustawodawstwem brytyjskim głową państwa i jednocześnie naczelnym dowódcą sił zbrojnych jest król (królowa). Faktycznie zaś całokształtem problematyki obronnej w tym również wojskowej kieruje premier i Komitet Polityki Obronnej.

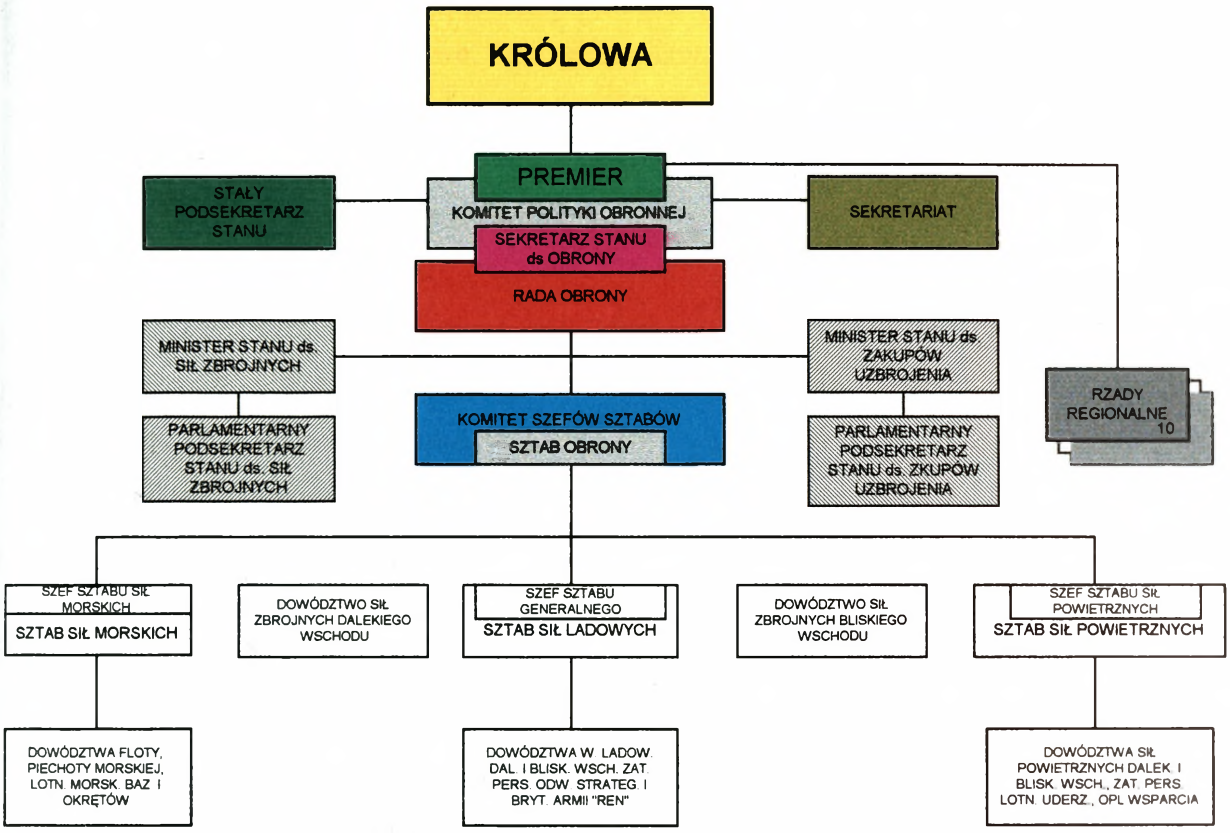
Do zadań Komitetu Polityki Obronnej należą sprawy polityki wojskowej, w tym określenie głównych kierunków rozwoju i wykorzystania sił zbrojnych. W skład jego wchodzą: premier – jako przewodniczący, sekretarz, ministrowie: obrony, spraw wewnętrznych, spraw zagranicznych, przemysłu i handlu. W zależności od potrzeb w pracach komitetu mogą uczestniczyć inni ministrowie oraz osobistości wojskowe. Wszystkie przedsięwzięcia w dziedzinie wojskowej Komitet Polityki Obronnej realizuje poprzez Ministerstwo Obrony. Ministerstwo Obrony odpowiedzialne jest za stan sił zbrojnych i przygotowanie obrony kraju, a w okresie wojny – za prowadzenie działań zbrojnych. Na czele Ministerstwa Obrony stoi sekretarz stanu ds. obrony. Jego dwaj zastępcy to ministrowie stanu ds. sił zbrojnych i ds. zakupów uzbrojenia. Minister obrony jest osobą cywilną. Kieruje on działalnością podległego resortu, rozpatruje i zatwierdza kandydatów na wyższe dowódcze i kierownicze stanowiska w ministerstwie. Ministrowi obrony podlegają także: szef sztabu obrony, parlamentarni sekretarze stanu ds. sił zbrojnych i ds. uzbrojenia oraz stały sekretarz stanu. Organami decyzyjnymi Ministerstwa Obrony są: Rada Obrony i Komitet Szefów Sztabów. W skład Rady Obrony wchodzą: sekretarz stanu ds. obrony – jako przewodniczący, jego dwaj zastępcy, sekretarze stany ds. sił zbrojnych i ds. uzbrojenia, stały sekretarz stanu, szef sztabu obrony, szefowie sztabów sił: lądowych, powietrznych, morskich, doradca ds. naukowych oraz szef zaopatrzenia wojskowego. W skład Komitetu Szefów Sztabów wchodzą: szef Sztabu Obrony – jako przewodniczący, pierwszy zastępca szefa Sztabu Obrony; szefowie sztabów sił: lądowych, powietrznych i morskich. W zależności od potrzeb, w posiedzeniach Komitetu bierze udział szef wywiadu wojskowego, zastępca szefa Sztabu Obrony ds. operacyjnych, a także zastępca podsekretarza stanu ds. strategii i polityki. Na zaproszenie szefa Sztabu Obrony w obradach mogą uczestniczyć inni przedstawiciele Ministerstwa Obrony, wyżsi rangą urzędnicy Ministerstwa Spraw Zagranicznych i innych ministerstw. Organem roboczym Komitetu Szefów Sztabów jest Sztab Obrony. Jest to operacyjny organ kierowania siłami zbrojnymi, podlegający szefowi Sztabu Obrony. Szef Sztabu Obrony jest głównodowodzącym siłami zbrojnymi, jednocześnie przełożonym szefów sztabów rodzajów sił zbrojnych, a także szefa wywiadu wojskowego.

Organem koordynującym działalność Sztabu Obrony i sztabów rodzajów sił zbrojnych jest Operacyjny Komitet Wykonawczy. Przewodniczącym Komitetu jest pierwszy zastępca

szefa Sztabu Obrony, ponadto w skład Komitetu wchodzą: zastępca szefa Sztabu Obrony ds. operacyjnych, szef Zarządu Operacyjnego Sztabu Sił Lądowych, pomocnicy ds. operacyjnych szefów Sztabów Sił Powietrznych i Morskich. W czasie wojny ogólne kierownictwo nad działaniami zbrojnymi sprawuje Komitet Polityki Obronnej funkcjonujący w takim samym składzie jak w okresie pokoju. Organizacja władz centralnych nie ulega zmianie. Obszar Wielkiej Brytanii zostaje podzielony na dziesięć regionów kierowanych przez tzw. rządy regionalne z wojskowymi komisarzami na czele. Granice regionów pokrywają się w zasadzie z granicami rejonów wojskowych administrowanych przez Dowództwa Regionów Wojskowych. Do podjęcia decyzji o zarządzeniu powszechnej mobilizacji i wypowiedzeniu wojny upoważniony jest Gabinet Ministrów (odpowiednik naszej Rady Ministrów). W podjęciu tej decyzji, która formalnie podlega zatwierdzeniu przez króla (królową), uczestniczą również członkowie wywiadu wojskowego. Wyspecjalizowanym organem do spraw kierowania reagowaniem kryzysowym jest Centrum Połączonych Operacji funkcjonujące w Ministerstwie Obrony. Kieruje nim szef Sztabu Obrony ds. operacyjnych, ćwiczeń i logistyki. W jego składzie pracują eksperci poszczególnych rodzajów sił zbrojnych oraz eksperci cywilni Ministerstwa Obrony. W sferze zainteresowania centrum są głównie kryzysy polityczno-militarne. Głównym zadaniem Centrum Połączonych Operacji jest zbieranie i ocena informacji, przygotowanie decyzji szefowi Sztabu Obrony, prowadzenie konsultacji na szczeblu ministerialnym i z wyższymi dowódcami NATO.

System telekomunikacyjny na potrzeby kierowania obronnością i bezpieczeństwem państwa jest systemem wydzielonym, fizycznie odseparowanym od innych systemów. Funkcje połączeniowe realizowane są przy wykorzystaniu wydzielonych urządzeń komutacyjnych umieszczonych w specjalnie zabezpieczonych pomieszczeniach. Dostęp do elementów systemu (transmisji, komutacji, urządzeń utajniających i abonenckich) jest ściśle ograniczony. Pojemność systemu to około 3 000 abonentów. System świadczy głównie usługi głosowe. Połączenia poza systemowe są możliwe jednak są one ograniczone do minimum. Szczeble decyzyjne w strukturze kierowania obronnością Wielkiej Brytanii przedstawia rysunek 3.4. Zbudowany system charakteryzuje się wyjątkowa prostotą. Wymagany poziom bezpieczeństwa osiągnięty został poprzez fizyczne oddzielenie go od innych systemów (wydzielone łącza, pomieszczenia, obsługa). System jest w stanie „*uśpionym*" tzn. zachowuje ciągłą gotowość do działania jednak nie jest wykorzystywany.

JAWNE
Zastrzeżone



Rys.3.4. Kolejne szczeble decyzyjne w strukturze kierowania obronnością Wielkiej Brytanii (wariant)

3.1.4. Kierowanie obronnością we Francji

Biała księga o obronie jest podstawowym dokumentem, w którym określono główne pryncypia francuskiej polityki obronnej. Prezydent Francji jako głowa państwa, odpowiedzialny jest za obronność kraju. Jest on jednocześnie najwyższym zwierzchnikiem sił zbrojnych i tylko on posiada uprawnienia do wydania rozkazu o użyciu broni jądrowej. Prezydent kieruje działalnością rządu, mianuje i odwołuje premiera, a na jego wniosek również ministrów. Wyspecjalizowanym organem kierowniczym i decyzyjnym w sprawach obronności państwa jest Rada Obrony (gdy obradom przewodniczy prezydent) lub Komitet Obrony (gdy obradom przewodniczy premier). W skład Rady wchodzą: prezydent, premier, ministrowie: obrony, spraw zagranicznych, spraw wewnętrznych, gospodarki i finansów. W obradach uczestniczą również: Urzędu Prezydenta. Na obrady mogą być również zapraszani inni ministrowie i wyżsi funkcjonariusze państwowi.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Decyzje dotyczące użycia wojsk, podejmuje Ścisły Komitet Obrony, wyłoniony z Komitetu Obrony, którego skład każdorazowo ustala prezydent (premier). Premier odpowiada bezpośrednio przed prezydentem za stan obronności państwa, sprawuje on kierownictwo ogólne i wojskowe. Jest uprawniony do wydawania wytycznych w zakresie obrony, kontroluje ich realizację, a także koordynuje działalność wszystkich ministrów w zakresie obronności.

Organami wykonawczymi premiera są:

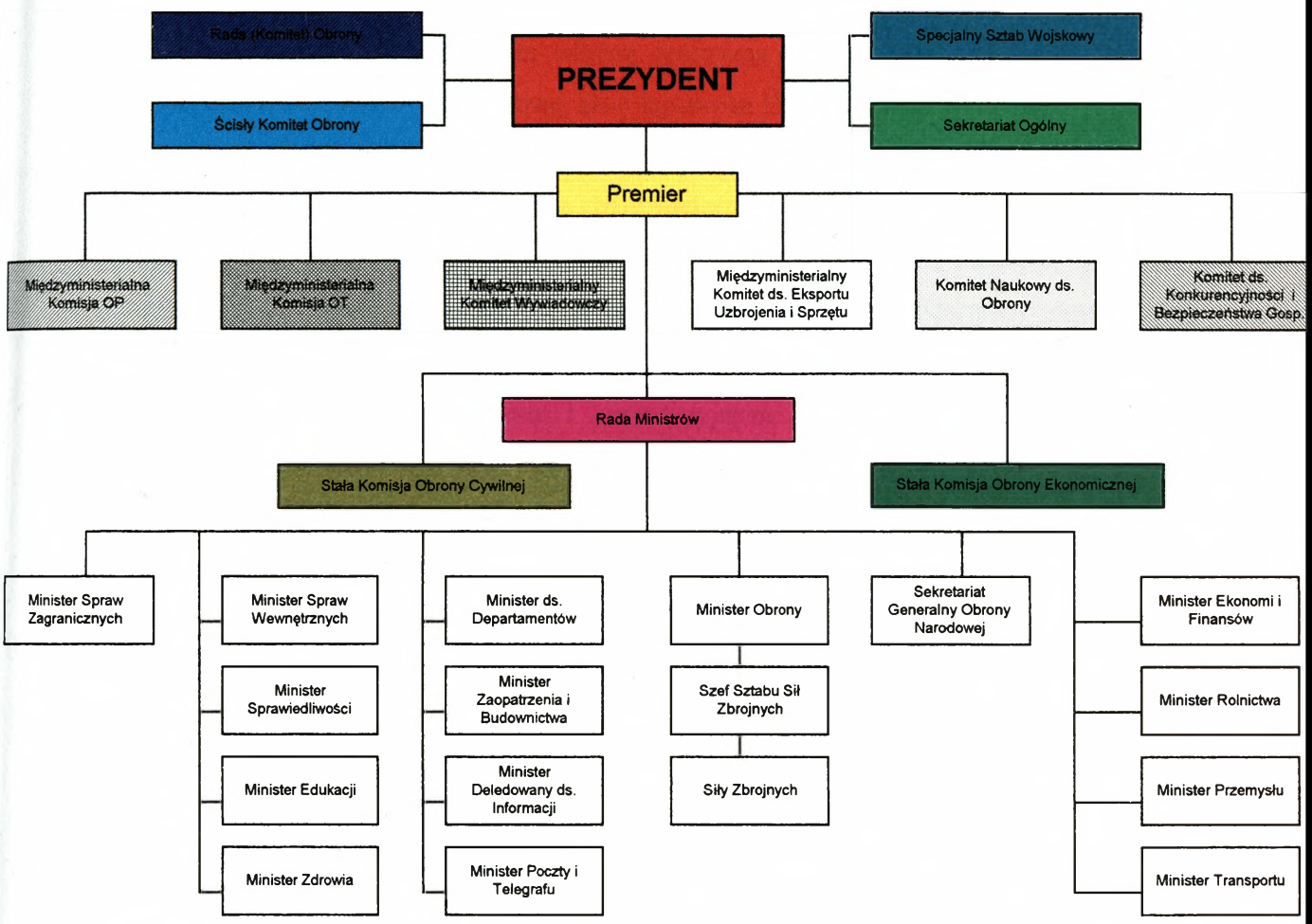
- minister obrony;
- sekretarz generalny obrony narodowej – przygotowujący i organizujący obrady Komitetu Obrony;
- Komitet Naukowy ds. obrony – ustalający potrzeby i kierunki oraz koordynujący działalność naukowo-badawczą w zakresie obronności;
- Międzyministerialny Komitet Wywiadowczy – opracowujący plany i koordynujący działalność służb specjalnych;
- Międzyministerialna Komisja Obrony Terytorialnej, Międzyministerialna Komisja Obrony Powietrznej – opracowująca decyzje i dyrektywy dotyczące polityki rządu w zakresie obrony terytorialnej i obrony powietrznej.

Minister obrony odpowiedzialny jest przed premierem za realizację polityki wojskowej rządu, opracowywanie koncepcji struktur organizacyjnych i użycia sił zbrojnych, gotowość bojową i mobilizacyjną wojsk, a także rozbudowę niezbędnej dla nich infrastruktury. Minister obrony jest uprawniony do przejęcia kierowania obroną państwa w przypadkach, które uniemożliwiłyby wykonywanie obowiązków przez prezydenta, przewodniczącego senatu i premiera.

Szef Sztabu Sił Zbrojnych podlega bezpośrednio ministrowi obrony, jednocześnie jest jego doradcą w sprawach organizacji i użycia sił zbrojnych. Jako najwyższy przełożony wojskowy odpowiada przed ministrem obrony za planowanie, organizację, wyszkolenie, gotowość bojową wojsk. Bierze udział w opracowywaniu budżetu wojskowego. Na okres wojny mianowany jest szefem Sztabu Generalnego i naczelnym dowódcą sił zbrojnych. Organami wykonawczymi szefa Sztabu Sił Zbrojnych są Ogólnowojskowe Centrum Operacyjne i Sztab Ogólnowojskowy.Ogólnowojskowe Centrum Operacyjne realizuje przedsięwzięcia militarne podejmowane przez rząd w celu zapobieżenia lub likwidacji sytuacji kryzysowych, gromadzi i opracowuje informacje szefowi sztabu niezbędne do sprawowania funkcji doradczych, a także jest organem dowodzenia wojskami. Rysunek 3.5. przedstawia szczeble kierowania obronnością Francji.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone



Rys.3.5. Szczeble kierowania obronnością Francji (wariant)

Sztab Ogólnowojskowy jest organem planistycznym szefa Sztabu Sił Zbrojnych. Do jego zadań należy: opracowanie planów użycia sił zbrojnych, organizowanie i prowadzenie szkolenia wszystkich rodzajów wojsk, uczestnictwo w pracach studyjnych dotyczących użycia wojsk.

Na szczeblu niższym za strefy odpowiada funkcjonariusz państwowy w randze prefekta. Dowódca okręgu wojskowego jest pomocnikiem prefekta do spraw obrony wojskowej strefy. Identyczna zasada obowiązuje w departamentach (jednostkach podziału administracyjnego mniejsza obszarowo od województwa w Polsce). We Francji system kierowania państwem na okres wojny, tak jak w Stanach Zjednoczonych Ameryki Północnej nie ulega zmianie.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Infrastruktura telekomunikacyjna sieci publicznej na potrzeby realizacji sieci narodowej może być wykorzystywana na wiele sposobów. Wydaje się że najprostszą metodą, biorąc pod uwagę wymagania bezpieczeństwa jest budowa sieci na bazie dzierżawionych łączy transmisyjnych z jednoczesną własną realizacją komutacji. Takie rozwiązania są stosowane na świecie np. w strategicznej sieci łączności Francji. Użyte systemy komutacyjne dla tej sieci są specjalnymi wersjami central publicznych. System obejmuje dużą liczbę abonentów na terenie kraju. Zarządzanie dzierżawionym i częściowo własnym potencjałem teletransmisyjnym oparte jest na nowoczesnej technologii ATM produkcji krajowego producenta ALCATEL. Wykorzystywane są również elektroniczne automatyczne centrale telefoniczne tego samego producenta. Pozwala to na wykorzystanie wspólnej platformy zarządzania systemem transmisyjnym i komutacyjnym. Zaletą tego systemu jest to, że umożliwia on pełną kontrolę nad systemem tzn. możliwość zdalnego nadawania uprawnień i priorytetów. Za wadę takiego rozwiązania należy uznać to, że koszt budowy takiej sieci jest nadal wysoki. Dodatkowo, korzystanie jedynie z łączy dzierżawionych naturalnie ogranicza zdolność obsługi zwiększonego ruchu. Jakkolwiek wydzielenie na stałe łączy umożliwia zastosowanie utajniania grupowego, tym niemniej jest ono stosunkowo łatwy do identyfikacji co może mieć znaczenie z punktu widzenia bezpieczeństwa.

3.2.Analiza porównawcza systemów kierowania w wybranych państwach NATO wynikające stąd wskazania dla własnych (narodowych) rozwiązań w tym zakresie

Wymagane jest, by państwa członkowskie NATO traktowały krajowe i międzynarodowe systemy łączności jako część globalnej zdolności obronnej sojuszu. W każdym kraju powinna być przygotowana skuteczna procedura organizacyjna umożliwiająca nadzorowanie krajowych systemów telekomunikacyjnych gwarantując niezawodną i bezprzerwową łączność w relacjach krajowych i międzynarodowych. Powinna być zagwarantowana regularna wymiana informacji pomiędzy krajami członkowskimi i wewnątrz sojuszu. W czasie pokoju operatorzy telekomunikacyjni powinni uwzględnić wiele zdarzeń, które mogą mieć wpływ na możliwość obsługi ruchu i świadczenia usług.

Największe zagrożenia to:

- ujawnienie informacji;
- utrata możliwości świadczenia usług lub ograniczenie jej dostępności;
- utrata kontroli nad siecią telekomunikacyjną;

JAWNE
Zastrzeżone

- stopniowa utrata potencjału spowodowana brakiem kadr odpowiedzialnych za obsługę lub serwisowanie.

Należy brać pod uwagę możliwości zagwarantowania wystarczających zasobów ludzkich, tak by dostępne kadry były właściwie przygotowane do funkcji które zostały im przydzielone.

Analiza porównawcza przedstawionych systemów nie da nam jednoznacznej odpowiedzi, który z nich jest lepszy, ponieważ w zakresie określonych wymagań zachodzą zależności wprost lub odwrotnie proporcjonalne. Możemy natomiast przeprowadzić analizę według następujących kryteriów:

Zakres świadczonych usług

System powinien świadczyć dwie ***główne*** grupy usług :

- usługi głosowe;
- transmisja danych, obrazów, fax, poczta elektroniczna.

W ramach świadczonych usług powinien zapewniać:

- automatyczne uzyskiwanie połączeń bezpośrednich i obejściowych;
- możliwość zestawiania priorytetowych połączeń dalekosiężnych;
- współdziałanie z systemami różnych operatorów sieci telekomunikacyjnych;
- bezpośrednie, konferencyjne i indywidualne połączenia między osobami funkcyjnymi;
- automatyczne poszukiwanie abonenta w sieci;
- przyjmowanie abonentów relokowalnych;
- możliwość tworzenia zamkniętych grup użytkowników;
- możliwość nadawania priorytetów;
- możliwość współpracy z abonentami będącymi w ruchu;
- i inne w miarę potrzeb.

Jedną z usług jest również system zarządzania, który powinien obejmować wszelkie działania związane ze sterowaniem, monitorowaniem i rejestrowaniem użycia zasobów sieci, w celu zapewnienia jej efektywnego wykorzystania zgodnie z przeznaczeniem i adaptacją do warunków występujących w jej otoczeniu. Konieczne jest zdefiniowanie struktury funkcjonalnej sieci zarządzania, ustalenie rodzaju wykorzystywanej sieci wymiany danych oraz przyjęcie odpowiednich protokołów telekomunikacyjnych.

Funkcje zarządzania i utrzymania powinny dotyczyć takich obszarów działania, jak:

- administrowanie i sterowanie, obejmujące zbiór wszelkich działań technicznych oraz niezbędnych działań organizacyjnych zmierzających do tego, aby system (urządzenie, abonent) realizował nałożone na niego funkcje i adoptował się do zmian w jego otoczeniu;

- utrzymanie, będące zbiorem działań technicznych i organizacyjnych zmierzających do utrzymania systemu w stanie, w którym może on realizować swoje funkcje lub przywrócenie mu takiego stanu, (możliwość kontroli i automatycznej rejestracji stanu eksploatowanych łączy);
- zabezpieczenie, obejmujące działania związane z planowaniem, gromadzeniem oraz przygotowaniem do wdrożenia nowych lub dodatkowych zasobów sieci, usług i udogodnień;
- utajnianie;
- taryfikacja.

Funkcje określające obszary działania systemu zarządzania, które powinny być wspólne dla systemów współdziałających, niezależnie od roli, zakresu i sposobu ich działania, wyznaczając rodzaj, tryb oraz zakres realizacji zadań związanych z zarządzaniem systemem.

Do zasadniczych zadań systemu zarządzania należy zaliczyć:

- przesyłanie, zapewniające przemieszczanie informacji między poszczególnymi elementami sieci zarządzania;
- rejestrowanie zdarzeń;
- przechowywanie, umożliwiające dostęp do informacji przez określony czas;
- wyszukiwanie, pozwalające selekcjonować zebraną informację;
- przetwarzanie, pozwalające analizować i przekształcać informację;
- ochronę informacji, pozwalającą nadzorować dostęp do odczytu i zmian w przechowywanej informacji.

Bezpieczeństwo informacji przekazywanej w systemie

System powinien spełniać następujące wymagania w zakresie bezpieczeństwa i ochrony informacji:

- ochronę przed nieuprawnionym dostępem do sieci teletransmisyjnej i wykorzystywania jej zasobów, w tym także treści przekazywanych informacji, w pewnych przypadkach powinna ona obejmować, również bezpieczeństwo fizyczne związane z dostępem do budynków, urządzeń czy określonych rejonów;
- ochronę przed nieuprawnionym dostępem do systemu zarządzania i wykorzystywania jego możliwości, w tym także ochronę poufności treści oraz trybu korzystania z informacji wykorzystywanej do celów zarządzania.

Niezawodność i żywotność systemu

W zakresie niezawodności i żywotności system powinien charakteryzować się:

- strukturą (topologią sieci) gwarantującą dużą niezawodność;

JAWNE
Zastrzeżone

- odpornością na zakłócenia radioelektroniczne;
- dużą mobilnością i elastycznością;
- wysokim poziomem stabilności bez względu na powstałą sytuację;
- wysokim wskaźnikiem niezawodności i odporności na destrukcyjne oddziaływanie;
- wymaganą wiernością transmisji;
- unifikacją urządzeń;
- wysoką odpornością na wykrycie i zakłócenie pracy środków radiowych;
- możliwością szybkiego odtwarzania gotowości.

System powinien być zbudowany z wykorzystaniem najnowszych technik i technologii telekomunikacyjnych (system całkowicie cyfrowy). Wskazane jest maksymalne wykorzystanie narodowej myśli technicznej i krajowego potencjału produkcyjnego.

Zasięg systemu (pojemność).

System powinien obejmować obszar całego kraju. Posiadać wyprzedzającą gotowość w stosunku do systemu kierowania państwem w sytuacjach kryzysowych i wojny. Skład i struktura systemu powinna odpowiadać składowi i strukturze systemu kierowania państwem w czasie kryzysu i wojny. Konfiguracja systemu (rozmieszczenie węzłów) powinna być taka, by zmiana systemu kierowania państwem nie powodowała konieczności rekonfiguracji systemu teleinformatycznego. System powinien gwarantować przejście na styku z sieciami resortowymi.

Koszty budowy i utrzymania systemu

Budowa systemu teleinformatycznego na potrzeby kierowania obronnością państwa jest kompromisem wynikającym z powyższych kryteriów. Generalnie można powiedzieć, że zwiększenie: zakresu świadczonych usług, bezpieczeństwa, niezawodności i pojemności systemu powoduje zwiększenie kosztów budowy i utrzymania systemu.

Wnioski

W Polsce funkcjonuje obecnie 16 samodzielnych nowych województw kierowanych przez wojewodów. Wiadomo, że usługi publiczne nie są, jak dotąd dobrze koordynowane, zarówno w wymiarze ponad wojewódzkim, jak i nawet wewnątrz niektórych z nich. Dążąc do rozwiązania tego problemu, kilka nowych województw zaczęło wdrażać rządowe centra antykryzysowe. Centrum takie powstało w Bydgoszczy, a Toruń i Warszawa planują podobne działania.

JAWNE
Zastrzeżone

Koordynacja tworzenia takich ośrodków pomiędzy nowymi województwami przyniosłaby naszemu krajowi wiele korzyści. Po pierwsze, zasoby dostępne w jednym województwie mogłyby zostać w przypadku potrzeby z łatwością wykorzystane w innym województwie. Po drugie, wymieniając informacje o sposobach funkcjonowania, centra mogłyby doskonalić własne operacje na podstawie najlepszych doświadczeń innych ośrodków. Po trzecie, istnieją kryzysy, które ze swej natury wymagają szczegółowego przygotowania planów ewentualnej reakcji na ich wystąpienie w skali wielu obszarów geograficznych. Przykładem może być tranzyt materiałów niebezpiecznych, który wymaga koordynacji pomiędzy województwami i komunikacji na szczeblu krajowym.

Doświadczenia z gromadzenia informacji na jednym etapie okazują się często cenne, również w innych etapach, np. największy udział w kosztach kryzysów ma etap likwidacji szkód i odbudowy. Niemniej jednak, zamiast po prostu odbudowywać wcześniejszą infrastrukturę, na tym etapie warto wykorzystać zasady zmniejszania szkód by zabezpieczyć się przed podobnymi kryzysami w przyszłości. Takie wzajemne relacje są argumentem na rzecz kompleksowego podejścia nie tytko do zarządzania kryzysami, lecz również do informacji kryzysowej.

Najważniejszym instrumentem prawnym regulującym obowiązki w zakresie niesienia pomocy w czasie katastrof np. w USA jest ustawa Roberta T. Stafforda o pomocy w katastrofach i sytuacjach nadzwyczajnych, znana również jako "ustawa Stafforda". Na potrzebę przyjęcia takiej ustawy złożyły się doświadczenia wielu krajów. W każdym przypadku na czas sytuacji nadzwyczajnej pełnia władzy jest przekazywana jednej agencji i jej władza jest uznawana przez pozostałe agendy rządu oraz przez sektor publiczny i prywatny. To właśnie w tej dziedzinie kierownictwo centralne i znaczące zaangażowanie wszystkich uczestników może prowadzić do istotnych ulepszeń w potencjale i do zauważalnego zmniejszenia strat wynikłych z kryzysu. W celu zapewnienia rozwoju, w modelach partnerstwa sektorów publicznego i prywatnego musi zostać wypracowane i utrzymane efektywne podejście organizacyjne. Zadanie organizacji polegałoby na rozwijaniu i wdrażaniu systemu, określaniu lub i rekomendowaniu ulepszeń, wypracowywaniu consensusu, zachęcaniu do udziału organizacji publicznych i prywatnych, wyszukiwaniu możliwości szkolenia, rozszerzaniu systemu, określaniu zapotrzebowania na technologię, dążeniu do normalizacji procedur, i zapewnieniu przywództwa, które ułatwiłoby międzynarodowy rozwój. Prywatny sektor gospodarki może w istocie odegrać kluczową rolę w zarządzaniu sytuacjami kryzysowymi, poprzez swój udział w podstawowej infrastrukturze (obejmującej telekomunikację, energetykę. bankowość, gospodarkę wodną, służby ratunkowe

i awaryjne, transport i zapewnienie utrzymania ciągłości funkcjonowania organów władzy), rolę w sektorze ubezpieczeniowym i wpływ kryzysu na gospodarkę kraju.

Kierowanie obronnością państwa jest procesem bardzo skomplikowanym, wymagającym posiadania odpowiednio przygotowanego systemu kierowania, funkcjonującego nieprzerwanie w okresie pokoju, kryzysu i wojny. Dotychczasowy system kierowania obronnością funkcjonował na bazie zdezaktualizowanych już dokumentów normatywnych z lat siedemdziesiątych i osiemdziesiątych.

Przyjęcie Konstytucji RP zapoczątkowało okres budowy nowego systemu kierowania, dostosowanego do zaistniałych zmian polityczno-militarnych. Jednak wiele zapisów konstytucyjnych, bez uszczegółowienia ich w ustawach i aktach wykonawczych, może spowodować ich niejednoznaczną interpretację, szczególnie w zakresie kompetencji poszczególnych organów kierowania. Dlatego też niezbędne jest szybkie przygotowanie ustaw szczegółowo regulujących sprawy obronności państwa, a szczególnie problematykę systemu kierowania obronnością.

Ustawy te powinny w sposób jednoznaczny określić miejsce i rolę poszczególnych organów kierowania w systemie, a także ich zadania i kompetencje w kierowaniu państwem w najbardziej krytycznych sytuacjach, w czasie zagrożenia militarnego i wojny. W czasie sytuacji kryzysowych należy podjąć działania w celu zapewnienia ciągłości świadczenia usług dla ludności oraz dzierżawionych usług międzynarodowych. W szczególności duże znaczenie ma zapewnienie łączności dyplomatycznej pomiędzy państwami członkowskimi NATO i innej ważnej dla członków sojuszu oraz pomiędzy sojuszem i innymi państwami, tak by umożliwić skuteczne działania na rzecz uniknięcia kryzysu, a także jeśli działania te okażą się nieskuteczne, podjęcia wysiłków w celu osiągnięcia pokoju. Jednak w czasie kryzysów i wojny konieczne jest zastosowanie środków kontroli tak, aby umożliwić podjęcie odpowiednich działań w zakresie zestawiania łączy bezpośrednich i obejściowych pomiędzy państwami sojuszu i innymi.

W tym, kontekście „środki kontroli" oznaczają zarządzanie łączami i ruchem obsługiwanym przez te łącza. Na żądanie właściwych władz krajowych operatorzy telekomunikacyjni powinni stosować środki kontroli odnośnie usług publicznych i dzierżawionych usług międzynarodowych. Rozwiązania te mogą poszerzyć zwykłe funkcje zarządzania siecią w czasie pokoju. W celu zagwarantowania skutecznego kontrolowania międzynarodowych usług telekomunikacyjnych, zarówno publicznych jak i dzierżawionych, ważne jest, aby wszystkie kraje członkowskie NATO wprowadziły uzgodnione środki kontroli jednocześnie i zgodnie z odpowiednimi rozporządzeniami NATO. Możliwe jest

JAWNE
Zastrzeżone

zbudowanie sieci specjalnych, które są wydzielone z sieci publicznych, na potrzeby władz krajowych w sytuacjach szczególnych zagrożeń, kryzysów międzynarodowych lub wojny. Krajowe sieci specjalne mają z reguły ograniczoną pojemność i możliwości obsługi ruch telekomunikacyjnego. Korzystne jest łączenie poszczególnych krajowych sieci specjalnych ze sobą w czasie pokoju lub we wczesnej fazie kryzysu w celu zapewnienia łączności właściwym abonentom specjalnym, co zależy od skali wdrożenia odpowiednich systemów sygnalizacji umożliwiających współpracę sieci międzynarodowych i w efekcie wysoką jakość transmisji. Konieczna może być rozbudowa tych sieci pod kątem obsługi dodatkowego ruch generowanego przez abonentów specjalnych. W celu zagwarantowania użyteczności sieci specjalnych i ich łączy na potrzeby zestawiania połączeń w warunkach wojennych, systemy i łącza tych sieci muszą być maksymalnie uodpornione w taki sposób, by prawdopodobieństwo bezprzerwowej łączności było możliwie wysokie. Wymaga to zaimplementowania różnych tras przesyłania ruch, stosowania wielu dróg obejściowych łączy. Biorąc pod uwagę ograniczoną pojemność krajowych sieci specjalnych, kraje członkowskie mogą wprowadzić kontrolę połączeń zewnętrznych przychodzących do sieci.

W krajach Europy Zachodniej takich jak Francja, Niemcy i innych, powszechnie wykorzystywane są szerokie możliwości systemów cyfrowych. W krajach tych na potrzeby obronności stworzono jednolite cyfrowe systemy łączności w postaci krajowych sieci specjalnych. Sieci te łączą sferę poza militarną kierowania obronnością kraju to jest Policję, Straż Graniczną, ośrodki kierowania administracją państwową, itp. jak również i sferę militarną - stanowiska kierowania obroną. Systemy te tworzą spójny system kierowania obronnością racjonalnie wykorzystujący infrastrukturę teletechniczną kraju umożliwiając jednocześnie tworzenie spójnych systemów kierowania obronnością i obroną. Systemy takie z uwagi na jednorodność sprzętową umożliwiają wykorzystywanie przez kierujących obroną wspólnych systemów informatycznych zwiększając tym samym szybkość obiegu informacji a co za tym idzie również wpływają na wysoką ich efektywność.

I tak np. firma OPTIMUS LOCKHEED MARTIN (OLM) proponuje model generalnie oparty na systemie Amerykańskiej Federalnej Agencji Antykryzysowej (FEMA). Zadaniem Agencji jest "ograniczanie strat ludzkich i materialnych oraz ochrona instytucji przed wszelkimi zagrożeniami poprzez kierowanie społeczeństwem i wspieranie go w ramach kompleksowego, opartego na ryzyku programu antykryzysowego, polegającego na zmniejszaniu szkód, przygotowaniach, reakcji i odbudowie". FEMA jest niezależną agencją rządu federalnego podległą prezydentowi. Niemniej jednak, bez względu na to czy

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

zostanie wybrany model FEMA, konieczne jest wyodrębnienie jednego ośrodka decyzyjnego posiadającego pełną kontrolę w czasie kryzysu oraz przygotowanie planów i procedur.

W sytuacji teoretycznie idealnej, polityka decydowałaby o wymaganiach technicznych. Wymagania techniczne przesądziłyby o projekcie systemu, a ten z kolei wymagałby doboru i zakupu komponentów technicznych odpowiednich dla wdrożenia właściwych procedur. W takiej sytuacji zostałaby sformułowana polityka adekwatna do wszystkich możliwych sytuacji i możliwe byłoby uniknięcie marnowania czasu i środków na zakup ,lub stosowanie systemów, które nie odpowiadają ich docelowemu przeznaczeniu. W takiej sytuacji "wzorcowej", w której czas i środki mogłyby by nieograniczone, doradzalibyśmy zdefiniowanie i wdrożenie krajowej polityki antykryzysowej przed rozwinięciem jakiegokolwiek potencjału operacyjnego.

Realia są jednak dalekie od ideału i z tego powodu proponuje się rozwijanie potencjału operacyjnego równolegle z formułowaniem i uchwalaniem nowej racjonalnej polityki antykryzysowej. W ten sposób działania te będą się uzupełniać. Reagowanie na kryzysy, likwidacja szkód, przygotowania i szkolenie oraz zmniejszanie zasięgu szkód to głównie obowiązki społeczności lokalnych, choć często potrzebują one pomocy szczebla wojewódzkiego lub centralnego.

Fundamentalnym problemem jest to, że zasięg kryzysów przekracza wiele granic: organizacyjnych, politycznych, geograficznych, profesjonalnych, tematycznych i socjologicznych. Oznacza to, że informacje dotyczące zaistniałego kryzysu muszą trafić do wszystkich zainteresowanych stron na szczeblu lokalnym, wojewódzkim i krajowym, zarówno w sektorze publicznym jak i prywatnym. Istnieje ponadto potrzeba zintegrowania informacji pomiędzy wielu dyscyplinami, organizacjami i regionami geograficznymi.

JAWNE
Zastrzeżone

4. OCENA WYKORZYSTANIA I MOŻLIWOŚCI SYSTEMU TELEKOMUNIKACYJNEGO W KIEROWANIU OBRONNOŚCIĄ PAŃSTWA

4.1. Sieć telekomunikacyjna kraju

System łączności państwa

Podstawowym elementem podsystemu kierowania obronnością państwa jest niezawodnie funkcjonująca łączność w szerokim znaczeniu tego słowa. Jej zdolność do wykonywania zadań na rzecz obronności zależy przede wszystkim od stanu i możliwości rozbudowy infrastruktury systemu telekomunikacyjnego na obszarze kraju oraz jego sprawności organizacyjno-technicznej.

Obszar systemu łączności państwa na potrzeby obronności kraju jest niezwykle rozległy i złożony, obejmuje wiele autonomicznych podsystemów, który w dużym uproszczeniu przedstawiono na rys. 4.1. System telekomunikacyjny, to zespół urządzeń i linii telekomunikacyjnych, połączony według określonych zasad oraz współpracujący ze sobą, przeznaczony do wymiany informacji pomiędzy użytkownikami - świadczenia usług telekomunikacyjnych[20]

. Sieć telekomunikacyjna użytku publicznego, administrowana przez resort łączności, stanowiąca podstawowe ogniwo systemu, przeznaczona jest do świadczenia usług na potrzeby ogółu społeczeństwa, gospodarki narodowej oraz organów władzy państwowej i administracji. Sieć telekomunikacyjną tworzą:

- obiekty i linie telekomunikacyjne (kablowe, napowietrzne i radiowe);
- obiekty teletransmisyjne;
- obiekty radiokomunikacyjne (łączności radiowej i radiotelefonicznej, radiofonii i telewizji);
- naziemne stacje łączności satelitarnej.

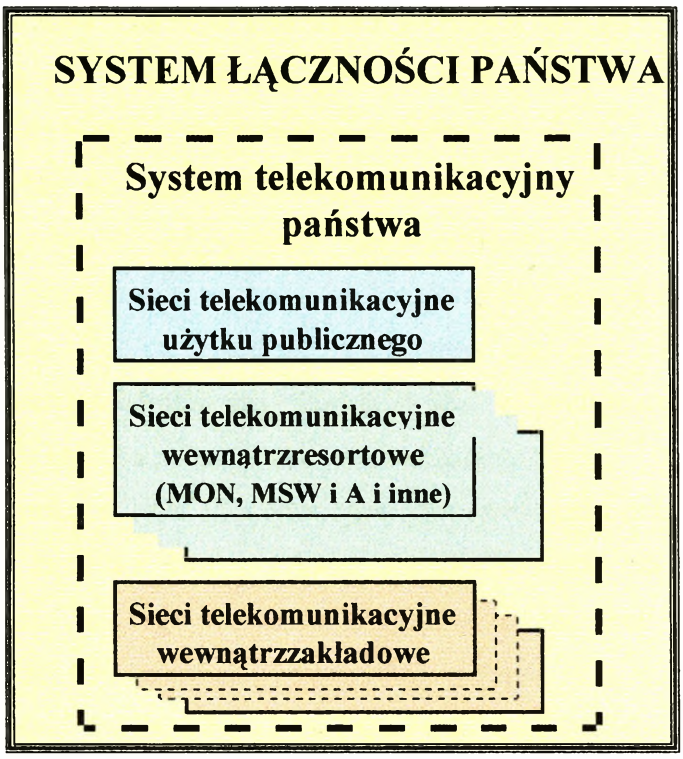
W Polsce działa wiele typów sieci telekomunikacyjnych o charakterze publicznym:

- komutowane sieci telefoniczne PSTN (Public Switched Telephone Network);
- teledacyjne sieci z komutacją kanałów CSPDN (Curcuit Switched Public Data Network);
- teledacyjne sieci z komutacją pakietów PSPDN (Public Switched Packed Data Network);
- sieci telegraficzne (Telex);

---

[20] Słownik pojęć z zakresu telekomunikacji w zastosowaniach cywilnych i wojskowych. AON. Warszawa 1996

JAWNE
Zastrzeżone



Rys. 4.1. System łączności państwa (wariant)

- radiotelefoniczne sieci komórkowe MT (Mobile Telephony);
- sieci wydzielone o charakterze lokalnym lub prywatnym (PABX, LAN, dyspozytorskie, specjalne).

W sieciach telekomunikacyjnych do połowy lat siedemdziesiątych stosowano powszechnie technikę przesyłania sygnałów analogowych za pomocą kanałów telefonicznych w podstawowym paśmie przenoszenia lub przez kosztowne międzycentralowe urządzenia zwielokrotnienia częstotliwościowego o niewielkiej krotności kanałów rozmównych. Jako linie przesyłowe stosowano wyłącznie pary kabli miedzianych o ograniczonej częstotliwości pracy, wymagające skomplikowanych filtrów, korektorów linii (krarupinizacja, pupinizacja) i tłumików zakłóceń przy przesyłaniu sygnałów o wyższych częstotliwościach. Tradycyjna telekomunikacja oparta na komunikacji porozumiewawczej obejmującej usługi telefoniczne, telegramowe i teleksowe wymagała kanałów o niewielkiej przepływności, wykorzystujących prawie wyłącznie analogowe linie telefoniczne z podstawowym pasmem przenoszenia

JAWNE Zastrzeżone

w zakresie 300 - 3400 Hz. Dopiero istotne zmiany w telekomunikacji stały się możliwe po opanowaniu cyfrowej techniki kodowania mowy, wprowadzeniu techniki zwielokrotnienia kanałów oraz światłowodów, a przede wszystkim włączeniu do sieci telekomunikacyjnej elementów komutacji (przełączania) pochodzących z technologii sieci komputerowych.

Uwarunkowania prawne standaryzacji telekomunikacji

Przed rokiem 1989 dostępność do usług telekomunikacyjnych w Polsce, ich jakość, powszechność i dostosowanie do potrzeb użytkowników sieci telekomunikacyjnej pozostawiały wiele do życzenia. Od stycznia 1992 r. ówczesny minister łączności podzielił przedsiębiorstwo Poczta Polska, Telegraf i Telefon na dwie firmy: Państwowe Przedsiębiorstwo Użyteczności Publicznej "Poczta Polska" i Telekomunikację Polską S.A. Lata 90-te to przewartościowanie pojęć dotyczących telekomunikacji.

Ustawa o łączności z 1990 r. (i późniejsze jej nowelizacje) dopuściła konkurencję w telekomunikacji. W myśl tej ustawy lokalni operatorzy mogą tworzyć własne sieci, a Telekomunikacja Polska S.A. ma obowiązek przyłączać ich do sieci użytku publicznego (ogólnokrajowej). Obecnie ustawa z dnia 21 lipca 2000r. „ Prawo telekomunikacyjne" określa właściwie wykonywanie i świadczenie jak i dostępność usług telekomunikacyjnych oraz eksploatację sieci. Obszar działalności telekomunikacyjnej i świadczonych usług telekomunikacyjnych nadzoruje i kontroluje powołany z dniem 01.01.2001r. Urząd Regulacji Telekomunikacji. Od kilku lat rośnie też zainteresowanie budową i modernizacją resortowych sieci telekomunikacyjnych, a w ostatnim czasie nowych sieci multimedialnych. To z kolei spowodowało wzrost zainteresowania centralami wyposażonymi w możliwość świadczenia usług ISDN i zaawansowanych usług multimedialnych. Jednak wysokie ceny usług i urządzeń końcowych (terminali ISDN) oraz ograniczenie techniczne operatorów uniemożliwiają powszechne korzystanie z usług ISDN.

Dla dostawców urządzeń sieci abonenckich, resortowych i wewnątrzzakładowych jedynym wymogiem formalnym wobec instalowanego sprzętu jest obecnie świadectwo homologacji. Obowiązujące w Polsce wymagania ustawowe przewidują, że urządzenia telekomunikacyjne przeznaczone do pracy w sieciach użytku publicznego lub do współpracy z tymi sieciami oraz wszystkie urządzenia radiokomunikacyjne nadawcze i nadawczo-odbiorcze mogą być zakładane i używane tylko po uzyskaniu świadectwa homologacji, za wyjątkiem urządzeń zwolnionych od obowiązku uzyskania tego świadectwa.

Świadectwo homologacji może być wydane przez ministra łączności lub upoważniony organ na podstawie opinii uprawnionych podmiotów, stwierdzającej, że urządzenie spełnia wymagania zawarte w obowiązujących przepisach prawnych oraz

JAWNE

Zastrzeżone

Polskich Normach wprowadzonych do obowiązkowego stosowania. Zważywszy, że Polskie Normy wprowadzone przez ministra łączności do obowiązkowego stosowania, a także obowiązujące przepisy techniczne są w znacznym stopniu zgodne z międzynarodowymi zaleceniami i standardami, można uznać, że polska procedura homologacyjna jest w dużej mierze zbieżna z zasadami wydawania certyfikatów przyjętych w UE.

Pierwszą, międzynarodową organizacją standaryzacyjną, była założona w 1865 roku w Paryżu, Unia Administracji Telegrafów, przemianowana w 1932 roku na Międzynarodową Unię Telekomunikacyjną (ITU – ang. International Telecommunication Union). Od chwili powstania Organizacji Narodów Zjednoczonych, ITU, stała się jej agendą skupiającą przedstawicieli rządowych administracji telekomunikacyjnych państw członkowskich. Siedzibą Unii jest Genewa.

W roku 1993 po reorganizacji Unii, Międzynarodowy Komitet Konsultacyjny Radiofonii (CCIR) oraz Międzynarodowy Komitet Konsultacyjny Telegrafii i Telefonii (CCITT) stały się sektorami standaryzacyjnymi ITU (w skrócie ITU-R dla radiofonii oraz ITU-T dla telekomunikacji).

Drugą organizacją standaryzacyjną o światowym zasięgu jest Międzynarodowa Organizacja Standaryzacyjna (ISO – ang. International Standard Organisation) założona w 1947 roku w Londynie, skupiająca narodowe organizacje standaryzacyjne (w Polsce Polski Komitet Normalizacji Miar i Jakości).

W Europie najważniejszym ośrodkiem standaryzacyjnym jest Europejski Instytut Standaryzacji Telekomunikacji (ETSI – ang. European Telecommunication Standard Institute), mający swą siedzibę w Sophia-Atipolis we Francji, działający od początku lat osiemdziesiątych.

Określenie standardów bywa używane w kontekście wielu dokumentów. Spośród rozmaitych typów standardów wyróżnia się trzy podstawowe typy:

1. Normy (True Standards) są wymaganiami określającymi usługę bądź produkt, które zwykle są akceptowane przez producentów sprzętu, dostawców usług, bądź administracje rządowe.
2. Regulacje (Regulations) to uzgodnienia międzynarodowe, wprowadzane w życie na podstawie umów, nabierające mocy standardów w dwóch dziedzinach:
   - we współdzieleniu radiowego pasma częstotliwości oraz
   - we współpracy dotyczącej wspólnego świadczenia usług.

Zalecenia (Recommendations) są najpopularniejszymi dokumentami publikowanymi przez ITU-T w dziedzinie telekomunikacji lub przez ITU-R w dziedzinie radiofonii.

JAWNE

Zastrzeżone

JAWNE
Zastrzeżone

Stosowanie tych zaleceń jest dobrowolne, aczkolwiek zdecydowana większość producentów sprzętu i operatorów sieci, stara się do nich dostosowywać. Zalecenia ITU-T (oraz ITU-R) możemy podzielić na trzy grupy:

- zalecenia dotyczące wydajności i efektywności pracy sieci;
- zalecenia dotyczące podziału częstotliwości w sieciach kablowych;
- zalecenia opisujące sprzęt i wyposażenie telekomunikacyjne.

Wielkość i dynamika rozwoju rynku telekomunikacyjnego powoduje konieczność uzgadniania i stosowania standardów obowiązujących wszystkich, którzy działają na tym rynku. Jednolitość standardów zwiększa także możliwości swobodnego dostępu do rynku wielu dostawców sprzętu i usług. Zasady standaryzacji stały się podstawą obowiązujących obecnie uregulowań prawnych. W Unii Europejskiej podstawą uregulowań są ujednolicone procedury dotyczące uznawania standardów telekomunikacyjnych (Wspólne Europejskie Regulacje Techniczne) oraz procedury badań technicznych i wydawania certyfikatów zgodności sprzętu z obowiązującymi standardami. Przyjęcie zasady wzajemnego uznawania certyfikatów przez kraje członkowskie Unii prowadzi do tego, że urządzenia telekomunikacyjne pochodzące z poszczególnych krajów Unii mogą być sprzedawane i użytkowane na terenie krajów Unii.

Należy zauważyć, że stosowany w UE wymóg certyfikacji końcowych urządzeń telekomunikacyjnych jest bezwzględny, a zasada wzajemnego uznawania certyfikatów nie obejmuje krajów nie będących członkami UE, a więc i Polski. W przypadku sprzętu pochodzącego z takich krajów obowiązek uzyskania certyfikatu może być traktowany jako instrument administracyjnej kontroli warunków wejścia na rynek UE.

Analizując całokształt zagadnień związanych z integracją polskiej telekomunikacji z telekomunikacją na świecie, a zwłaszcza w krajach UE, należy podkreślić, że rozwiązywanie problemów związanych z certyfikacją i standaryzacją jest jednym z kluczowych elementów mogących ułatwić lub utrudnić realizację procesu integracyjnego.

W przypadku polskich procedur homologacyjnych należy dodatkowo uwzględnić wymóg uzyskania świadectwa homologacji również w stosunku do urządzeń wewnątrzsieciowych - co wynika z dużej liczby nadal eksploatowanych przestarzałych urządzeń, których wymiana i modernizacja odbywa się sukcesywnie, ale powoli. Ta bariera sprawia, że trwający proces rozbudowy sieci krajowej wymaga zachowania możliwości współpracy takich urządzeń z nowymi instalowanymi urządzeniami i systemami telekomunikacyjnymi m.in. poprzez stosowanie wymogu zachowania kompatybilności technicznej i funkcjonalnej.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

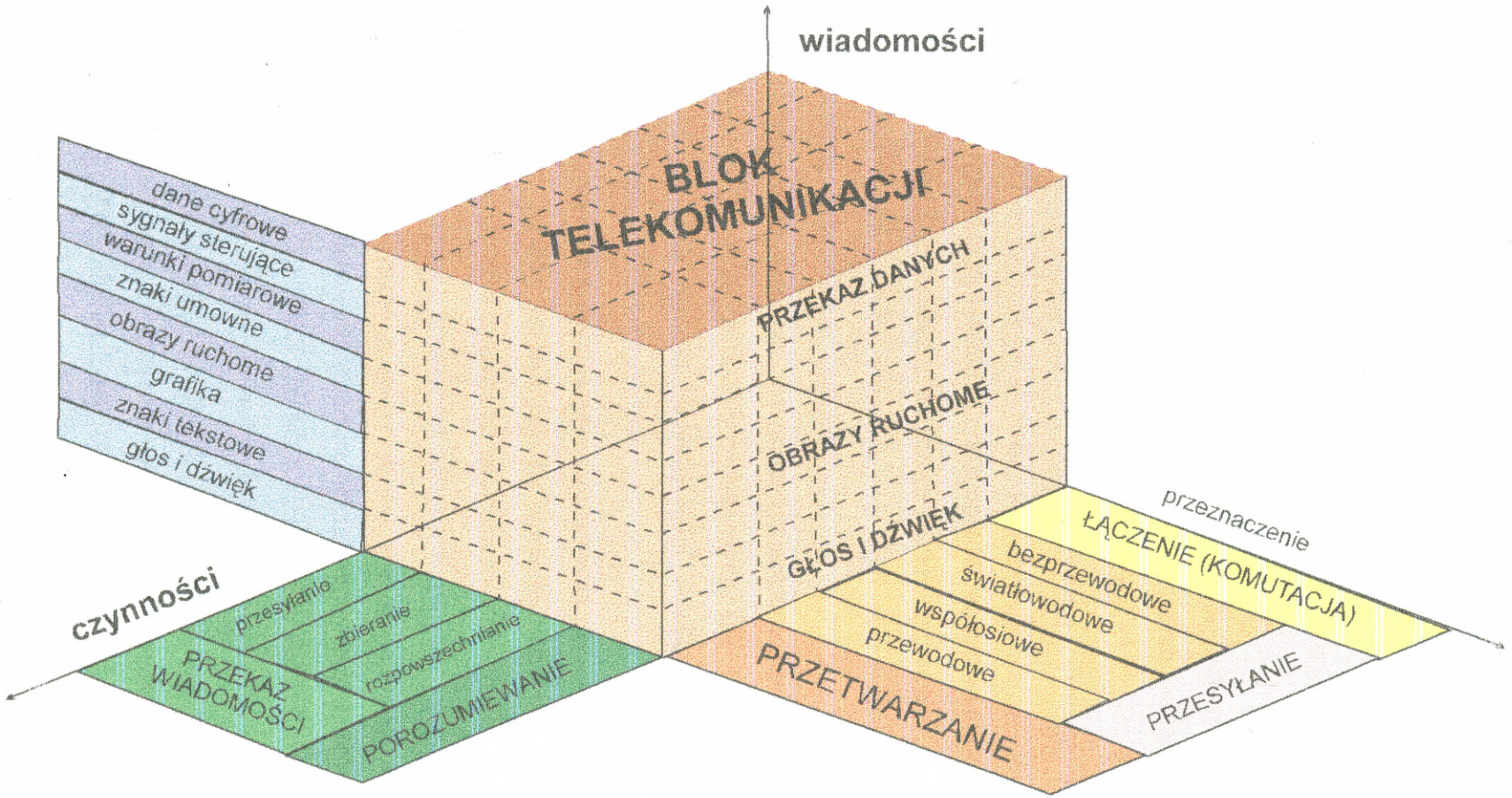
Procedury te dotyczą końcowych urządzeń telekomunikacyjnych i nie odnoszą się do urządzeń w wnątrzsieciowych instalowanych przez poszczególnych operatorów. Ustaleniem jednolitych parametrów technicznych urządzeń wewnątrzsieciowych i systemów w UE zajmuje się Europejski Instytut Standardów Telekomunikacyjnych EIST, którego członkiem jest również polska administracja łączności i Instytut Łączności w Warszawie, pełniący rolę krajowej jednostki standaryzacyjnej w tym zakresie na mocy porozumień z udziałem Polskiego Komitetu Normalizacji.

4.2. Klasyfikacja telekomunikacji

Termin telekomunikacja wywodzi się z greckich słów *tele* (odległy) i *communicare* (dzielenie się z kimś), co łącznie oznacza przesyłanie wiadomości na odległość, bez wnikania, w jaki i jakimi środkami zostanie to zrealizowane. Obecnie termin telekomunikacja oznacza przesyłanie informacji (np. głosu, dźwięku, danych, sygnałów optycznych, faksów, grafiki i obrazów ruchomych) na odległość za pomocą urządzeń elektronicznych zarówno w postaci sygnałów analogowych jak i cyfrowych. Podział telekomunikacji przedstawiono na rys.4.2.

Ze względu na rodzaj przekazywanych wiadomości wyróżnia się telefonię (dział telekomunikacji obejmujący przesłanie wiadomości słownych - dźwięków mowy, za pomocą sygnałów elektrycznych pomiędzy abonentami sieci telefonicznej), radiofonię (przekazywanie dźwięku, mowy i muzyki), telegrafię (znaków pisma), symilografię (obrazów nieruchomych), telemetrię (danych pomiarowych), sygnalizację (umownych znaków zastępujących zdania), telemechanikę (impulsów sterujących), teledację (danych cyfrowych). Ze względu na rodzaj wykonywanych operacji w procesie przekazywania wiadomości wyróżnia się odrębne dziedziny zajmujące się: techniką przetwarzania wiadomości na sygnał i odwrotnie, teletransmisją – związaną z przesyłaniem sygnałów po łączach, telekomutacją – związaną z tworzeniem dróg połączeniowych, umożliwiającą tworzenie i likwidowanie zestawów łączy. Najnowsza klasyfikacja ujmuje usługi telekomunikacyjne w dwie wzajemnie przenikające się grupy: aplikacje telekomunikacyjne i usługi przenoszenia, zwane również usługami transportowymi sieci.

JAWNE
Zastrzeżone



Rys.4.2. Ogólny podział telekomunikacji (wariant)

JAWNE

Zastrzeżone

Pomimo szybkiego rozwoju różnorodnych usług telekomunikacyjnych, to jeszcze nadal dominująca rolę spełnia jednak rynek usług telefonicznych. Do realizacji określonych usług telekomunikacyjnych przeznaczone są różne rodzaje łączy telekomunikacyjnych. Ich rodzaje i cechy użytkowe przedstawiono w tabeli 4.1. Przepływności i zasięgi łączy telekomunikacyjnych zamieszczono na rysunku 4.3.

Intensywny rozwój technologii i usług telekomunikacyjnych w XX wieku doprowadził do powstania nowych dziedzin telekomunikacji związanych z przesyłaniem głosu, dźwięku, obrazu i danych. Funkcjonujące do tej pory kryteria podziału telekomunikacji obejmują wiele sposobów klasyfikacji, wśród których do najważniejszych należą:

Ze względu na zastosowanie przekazów wyróżnia się:

- telekomunikację porozumiewawczą, dotyczącą dwukierunkowego przekazywania wiadomości miedzy dwoma lub więcej punktami. W tym sposobie łączenia rozmówcy lub abonenci wymieniają wiadomości przeznaczone wyłącznie dla nich;
- telekomunikację rozsiewczą dotyczącą jednokierunkowego przekazywania wiadomości z jednego punktu do wielu punktów, przy czym stacja nadawcza nadaje jednocześnie dla wielu bliżej nie określonych odbiorców;
- telekomunikację zbiorczą, dotyczącą jednokierunkowego przekazywania (zbierania) wiadomości z wielu punktów pomiarowych lub badawczych do jednego punktu odbiorczego. Taka sytuacja zachodzi m.in. w telemetrii i w teledacji, tj. zdalnym przekazywaniu wyników pomiarów.

Współczesna infrastruktura teleinformatyczna obejmuje dwie do niedawna odrębne, a obecnie coraz bardziej przenikające się hierarchiczne struktury komunikacyjne: rozległe cyfrowe sieci komputerowe oparte na strukturach sieciowych typu LAN, MAN i WAN oraz sieci telekomunikacyjne , dla których centralnym punktem nadal pozostają cyfrowe systemy komutacji (centrale) wraz z różnorodnymi sieciami dostępu abonenckiego W sieciach komputerowych podstawową strukturę teleinformatyczną dostępu lokalnego tworzą sieci LAN typu Ethernet (10 Mb/s i 100 Mb/s, 1000 Mb/s), Token Ring (4 i 16 Mb/s) i FDDI (100 Mb/s), przeznaczone dla indywidualnych lub grupowych użytkowników z wykorzystaniem zasobów multimedialnych. Fragmenty tych homogenicznych i heterogenicznych sieci komunikacyjnych są łączone między sobą za pomocą węzłów (krotnice synchroniczne klasy DXC, SDXC i SXC, multipleksery ADM, krotnice PCM, routery). Na najniższym poziomie komutacji funkcjonują systemy komutacji (cyfrowe) i centrale telefoniczne (głównie analogowe), a także analogowe i cyfrowe centrale abonenckie PABX.

JAWNE
Zastrzeżone

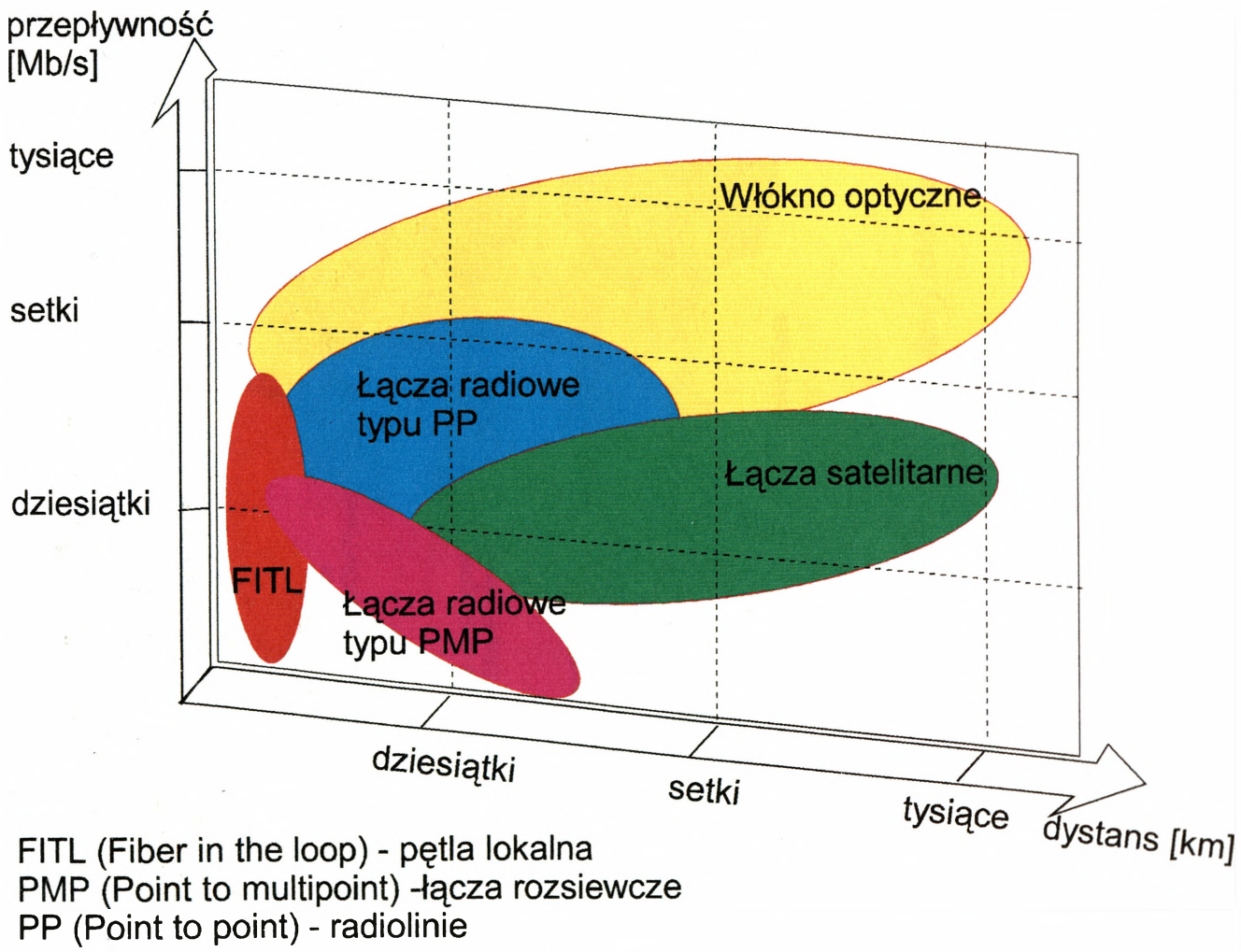
Tabela.4.1.

Parametr	Rodzaj łącza		Główne cechy użytkowe
Rodzaj Transmisji	**Analogowe**		Przenoszenie ciągłego sygnału analogowego w całym dostępnym paśmie częstotliwości.
	Cyfrowe		Transmisja sygnału w postaci cyfrowej. W porównaniu do łącza analogowego znacznie wyższa odporność na zakłócenia.
Sposób Relacji	**Komutowane**		Jest zestawiane przez system komutacyjny wyłącznie na czas trwania rozmowy lub usługi. Kontrolę nad zestawieniem, utrzymaniem i rozłączeniem realizują centrala telefoniczna lub system komutacji. Możliwość transmisji danych
	Dzierżawione (trwałe i okresowe)		Linie dzierżawione są najlepszym rozwiązaniem w sytuacji, gdy ruch odbywa się stale, cechuje się dużą przepływnością, a każde żądanie transmisji musi być obsłużone bezzwłocznie. Opłacalne tylko przy dużym trafiku (generowanym ruchu). Większa szybkość niż łączy komutowanych, przy niższej stopie błędów - co wynika z omijania pól komutacyjnych w centrali telefonicznej. Trasy i punkty końcowe ustalane czasowo lub na stałe z wyprzedzeniem realizacji połączeń.
Charakter Medium	**Kablowe**	**Przewodowe**	Powszechnie stosowane medium miedziane znane jako: linia napowietrzna, kabel prosty, skrętka, podwójna skrętka, kabel wielożyłowy, kabel współosiowy ((koncentryk). Typowy zakres przenoszenia od 0 (prąd stały) do kilkudziesięciu MHz.
		Światłowodowe	Oferta najwyższych przepływności binarnych opartych na włóknach optycznych jedno- i wielomodowych. Maksymalna przepływność powyżej kilkudziesięciu Gb/s.
		Hybrydowe	Połączenie miedzianej i optycznej technologii przekazu z przeznaczeniem do realizacji abonenckich usług multimedialnych. Interaktywne i asymetryczne usługi wideofoniczne o przepływności kilku Mb/s.
	Bezprzewo-Dowe	**Podczerwone**	Wykorzystanie promieniowania podczerwonego do tworzenia bezprzewodowych sieci lokalnych w pomieszczeniach budynków i halach fabrycznych. Typowa przepływność do 10 Mb/s, maks. 50 Mb/s.
		Radiowe naziemne (stałe i komórkowe)	Różnorodna oferta komunikacji radiowej opartej na stałych łączach dwupunktowych typu P-P (radiolinie) i wielopunktowych typu P-M, a także łączności rozsiewczej (radiofonia i telewizja) oraz komórkowej (analogowej i cyfrowej)
		Satelitarne	Obsługa szerokopasmowej międzykontynentalnej łączności telefonicznej i telewizyjnej wraz z przekazem danych. Utrzymanie komunikacji na obszarach trudno dostępnych (VSAT), globalnej komunikacji komórkowej o charakterze osobistym (2 Mb/s) oraz komunikacja , nawigacja i lokalizacja pojazdów znajdujących się w ruchu.
Szybkość Transmisji	**Podakustyczne**		Telemetryczne i komunikacyjne łącza o szybkości nie przekraczającej 600 b/s
	Akustyczne		Analogowe łącza transmisyjne (0.3 -64 kb/s)
	Wąskopasmowe		Cyfrowe łącza komunikacyjne do szybkości maksymalnej 2 Mb/s
	Szerokopasmowe		Komunikacja z szybkością powyżej 2 Mb/s

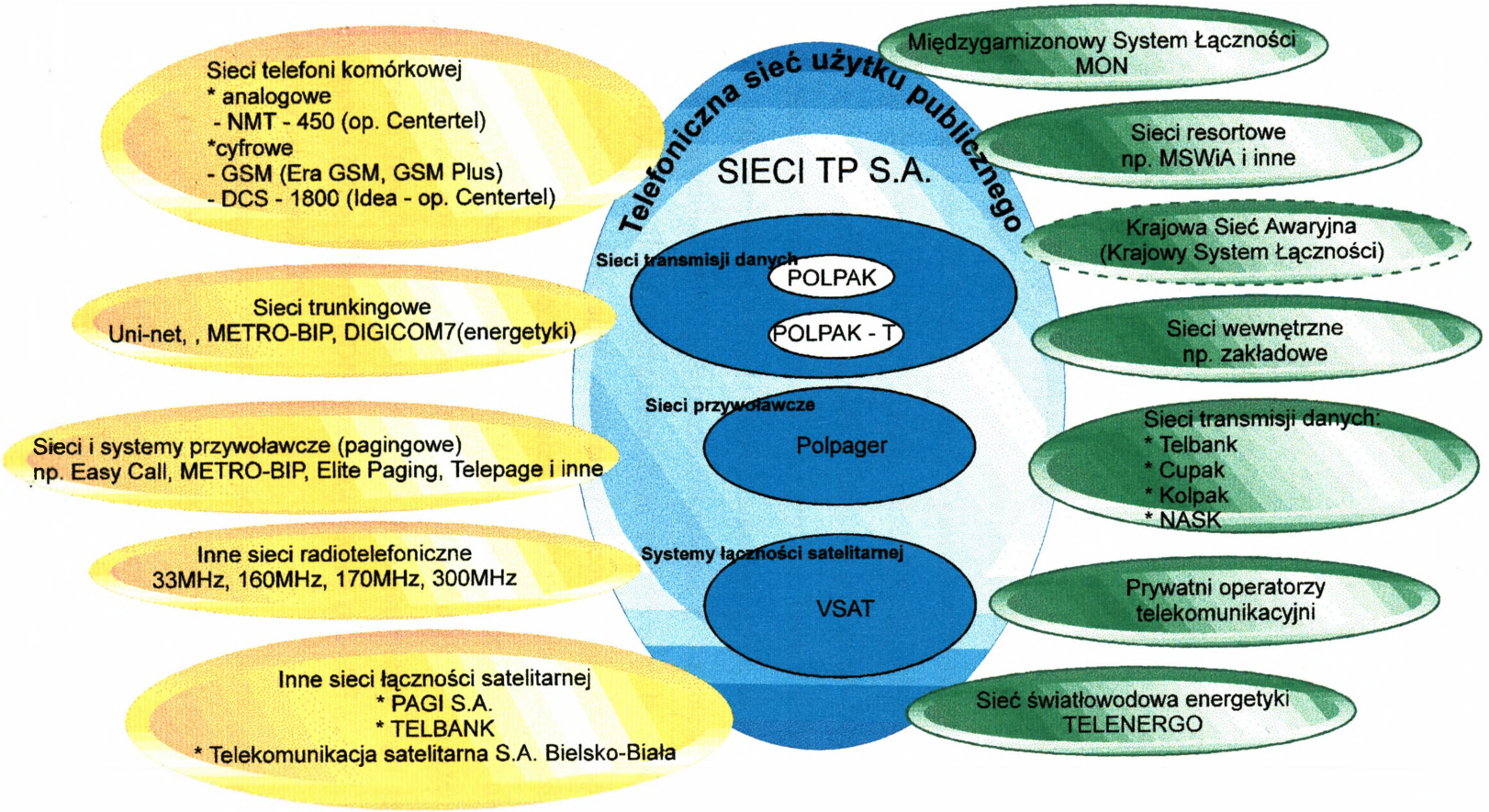
Oddaleni indywidualni użytkownicy mają możliwość włączenia się do sieci teleinformatycznej:

JAWNE
Zastrzeżone

- komutowana lub dzierżawioną linia telefoniczna za pośrednictwem modemów i central telefonicznych PABX;
- kanałami cyfrowymi ISDN, przez centralę lub systemy komutacji cyfrowej;
- kanałami telewizji kablowej, z wykorzystaniem kanału zwrotnego i modemów szerokopasmowych RF (Radio Frequency), zwanych kablowymi;
- torami światłowodowymi, przez sieci optyczne FITL lub za pomocą techniki hybrydowej HFC i modemów DSL. Odrębną grupę stanowią bezprzewodowe sieci dostępu abonenckiego RRL funkcjonujące w kilku standardach europejskich, specjalizowane sieci teledacyjne, przywoławcze i komórkowe (NMT, GSM, DCS), jak też systemy komunikacji i nawigacji satelitarnej (VSAT, GPS, UMTS, FPLMTS i inne). Ogólną infrastrukturę telekomunikacji kraju przedstawiono na rys.4.4.



Rys. 4.3. Typowe przepływności i zasięgi łączy telekomunikacyjnych.



Rys.4.4. Schemat infrastruktury telekomunikacyjnej kraju (wariant)

JAWNE
Zastrzeżone

4.3. Zintegrowana usługowo sieć cyfrowa ISDN

ISDN (ang. Integrated Services Digital Network) Telefonia jest nadal dominującą usługą w sieciach telekomunikacyjnych, to zapotrzebowanie na zaawansowane nietelefoniczne usługi gwałtownie rośnie. Kolejnym etapem rozwoju telefonii jest ISDN[21]. W wąskopasmowej sieci ISDN (typu 2B + D) abonent ma możliwość dostępu do dwóch jednakowych, dwukierunkowych i wzajemnie niezależnych kanałów informacyjnych B, każdy o maksymalnej przepływności binarnej 64 kb/s, oraz do jednego kanału D o szybkości 16 kb/s. Kanał D jest przeznaczony do przesyłania sygnalizacji lub transportu danych telemetrycznych. Powszechnie stosowana sieć analogowa pozwala na korzystanie z różnych usług (np. telefonicznych, transmisji danych) pod warunkiem posiadania oddzielnego łącza (numeru) dla każdej z nich. ISDN umożliwia korzystanie ze wszystkich rodzajów usług przy użyciu tylko jednego łącza (numeru). Transmisja w sieci ISDN odbywa się cyfrowo od abonenta do abonenta. ISDN to jedno łącze, 2 linie jednocześnie, 8 urządzeń. Jedno łącze ISDN umożliwia instalację 8 urządzeń końcowych (np. telefon, telefaks, komputer), z których każde może posiadać własny numer wewnętrzny. Dwa z nich mogą pracować równocześnie. Wybór urządzenia końcowego następuje automatycznie, to znaczy, że rozmowa jest łączona z aparatem telefonicznym, połączenie inicjowane przez telefaks z telefaksem, a przesyłane pliki danych trafiają do komputera. Poza omówionym łączeniem automatycznym istnieje także możliwość wybierania urządzenia końcowego poprzez jego numer wewnętrzny. Do łącza ISDN można przyłączyć: telefony ISDN, telefaksy, zestawy wideokonferencyjne, komputery wyposażone w karty ISDN itp. Okazuje się jednak, że nie tylko, jeżeli użytkownik posiada sprzęt analogowy, może go również wykorzystać. Potrzebne mu będzie dodatkowe urządzenie tzw. adapter, umożliwiające funkcjonowanie tego sprzętu w sieci cyfrowej z integracją usług. Zalety ISDN przedstawiono na rys.4.5[22]..

Usługi w sieciach ISDN

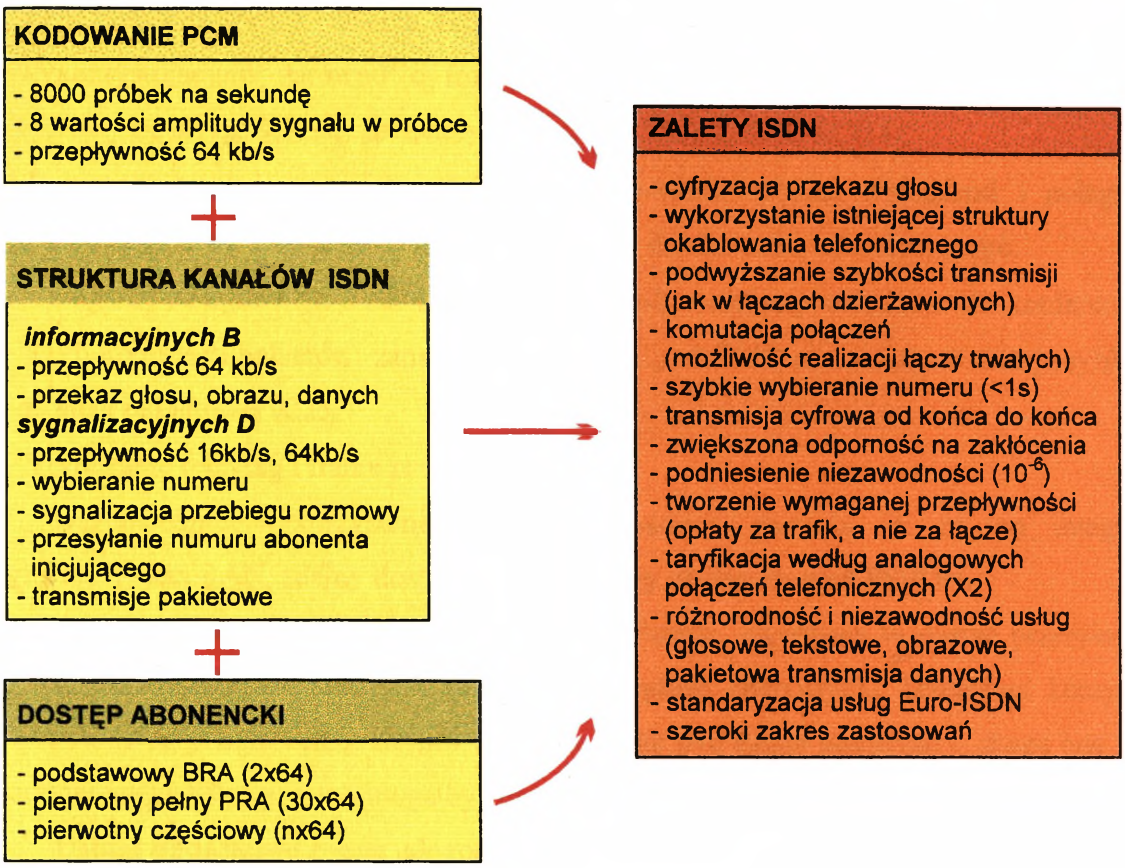
Usługi dostępne w sieciach ISDN podzielone są na następujące grupy:

A. Usługi bazowe /usługi przenoszenia/ (bearer services);
B. Teleusługi (teleservices);
C. Usługi dodatkowe;
D. Usługi dodane.

---

[21] Rick Arnold, *ISDN bez tajemnic,* MIKOM, Warszawa 1998
[22].Vademecum Teleinformatyka, cz.1. Networld. 1998

JAWNE
Zastrzeżone



Rys.4.5. Zalety zintegrowanej sieci cyfrowej ISDN.

Usługi przenoszenia obejmują zestawianie i rozłączanie połączeń pomiędzy użytkownikami oraz przesyłanie informacji pomiędzy stykami użytkownika a siecią i w samej sieci, bez ingerencji w jej treść. Przykładami usług przenoszenia są:

- Usługa trybu łączowego 64 kbit/s, nieograniczone, która zapewnia w pełni przezroczysty kanał cyfrowy do transmisji plików oraz dostęp do sieci pakietowej X.25 oraz TD o niższych szybkościach w postaci zwielokrotnionej do szybkości 64kb/s Przy tej usłudze sieć nie zapewnia przekazywania wewnątrzpasmowych sygnałów tonowych w kanale B.
- Usługa trybu łączowego - 3,1 kHz audio odpowiadająca obecnym usługom telefonicznym. Usługa wykorzystywana do transmisji sygnałów mowy, TD faksów grup 1,2,3, oraz sygnałów od urządzeń dołączonych poprzez modemy. Sygnał cyfrowy na styku S/T ma charakterystykę typu A /zal. CCITT G.711/. Usługa umożliwia współpracę systemów cyfrowych z siecią analogową.
- Usługa trybu łączowego 64 kb/s do transmisji mowy - mowa (speech) odpowiada usłudze telefonicznej ale tylko w sieci ISDN. Sygnał foniczny zakodowany zgodnie z zaleceniem

JAWNE
Zastrzeżone

G.711. może być przekazany zarówno innemu użytkownikowi systemu, jak i systemom rozpoznawania mowy. Usługa zapewnia poprawną komunikację pomiędzy abonentami wykorzystującymi zarówno cyfrowe, jak i analogowe aparaty telefoniczne. Sygnał cyfrowy na styku S/T ma charakterystykę typu A /zal. CCITT G.711/.

- Usługa trybu łączowego 2 x 64 kb/s odpowiada usłudze wideofonii i polega na rezerwowaniu dwóch kanałów na tej samej trasie do abonenta wywoływanego.
- Usługa trybu łączowego 1920 kb/s, kanał H12 odpowiada np. usłudze wideokonferencji;
- Tryb komutacji pakietów: zapewnia usługi SVC, lub PVC oraz dostęp o dużej szybkości do sieci pakietowej X.25.
- Tryb frame relaying i frame switching.

Bezpośrednie wykorzystanie usług przenoszenia pozwala in. in. na integrację segmentów sieci LAN, zdalny dostęp do tej sieci, czy dostęp do sieci PSPDN.

Teleusługi są grupą usług o zunifikowanej formie, ingerującą w postać przesyłanych danych, zapewniającą dodatkowo sterowanie urządzeń końcowych. Teleusługi korzystają ze zbioru usług przenoszenia. Zestaw teleusług może być ciągle poszerzany, mogą one mieć charakter specjalistyczny, lub mogą być osiągane tylko przez określony krąg odbiorców.

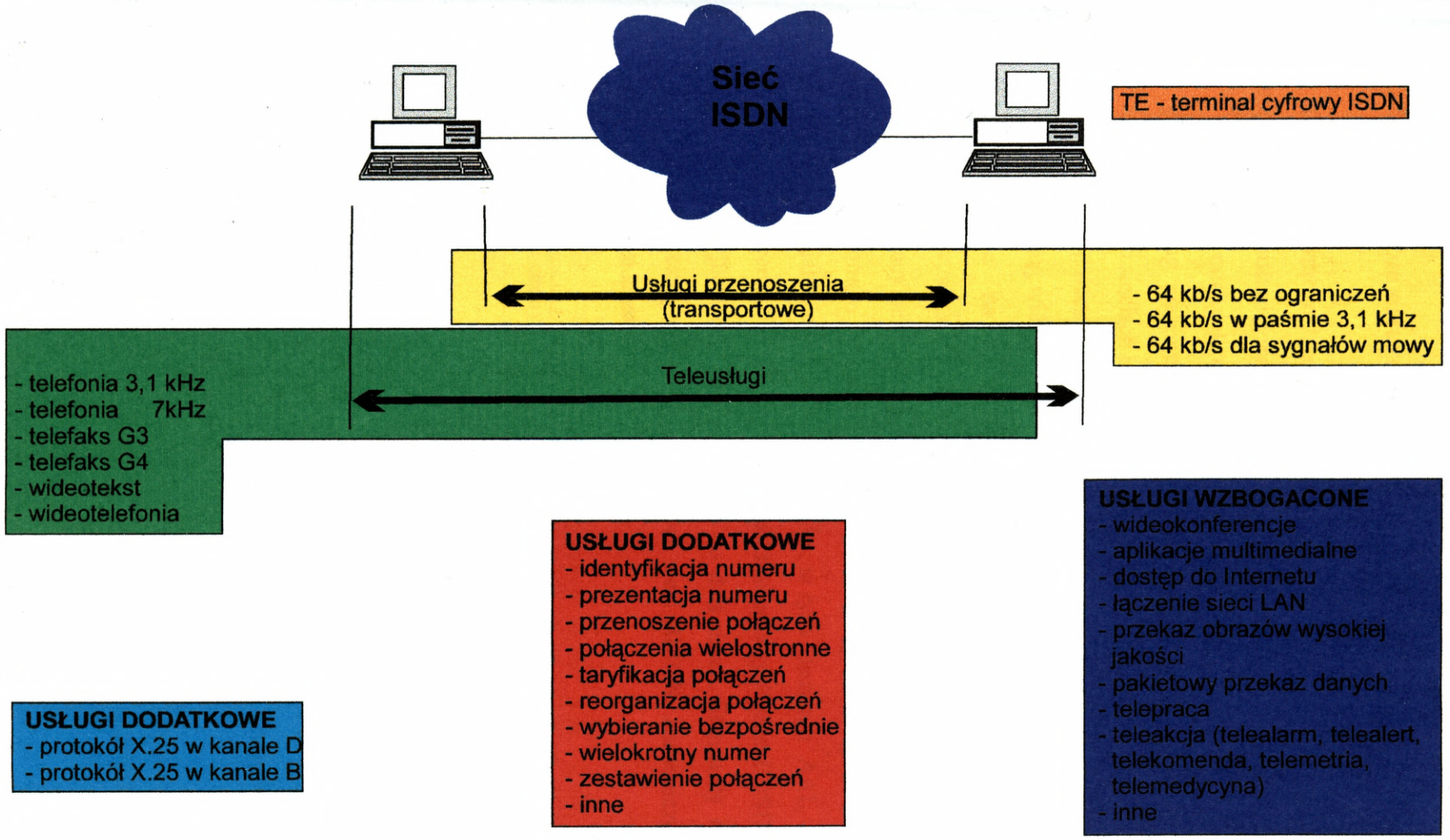
Usługi dodatkowe zwane udogodnieniami. Zwiększają funkcjonalność podstawowych usług telekomunikacyjnych. Zapewniają wygodę oraz łatwość sterowania przebiegiem łączenia.

Usługi dodane Jest to kategoria udogodnień realizowana w oparciu o istniejącą infrastrukturę sieciowo-transportową, np.:

- dostarczanie wiadomości /np. poczta elektroniczna (X.400), EFT/;
- wyszukiwanie informacji /np. bazy danych z serwisem informacji ekonomicznych/;
- uzupełnianie i redagowanie danych /np. wymiana formularzy elektronicznych/, konwersja protokołów;
- dostęp do sieci komutacji pakietów;
- cyfrowe łącza dzierżawione 2400, 4800, 9600, 56 000 b/s;
- cyfrowe łącza dzierżawione 1.544 Mb/s /dzierżawa krótko i długoterminowa/ itp.

Podział usług w zintegrowanej usługowo sieci cyfrowej został przedstawiony na rys 4.6

JAWNE
Zastrzeżone



Rys.4.6. Podział usług sieci ISDN.

JAWNE
Zastrzeżone

JAWNE

Zastrzeżone

4.4. Zintegrowane usługowo sieci szerokopasmowe B-ISDN

O potrzebie wprowadzenia systemu B-ISDN zadecydowały między innymi:

- popyt na nowe usługi generowany głównie przez duże centra finansowe , w tym :
  - potrzeba wymiany danych w układzie punkt-wiele punktów;
  - potrzeba usług niekomutowanych w połączeniach pomiędzy zasobami komputerowymi w prywatnych sieciach LAN;
  - przesyłania pakietów danych w sieci komutowanej;
  - potrzeba usług wielonośnikowych i przesyłania obrazów.
- zapotrzebowanie na łącza szerokopasmowe dla transmisji sygnałów wizyjnych i akustycznych wysokiej jakości;

Prace standaryzacyjne w zakresie sieci B-ISDN CCITT rozpoczęło na początku 1985 r. Zasadniczym przełomem było przyjęcie asynchronicznego trybu przesyłania informacji /system ATM/ i zasad podziału sieci na kilka poziomów, w tym poziomu AAL /Adaptation Layer/. Do 1990 r przyjęto zalecenia serii I dotyczące aspektów ogólnych sieci B-ISDN.

Prace standaryzacyjne trwają nieprzerwanie po dziś dzień. Standardy opracowane dotychczas umożliwiają praktyczną realizację konkretnych sieci BISDN. Zasadnicze różnice systemów N-ISDN i B-ISDN przedstawia tabela 4.2.

Tabela 4.2

Porównywane cechy	N-ISDN	B-ISDN
Dostęp użytkownika do sieci	Dostęp do kanałów o z góry określonej przepływności np.: 2B+D, 30B+D	Przepływność punktu styku „użytkownik-sieć" jest bardzo duża np.155 Mb/s, 622 Mb/s.
Media transmisyjne	Łącza jednotorowe oparte na wykorzystaniu symetrycznych kabli miedzianych	Wyłącznie kable światło-wodowe-
System komutacji	Komutacja kanałów, w sieci sygnalizacyjnej komutacja pakietów	Wyłącznie komutacja pakietów

JAWNE

Zastrzeżone

JAWNE

Zastrzeżone

Wybrane usługi w sieciach B-ISDN

- *usługi konwersacyjne*: wideotelefonia, wideotelekonferencja, przesyłanie informacji akustycznych i wizualnych, ultraszybka transmisja danych, transfer zbiorów baz danych, szybkie telesterowanie, szybkie przesyłanie danych telefaksowych, przesyłanie obrazów o dużej rozdzielczości, nadzór obszarów chronionych;
- *usługi komunikatowe:* poczta wizyjna, poczta sygnałów akustycznych, przesyłanie dokumentów;
- *usługi odszukiwania* /dokumentów wizyjnych, obrazów o dużej rozdzielczości, danych/;
- *usługi dystrybucji* sygnałów wizyjnych z udziałem i bez udziału użytkowników /w systemach PAL, SECAM, NTSC/, wideografia

Styki dostępu użytkownika UNI (User Network Interface) są standaryzowane dla dwóch częstotliwości: 155 Mb/s i 622 Mb/s.Współpraca podzespołów dostarczanych przez różnych producentów stała się wreszcie możliwa i prosta w realizacji. Znikła więc konieczność używania dodatkowych interfejsów, co przyśpieszyło budowę sieci i obniżyło koszty jej instalacji.

4.5. Telefonia komórkowa

Istnieją dwa systemy telefonii komórkowej: analogowy NMT (ang. Nordic Mobile Telephony) - standard skandynawski i cyfrowy GSM (ang. Global System for Mobile Communication). Nowością na polskim rynku jest system DCS, który pracuje na częstotliwości 1800 MHz. DCS opłaca się budować w większych miastach, gdzie jest duży ruch. Systemy komórkowe są alternatywą dla telefonii przewodowej (niestety znacznie droższą). Z "wojskowego punktu widzenia" systemy komórkowe (jak i inne systemy radiowe) nie zapewniają wystarczającej odporności na zakłócenia celowe. Spełniają one swą rolę jedynie podczas klęsk żywiołowych (przykładem może być ostatnia powódź).

W latach osiemdziesiątych powstały pierwsze systemy telefonii komórkowej pierwszej generacji (1G) oparte na technice analogowej - AMPS, NMT, TACS. Dla telefonii 1G zostały określone podstawowe cechy komunikacji: transmisja danych - 9,6 kb/s, transmisja mowy - kodowanie z przepływnością 13 kb/s, dostęp do kanału radiowego ze zwielokrotnieniem czasowym i ramką TDMA współpracujący z siecią pakietową publiczną - protokół X.25, przesyłaniem SMS-ów (krótkich wiadomości tekstowych) oraz realizacja połączeń alarmowych.

JAWNE

Zastrzeżone

W Polsce był to system NMT 450 wprowadzony przez Centertel w 1991r, system pracujący w częstotliwości 450 MHz z liczbą kanałów 200 pokrywający 95% powierzchni kraju. Systemy analogowe miały sporo wad - małą odporność na zakłócenia, łatwość podsłuchu rozmów, brak roamingu międzynarodowego i niedostateczna transmisja danych. Wymusiło to powstanie systemów komórkowych drugiej generacji (2G) popularnie zwanych GSM pracujących w technice cyfrowej. Pierwszy system GSM na świecie został oddany w 1991r, natomiast w Polsce system GSM 900 został wprowadzony w 1996r przez firmy PTC (Polska Telefonia Cyfrowa) w sieci Era Gsm oraz Polkomtel S.A. w sieci Gsm Plus. W 1998 r koncesję na GSM 1800 dostał trzeci polski operator Centertel - sieć Idea. Telefonia 2G w 1995r. otrzymała usprawnienia, tj. transmisja telefaksowa, interfejs komputerowy, usługi telekonferencyjne, czy identyfikacja abonenta za pomocą karty SIM. Następną fazą ewolucji systemów komórkowych jest faza 2,5G, będąca fazą przejściową pomiędzy drugą i trzecią generacją telefonii komórkowej. Telefonia 2,5G powstała w 1997r opiera się na dwóch szybszych technologiach transmisji: HSCSD (Hight Speed Circuit Swiched Data) do 115 kb/s i GPRS (General Packed Radio Service) do 170 kb/s. Transmisja danych HSCDSD umożliwia zwiększenie szybkości przekazu poprzez przydział kilku szczelin czasowych do jednego połączenia, każda o szybkości nominalnej 9,6 kb/s, Jedna transmisja może zajmować 7 szczelin (67,2 kb/s), a przy zastosowaniu kompresji przepływność zwiększa się do 115 kb/s. Natomiast transmisja pakietowa GPRS polega na powiązaniu i wspólnym sterowaniu kilku kanałów transmisyjnych w jeden tor komunikacyjny. Możliwe jest przyporządkowanie 8 szczelin czasowych w jednym kanale radiowym (76,5 kb/s), a przy zastosowaniu kompresji przepływność zwiększa się do 170 kb/s. Ostatnim krokiem ku telefonii 3G po wprowadzeniu transmisji GPRS jest etap transmisji EDGE (Enhansed Data GSM Evolution) umożliwiającą transmisję z przepływością 384 kb/s poprzez infrastrukturę GSM. Przez wiele lat systemy GSM będą funkcjonować równolegle z UMTS. W tabeli 4.3. przedstawione zostały podstawowe cechy generacji systemów komórkowych.

Najwięksi producenci urządzeń i telefonów komórkowych. Ericsson, Nokia, Motorola i Uniwired Planet podjęli inicjatywę opracowania jednolitej, uniwersalnej i ogólnie akceptowalnej w przyszłości aplikacji WAP (Wireless Application Protocol) przeznaczonej dla abonentów telefonii komórkowej. Uzgodniono wersję tego protokołu, która niewątpliwie uzyska z czasem rangę standardu współpracy prostych i najprostszych terminali bezprzewodowych z siecią Internetu. W specyfikacji zdefiniowano uniwersalne środowisko pracy WAE (Wireless Application Enviroment) dla istniejących i przyszłych aplikacji opartych na internetowym

JAWNE
Zastrzeżone

modelu typu klient-serwer, w postaci stron i skryptów udostępnianych przez serwery sieciowe WWW (WML) dla przeglądarek klienta. Istotnym elementem specyfikacji jest specjalny język opisu stron internetowych WML (Wireless Markup Language), wzorowany na dotychczasowych procedurach HTML i HTTP, a także protokole TCP/IP. Dzięki temu abonenci niespójnych systemów sieci komórkowych lub przywoławczych, używający dowolnego rodzaju terminali mobilnych (o niewielkich rozmiarach i różnorodnych ekranach), będą mieli dostęp do tych samych aplikacji i usług.

Aby to było możliwe, muszą się jeszcze powszechnie pojawić terminale działające zgodnie z protokołem WAP oraz operatorzy dostarczający specjalnych bram (gateway) internetowych WAP Proxy, łączących lokalne systemy komórkowe z siecią Internetu bądź intranetu. Ponadto w sieci komunikacyjnej muszą funkcjonować specjalizowane serwery WTA (Wireless Telephony Application), operujące w języku WML i przeznaczone do tworzenia usług internetowych dla prostych bezprzewodowych terminali końcowych

Pierwsze komercyjnie dostępne telefony komórkowe z protokołem WAP już były demonstrowane na wystawie w Cannes jako: OneTouch Pocket (Alcatel), Nokia 7110 (Nokia) i SGH-800 (Sagem). Chociaż mogą one działać z sieciami 2G (faza 2+), to korzystanie z dobrodziejstw wynikających z protokołu WAP będzie możliwe dopiero po wprowadzeniu szybszej pakietowej transmisji danych GPRS. Rosnąca liczba użytkowników oraz zwiększające się ich wymagania spowodowały konieczność rozpoczęcia pracy nad kolejnym etapem telekomunikacji przenośnej. Dlatego największe światowe organizacje takie jak Międzynarodowa Unia Telekomunikacyjna (ITU) a nawet Komisja Europejska, rozpoczęły prace nad nowym, ogólnoświatowym standardem. Założenia przygotowywane w ITU nazwano IMT-2000 (od międzynarodowej telefonii ruchomej - *international mobile telephony*).Prace, prowadzone od początku lat dziewięćdziesiątych przez ITU, nad standaryzacją przyszłego systemu komunikacji osobistej zakładały utworzenie jednolitego systemu lądowego (dla całego globu), nazywanego początkowo FPLMTS (Future Public Land Mobile Telecommunication System). Niezwykle szybki rozwój systemów satelitarnych spowodował rozszerzenie funkcji i zasięgu tego naziemnego systemu globalnego o segment satelitarny i rozwiązania techniczne łączące ziemskie systemy telefonii komórkowej z systemami satelitarnej łączności ruchomej.

Wspólny wysiłek wielu służb normalizujących, z uwzględnieniem różnych zastosowań systemu, zaowocował opracowaniem światowego standardu radiokomunikacyjnego oznaczonego IMT-2000 (International Mobile Telecommunications).

JAWNE
Zastrzeżone

Tabela 4.3.

GENERACJA I (1G):	GENERACJA II (2G):	GENERACJA III (3G):
- analogowe (AMPS,NMT,TACS) - transmisja danych 9,6 kb/s - SMS do 160 znaków	- cyfrowe GSM900,DCS1800 – usługi wąskopasmowe: głos,dane,SMS,VMS,faks - poczta głosowa VMS - -połączenia alarmowe - brak roamingu międzynarodowego	- cyfrowe globalne UMTS (IMT-2000) - zintegrowane usługi wąsko- i szerokopasmowe - transmisja danych EDGE 384kb/s, WCDMA 2Mb/s - usługi internetowe i multimedialne - transmisja danych HSCDSD 115kb/s, GPRS do 170kb/s – usługi dodatkowe – roaming międzynarodowy
1981 r.	1991 r.	2002 r. 2003r.

Podstawowe cechy generacji systemów komórkowych

Zakończenie długiego procesu normalizacji i zatwierdzenie standardu IMT-2000 przez ITU przewiduje się w najbliższym czasie. Ze względu na zbyt duże różnice występujące między infrastrukturą sieci eksploatowanych w poszczególnych częściach świata i różne zajętości pasm radiowych postanowiono, że systemy globalne będą funkcjonowały w kilku odmianach regionalnych (Europa, USA, Japonia, Chiny, Korea i in.), przy zachowaniu możliwie wielu wspólnych cech i wymagań ogólnych systemu IMT-2000 o wysokiej przepustowości, także podstawowych zakresów częstotliwości ustalonych przez ITU. Największe odstępstwa od standardu i związane z tym kłopoty, wynikające z wcześniejszego zagospodarowania podstawowych zakresów częstotliwości na inne potrzeby, będą widoczne na terenie amerykańskim. Europejską wersję tego uniwersalnego standardu o nazwie UMTS (Universal Mobile Telecommunications System) przedstawiła (1997 r.) organizacja normalizacyjna ETSI. Zawarto w niej większość propozycji systemu IMT-2000 w prawie nie zmienionej postaci, chociaż modyfikacje dotyczą nie tylko pasm częstotliwości. Projekt stanowi de facto konwergencję wielu dotychczas działających sieci, przez modernizację istniejących systemów naziemnych (dyspozytorskich, komórkowych, przywoławczych), z systemami satelitarnymi. W rezultacie indywidualny abonent ruchomy otrzymuje nową jakość usług multimedialnych o przepływności od 64 kb/s do 384 kb/s, rozszerzanych w środowisku lokalnym do 2 Mb/s.

Zgodnie z ustalonym przebiegiem prac standaryzacyjnych w wymaganiach na sieć osobistą trzeciej generacji IMT-2000, (zaproponowanych w rok 1999), określono ostatecznie trzy projekty interfejsów radiowych dla systemów 3G obejmujące rozwiązania:

- interfejs radiowy według nowego standardu UTRA (UMTS Terrestial Radio Access), rekomendowany przez ETSI dla europejskich systemów UMTS,
- interfejs radiowy CDMA 2000, stanowiący rozwinięcie dotychczasowego standardu IS-95 według TIA (Telecommunications Industry Association), z przeznaczeniem do stosowania w USA,
- interfejs radiowy UWCC-136, będący ewolucyjnym rozszerzeniem istniejącego standardu IS-136, rekomendowany przez UWCC (Universal Wireless Communications Consortium) na terenie USA.

Interfejs UTRA. Większość przedstawionych propozycji interfejsu radiowego, włącznie z europejskim UMTS opiera się na technice WCDMA (Wideband Code Division Multiple Access), a więc szerokopasmowym rozpraszaniu widma za pomocą ciągu kodowego. Oryginalną koncepcją interfejsu radiowego UTRA (UMTS Terrestial Radio Access) jest działanie w dwóch

JAWNE

Zastrzeżone

trybach pracy dupleksowej: FDD (Frequency Division Duplex) i TDD (Time Division Duplex). Te i inne przyjęte rozwiązania dają elastyczność w konfigurowaniu kanału transmisyjnego, możliwość równoległej transmisji o zmiennej szybkości w kilku kanałach, stosowanie efektywnej transmisji pakietowej, łatwe przenoszenie do innych systemów, ze szczególnym uwzględnieniem sieci GSM. Mają one również na celu: zaoferowanie optymalnego bilansu energetycznego dla obydwu kierunków transmisji (anteny adaptacyjne), lepsze wykorzystanie dostępnego widma i łatwe wdrażanie przekazów. Parametry interfejsu radiowego WCDMA i sieci szkieletowej pozwalają na wykorzystanie dotychczasowych zasobów sieci GSM, budowę terminali uniwersalnych GSM/UMTS oraz ewolucyjny rozwój systemów komunikacji osobistej UMTS.

Zgodnie ze światowymi tendencjami konwergencji teleinformatyki za pomocą systemu UMTS można będzie konsekwentnie ujednolicić globalną infrastrukturę telekomunikacyjną przez: integrację wielu sieci i usług, personalizację dostępu do sieci, rozszerzenie dostępu do usług szerokopasmowych i rozpowszechnianie technik dostępu bezprzewodowego. System UMTS został zdefiniowany jako standard otwarty dla systemów mobilnych o dużej szybkości transmisji, zarówno dla systemów naziemnych, jak i satelitarnych. Ma on zapewnić międzynarodowy roaming sieciowy za pomocą uniwersalnego terminala osobistego 3G, dostęp do wszystkich istniejących usług internetowych wraz z ofertą nowych usług szerokopasmowych. System ma umożliwiać transmisję wąskopasmową i szerokopasmową z dostępem lokalnym do 2 Mb/s i globalnym bez ograniczenia odległości (z maks. przepływnością do 384 kb/s).

Stosunkowo krótkie terminy realizacji poszczególnych regionalnych systemów szerokopasmowych wynikają z ich podobieństwa do technologii stosowanych w środowisku GSM i stanowią niejako ewolucję tych sieci w kierunku szerszego pasma transmisji 3G.

Terminale i usługi szerokopasmowe 3G. Zakres nowych usług dostępnych w systemie UMTS jest duży, co jest związane z możliwością dostępu do szerokiego pasma głównie z ofertą usług multimedialnych przedstawia tabela. 4.4. System UMTS jest bowiem optymalizowany nie pod kątem transmisji mowy, lecz globalnych i zróżnicowanych przekazów multimedialnych.

Stanowi to zasadniczą różnicę w ofercie usług między systemami cyfrowymi dotychczasowej generacji (2G) i systemami trzeciej generacji 3G. Docelowo usługi 3G będą dostępne za pomocą jednego (fizycznie) wspólnego terminalu działającego w różnych środowiskach sieciowych, zarówno wewnątrz pomieszczeń (na wzór terminali systemu DECT), jak i na zewnątrz budynków, także w pojazdach.

JAWNE

Zastrzeżone

JAWNE

Zastrzeżone

Tabela 4.4.

Transmisja fonii	3 – 32
Transmisja danych	2,4 – 64
Dźwięk wysokiej jakości	64
Wideokonferencje	64-384
Wiadomości SMS	1,2-9,6
Usługi na odległość	1,2-9,6
Lokalizacja pozycji i nawigacja	64
Telefax	64
Telezakupy	2,4-768
Gazeta elektroniczna	2,4-2000
Dostęp do danych, internetu	2,4-768

Przepływność dla poszczególnych usług [kb/s]

Terminale i telefony 3G nie są jednak wcale standaryzowane, co oznacza, że można oczekiwać bardzo zróżnicowanych terminali wideofonicznych, nie tylko pod względem oferowanych funkcji, ale i ich ergonomii. Dalsza ich przyszłość wiąże się przede wszystkim z rozwojem kamer cyfrowych, modernizacją systemów rozpoznawania obrazów oraz ciągłej miniaturyzacji komunikatorów PDA, pozycjonerów GPS, laptopów i browserów internetowych.

Zgodnie z przyjętymi założeniami systemy trzeciej generacji mają cechy sieci globalnej i uniwersalnej. Globalny charakter sieci UMTS oznacza, że abonent tego systemu ma ciągłość oferowanych mu usług telekomunikacyjnych, czyli taki sam zestaw usług, personalizację, numerację, identyfikację, a także przenoszenie połączeń (roaming) między operatorami, przełączanie kanałów (handover) i wiele innych funkcji, niezależnie od tego, gdzie się znajduje i który typ sieci jest jego bazą macierzystą. Z kolei uniwersalność sieci 3G polega na integracji usług komórkowych z innymi usługami, do tej pory identyfikowanymi z sieciami innego typu (stacjonarne, przywoławcze, dyspozytorskie).

Rozwiązaniem idealnym jest pełny zakres oferowanych usług, dostępny wszędzie i w każdej sytuacji. O szybkości dochodzenia do takiego stanu zadecydują głównie potrzeby,

JAWNE Zastrzeżone

gdyż wydaje się, że poszczególne elementy technologii takiego przekazu znajdują się w końcowej fazie realizacji.

Zwłaszcza że świadczenie usług multimedialnych za pomocą wideoterminali przenośnych będzie nadal motorem napędowym, przyspieszającym realizację systemu globalnego - wideoterminali przyszłości, łączących klasyczne funkcje telefonu komórkowego z wieloma użytecznymi funkcjami domowymi (dźwięk, dane, multimedia, film i zdalne sterowanie obiektami) oraz realizację nowych, jeszcze nie do końca (lub wcale) zdefiniowanych funkcji usługowych.

Wprowadzenie IMT-2000 ma spowodować, ze przyszłe sieci łączności bezprzewodowej zapewnią tę samą jakość połączeń, pasmo i szybkość transmisji, jak nowoczesne sieci przewodowe. Wymaga to stworzenia zbioru norm i wymagań technicznych, które powinny nadać kierunek rozwojowi techniki, sieci i usług telekomunikacji ruchomej, a także zapewnić współdziałanie z przewodową infrastrukturą sieci telefonicznych i sieci komputerowych. Ponieważ jednak do ogólnoświatowego systemu będziemy dochodzić przez ewolucję już działających sieci i systemów to założenia IMT-200 zgodnie z wymaganiami ITU, mają stać się podstawą dalszych prac nad systemami regionalnymi.

4.6. Transmisja danych

Ważną dziedziną usług telekomunikacyjnych jest transmisja danych. Usługi transmisji danych oferowano w sieciach POLPAK, POLPAK-T, KOLPAK, TELBANK, PKONET czy NASK (Naukowa Akademicka Sieć Komputerowa). Dla przykładu podano krótki opis sieci POLPAK -T(operator TP S.A.) i sieci komputerowej TELBANK S.A.

Sieć POLPAK-T

Sieć POLPAK-T jest szybką siecią szkieletową służącą dla potrzeb transmisji pomiędzy użytkownikami wymagającymi bardzo dużych prędkości. W pierwszej fazie będzie to sieć bazująca na protokole Frame Relay z docelową możliwością rozbudowy dla transmisji w trybie ATM.

Za pomocą sieci POLPAK-T realizowany jest dostęp do INTERNETU (TPNET - podłączenie za pomocą łącza dzierżawionego lub dostępu komutowanego).

Sieć szkieletowa POLPAK-T składa się z 15-tu sieci MAN co pokrywa równomiernie obszar Polski. Węzły sieci (175 w całym kraju) znajdują się we wszystkich większych miastach,

JAWNE
Zastrzeżone

w tym każdym wojewódzkim. Porty sieci POLPAK-T mogą pracować z prędkością transmisji od 64 do 2048 kb/s. Oprócz tego każdy węzeł wyposażony jest w porty dla połączeń międzywęzłowych z interfejsem G 703 w liczbie od 4 do 8 sztuk w zależności od ilości połączeń do innych węzłów. W oparciu o sieć POLPAK-T w 16 województwach jest możliwy dostęp PSTN (4.500 tys. modemów) do Internetu (protokół PPP). Prędkość transmisji na modemach to 28.8 kb/s lub 33.6 kb/s a już wkrótce 56kb/s.

Bankowe Przedsiębiorstwo Telekomunikacyjne "TELBANK" S.A.

"TELBANK" S.A. jest to spółka akcyjna polskich banków, działająca na rynku telekomunikacyjnym od września 1992 roku. BPT "TELBANK" S.A. jest operatorem telekomunikacyjnym działającym na obszarze Rzeczypospolitej Polskiej zgodnie z zezwoleniem ministra łączności (Sieć BPT przedstawiono na rys .4.7.).

Zakres działania BPT obejmuje świadczenie usług telekomunikacyjnych oraz usługi w zakresie zakładania, używania i utrzymania sieci oraz systemów telekomunikacyjnych, a także sprzedaży urządzeń i systemów telekomunikacyjnych. Świadczone przez BPT usługi telekomunikacyjne obejmują: usługi transmisji danych, usługi z wartością dodaną, usługi ISDN, dzierżawę kanałów i urządzeń telekomunikacyjnych, które są oferowane w sieci telekomunikacyjnej użytku publicznego (dla wszystkich zainteresowanych klientów) oraz usługi telefoniczne w wydzielonej sieci telekomunikacyjnej (dla banków i administracji państwowej).

Charakterystyczną cechą sposobu działania BPT jest dostosowywanie usług do potrzeb klientów oraz oferowanie im rozwiązań na najwyższym, światowym poziomie. Sieć TELBANK (stanowiąca zbiór zintegrowanych ze sobą sieci telekomunikacyjnych administrowanych przez BPT), jest przeznaczona dla szerokiego kręgu klientów, bez względu na ich wyposażenie techniczne i położenie geograficzne.

Sieć TELBANK zapewnia niezawodną łączność na terenie całej Polski oraz dostęp do sieci międzynarodowej. BPT "TELBANK" S.A. oferuje standardowe usługi telekomunikacyjne, ale na dużo wyższym od standardowego poziomie:

- cyfrowe kanały transmisyjne - sieć TELBANK-M (w relacjach międzymiastowych);
- sieci miejscowe;
- połączenia telefoniczne;
- teleinformatyczne oraz usługi multimedialne - sieć TELBANK-T;
- połączenia teleinformatyczne krajowe i międzynarodowe w sieci pakietowej - sieć TELBANK-P;

JAWNE
Zastrzeżone

Sieć TELBANK obejmuje:

sieć międzymiastowych kanałów stałych
TELBANK - M

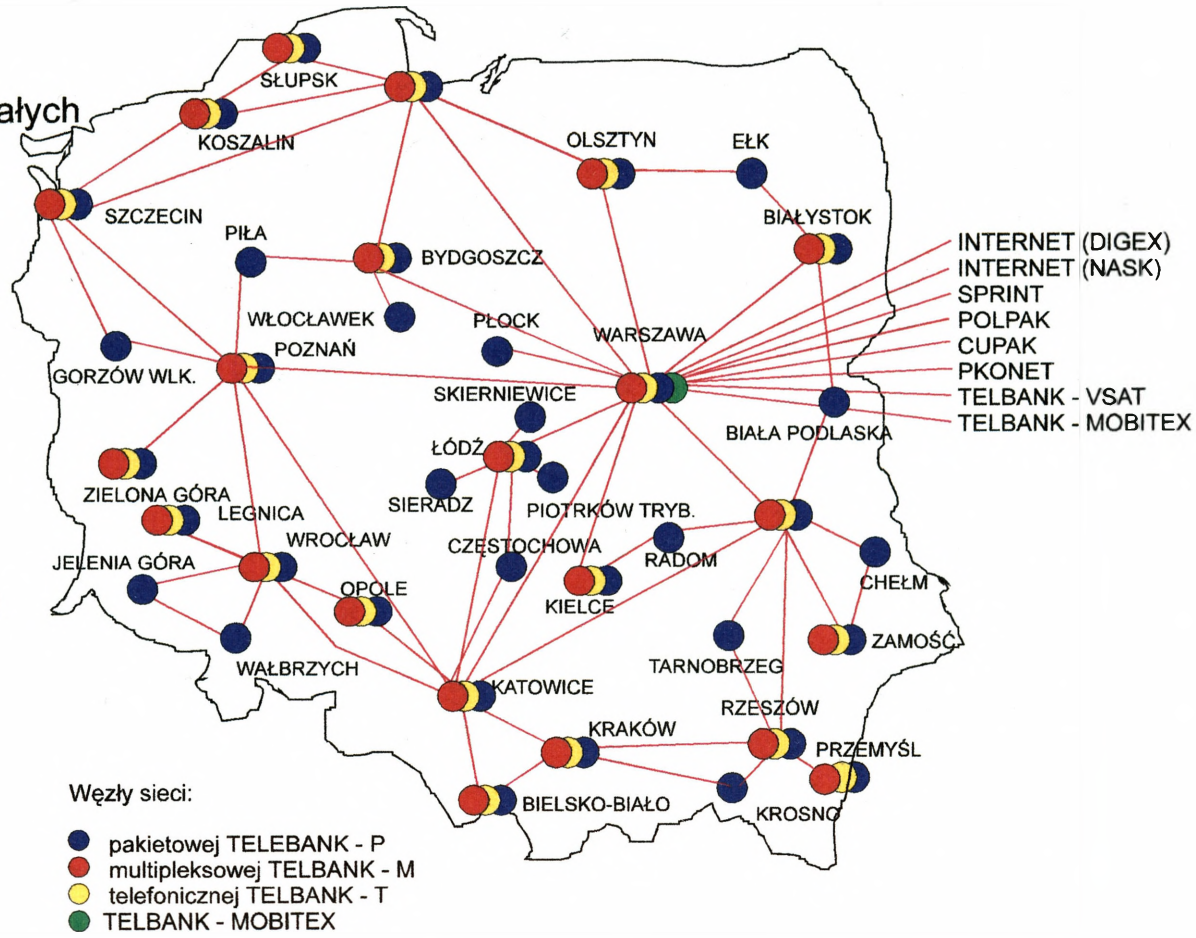
sieć pakietową
TELBANK - P

sieć telefoniczną o cechach ISDN
TELEBANK - T

sieć satelitarną
TELBANK - VSAT

system ruchomej transmisji danych MOBITEX
TELBANK - R

sieć Internetową
BPTNet



Rys.4.7. Schemat sieci TELBANK (wariant)

JAWNE

Zastrzeżone

JAWNE
Zastrzeżone

- połączenia teleinformatyczne w sieci satelitarnej VSAT - sieć TELBANK-VSAT;
- połączenia teleinformatyczne krajowe FRAME RELAY - sieć TELBANK-M;
- pocztę elektroniczną w standardzie X.400/X.500 - system TELBANK400;
- dostęp do sieci INTERNET - sieć BPTNet;
- połączenia teleinformatyczne w radiowym, ruchomym systemie transmisji danych - sieć TELBANK-R (MOBITEX);
- szkolenia i testy akceptacyjne;;
- dostęp do sieci rozliczeń międzybankowych Krajowej Izby Rozliczeniowej (KIR) i SWIFT (ogólnoświatowa sieć rozliczeń międzybankowych);
- usługi konsultingowe w zakresie tworzenia i projektowania sieci lokalnych i rozległych,
- realizację projektów w zakresie wdrażania oraz integracji systemów i usług.

INTERNET

INTERNET jest obecnie największą na świecie siecią TD. Jej protoplastą była sieć ARPANET łącząca liczne ośrodki wojskowe, przemysłowe i uniwersyteckie w USA. Wkrótce sieć, z uwagi na jej zalety, rozszerzyła się na cały świat[23]. Stworzono olbrzymią ilość, specjalnie dla niej stworzonego, oprogramowania, w tym aplikacje stosowane w sieciach rozległych, umożliwiające zdalną pracę na komputerach dużej mocy, dostęp do różnorodnych baz danych, transmitowania plików oraz aplikacje stosowane głównie w sieciach lokalnych (np. sieciowy system plików NFS). Dotychczas najbardziej popularną usługą jest WWW (World Wide Web). Sieć INTERNET funkcjonuje w oparciu o pakiet protokołów TCP/IP (transmisja datagramowa – bezpołączeniowa). Filozofia TCP/IP jest antytezą filozofii ISO/OSI RM[24] (model referencyjny OSI), lecz ze względu na swoją popularność TCP/IP stanowi praktycznie podstawę wszystkich sieci działających w oparciu o system operacyjny UNIX

. W TCP/IP protokoły są bardzo proste i gdy pojawia się konieczność rozbudowy sieci dodawane są nowe protokoły[25]. Najważniejsze protokoły TCP/IP obejmują: IP- Internet Protocol, ICMP – Internet Control Message Protocol, UDP – User Datagram Protocol, TCP – Transmission Control Protocol. Inne protokoły poszerzające możliwości sieci to: SMTP – wersja poczty elektronicznej na bazie TCP/IP, Telnet – umożliwiający tworzenie

---

23 - Popularność sieci INTERNET porównuje się do powszechności systemu operacyjnego MS DOS.

24 - model referencyjny ISO/OSO posiada 7 warstw, natomiast TCP/IP – 4 warstwy. Model OSI powstał na zapotrzebowanie telekomunikacji i zdaniem specjalistów jest pod wieloma względami lepszy, natomiast TCP/IP z uwagi na INTERNET – coraz popularniejszy.

25 - w odróżnieniu, w ISO rozbudowa funkcjonalności sieci polega na poszerzeniu protokołów.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

wirtualnegoterminala sieciowego, FTP (File Transfer Protocol) – umożliwiający korzystanie z zasobów sieci.

Aktualnie wykorzystywany w INTERNECIE zestaw protokołów TCP/IP nie nadaje się do transportu strumieni danych multimedialnych. W standardowym protokole IP wyróżnia się dwa rodzaje pakietów: „unicast" (adresowanych do jednego ściśle określonego odbiorcy) i „broadcast" (docierające do wszystkich komputerów w obrębie jednej sieci lokalnej). Z chwilą, gdy pojawiło się zapotrzebowanie na usługi przesyłania dźwięku i obrazu w INTERNECIE pojawiła się również potrzeba przesyłania pakietów multicasingowych. O ile już w protokole IP stworzonym na początku lat 70-tych dopuszczano adresacje multicastową, to istniejące aplikacje, jak również stosowane routery pozwalały na jej stosowanie tylko w obrębie sieci lokalnych (lub wykorzystując pakowanie jej w zwykłe pakiety tworzenie w sieci rozległej „wysp multicastowych"). Sieć INTERNET jest ciągle rozwijana. Jej możliwości gwarantują wysoką pozycję wśród sieci dostępowych z integracją usług i powodują, że może stanowić poważną konkurencję dla innych rozwiązań. Można stwierdzić, że cechą, która będzie stanowić o daiszej popularności INTRNETU w przyszłości, będzie dostępność w niej usług multimedialnych (np. radio, telefon, telewizja rozsiewcza, wideokonferencja itp.). W INTERNECIE wykorzystywane są trzy grupy oprogramowania umożliwiające przekazywanie dźwięku oraz video: oprogramowanie telekonferencyjne umożliwiające przekazywanie dźwięku i obrazu równocześnie pomiędzy wieloma użytkownikami sieci. Aktualnie niepisany standard tworzą dźwięku zbliżona jest do jakości sygnałów radiowych zakresu fal AM (pasmo 4 kHz) oraz dwie aplikacje multicastingowe korzystające z protokołu RTP: VAT - Visual Audio Tool. (Przesyłane sygnały podlegają procesom kompresji i dekompresji. Jakość przesyłanego NV - Network Video. Typowa szybkość transmisji 128 kb/s umożliwia przesyłanie 3 do 5 klatek/sekundę obrazu zakodowanego w systemie PAL (384x240 pikseli), lub NTSC (320x240 pikseli). Program umożliwia przesyłanie obrazów z maksymalną szybkością do 30 klatek/sekundę (przy wymaganej przepustowości rzedu 1,5 Mb/s). Program umożliwia również przesyłanie dowolnych okien X-Windows. Do transmisji Video używane są również inne programy np.: IVS (INRIA Videoconferencing System) – niekompatybilny z NV oraz VIC (obsługujący obydwa formaty NV i IVS). Wyżej wymienione aplikacje z uwagi na to, że są rozwijane głównie dla różnych wersji systemu UNIX, nie zdobyły wielkiej popularności w środowisku użytkowników komercyjnych (korzystających z systemu MS-DOS. Dla tych użytkowników zostały opracowane aplikacje (nie pracujące jednak pod systemem UNIX):

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

- RealAudio – służący do transmisji dźwiękowych oraz StreamWorks – umożliwiający przekaz dźwięku i obrazu (również wykorzystuje się metody kompresji sygnałów),
- oprogramowanie transmisyjne, w którym przekaz odbywa się w jednym kierunku od nadawcy do odbiorców (podobnie jak w radio, czy telewizji),
- oprogramowanie typu „telefon przez INTERNET" zapewniające dwukierunkową komunikację dźwiękową pomiędzy parą użytkowników sieci.

Obecnie rozwijana jest nowa wersja sieci INTERNET – tzw. INTERNET-II w którym wykorzystuje się łącza międzywęzłowe o bardzo dużych przepustowościach (rzędu 2 Gb/s). Zakłada się, że będzie on stanowił poważną konkurencję dla tradycyjnych zintegrowanych sieci szerokopasmowych i może spowodować rewolucję w dalszych kierunkach rozwoju światowej telekomunikacji.

4.7. Systemy komutacyjne

Systemy komutacyjne można klasyfikować na wiele ***sposobów*** np.: ze względu na następujące kryteria wyróżniające:

A. Kryterium rozwiązań technicznych i stosowanych technologii. Z uwagi na to kryterium wyróżnia się :

1. systemy komutacji ręcznej;
2. systemy komutacji półautomatycznej;
3. systemy komutacji automatycznej wykorzystujące:

- elektromechaniczne /np. biegowe/
- centrale elektromechaniczne ze sterowaniem elektronicznym /np. centrale krzyżowe/
- centrale quasielektroniczne /np. ESM - SIEMENS/
- centrale centrale elektroniczne /np. E-10 /
- centrale optoelektroniczne.

Systemy wymienione w punkcie 3 są znane i stosowane w sieciach telekomunikacyjnych na świecie, jak również w Polsce. Na uwagę zasługują centrale optoelektroniczne.

B. Kryterium ***metody*** komutacji informacji w węzłach komutacyjnych. Z uwagi na to kryterium wyróżnia się pięć podstawowych metod komutacji:

- komutacja kanałów /łączy/
- komutacja wiadomości
- komutacja pakietów
- komutacja hybrydowa
- komutacja blokowa

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Komutacja kanałów (KK) polega na tworzeniu, na żądanie, pomiędzy dwiema lub więcej stacjami końcowymi drogi połączeniowej do ich wyłącznego użytku aż do chwili rozłączenia. Połączenie jest tworzone przez zajmowanie kolejnych odcinków drogi połączeniowej /tj. kanałów/ na trasie między węzłami sieci telekomunikacyjnej znajdującymi się pomiędzy tymi stacjami. Zajmowanie drogi odbywa się zgodnie z informacjami sygnalizacyjnymi wysyłanymi przez stację inicjującą połączenie i ewentualnie uzupełnianymi dodatkowymi informacjami przez węzły sieci. Po zestawieniu połączenia droga dla informacji jest na ogół "przeźroczysta". Ta metoda komutacji jest powszechnie stosowana w sieciach telefonicznych typu PSTN, IDN, ISDN /w zastosowaniach powszechnych i wojskowych/. W systemach cyfrowych PCM komutacja kanałów jest konsekwencją techniczną synchronicznej transmisji informacji (informacja jest przesyłana i komutowana w postaci "sztywnej" struktury - ramki) oraz koniecznością kompatybilnej współpracy z systemami analogowymi. Konsekwencją natłoku w sieci z komutacją kanałów są straty ruchu (odrzucanie żądań obsługi). Wady i zalety komutacji kanałów przedstawiono w tabeli 4.5.

Tabela 4.5.

Podstawowe wady systemu KK	Podstawowe zalety systemu KK
-słabe wykorzystywanie zasobów systemu telekomunikacyjnego (kanał jest zajęty także w okresie "ciszy"). Wadę tę częściowo można eliminować stosując system TASI (Time Assignment Speech Interpolation) umożliwiający wykorzystanie przerw pomiędzy sygnałami mowy do przesyłania innych sygnałów (np. sygnałów mowy innych połączeń, lub trans misji danych)	-małe i stałe opóźnienia informacji przesyłanych pomiędzy stacjami końcowymi oraz ich nadchodzenie w kolejności w jakiej zostały wysłane
-stosunkowo długie czasy zestawiania połączeń Wada redukowana w nowoczesnych systemach KK poprzez realizację tzw. "szybkiej komutacji kanałów".	

Komutacja wiadomości (KW) polega na tym, że informacje /o różnych długościach/ są przesyłane pomiędzy stacjami końcowymi w postaci wiadomości zawierających adres stacji docelowej /mogą być magazynowane w węzłach sieci/. Komutacja wiadomości jest najbardziej typowym przykładem metody "zapamiętaj i prześlij". Jest szczególnie przydatna do organizacji systemów dystrybucji wiadomości MHS /Message Handling Systems/. Na bazie komutacji wiadomości może być organizowana np. poczta elektroniczna (e-maill) oraz współpraca służb teleksowych i teletekstowych.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Komutacja wiadomości znajduje zastosowanie w sieciach teleinformatycznych "cywilnych" oraz wojskowych.W systemach wykorzystujących komutację wiadomości zachodzi na ogół konieczność dodatkowej strukturyzacji informacji dla celów transmisyjnych. Wady i zalety komutacji wiadomości przedstawiono w tabeli 4.6.

Tabela 4.6.

Podstawowe wady systemu KW	Podstawowe zalety systemu KW
-większe wykorzystanie kanałów. Kanały są zajmowane tylko w czasie rzeczywistego przesyłania wiadomości	-przesyłanie informacji w czasie nierzeczywistym. -większe i nierównomierne opóźnienia.

Komutacja pakietów_(KP) jest również przykładem metody "zapamiętaj i prześlij". W odróżnieniu od komutacji wiadomości, w systemach z komutacją pakietów informacja jest wymieniana pomiędzy stacjami końcowymi w postaci grup elementów binarnych o ograniczonej długości zwanych pakietami. Długie wiadomości są przed przesłaniem ich w sieci dzielone na pakiety, a następnie odtwarzane (zestawiane) w stacji końcowej. Pakiety mają ściśle określoną strukturę obejmującą: nagłówek zawierający adres i informacje sterujące, część wiadomości oraz informacje zabezpieczające przed błędami.

Systemy komutacji pakietów są sprawdzonym rozwiązaniem w zastosowaniu do teleinformatyki i na jej bazie budowane są współczesne publiczne sieci pakietowe (np. krajowa sieć POLPAK), sieci dedykowane tj. przeznaczone dla potrzeb określonych grup użytkowników (np. sieci krajowe TELBANK, KOLPAK, NASK itp.) oraz wojskowe (np. planowana do rozwinięcia w ubiegłym dziesięcioleciu sieć powiadamiania i alarmowania WP- FUNKIA, sieci dla potrzeb rodzajów wojsk i służb (dla potrzeb logistyki) oraz sieci kierowania systemami i środkami walki. Konsekwencją natłoku w sieci z komutacją pakietów jest wydłużenie kolejek pakietów czekających na obsługę i wynikające stąd opóźnienia w dostarczaniu pakietów do odbiorcy.

Do współpracy sieci pakietowych z sieciami o innych technikach komutacji na styku "węzeł-węzeł" stosowane są urządzenia pośredniczące - konwertery międzysieciowe, których funkcja polega na wzajemnym dopasowywaniu różnych kodów, szybkości transmisji oraz protokołów komunikacyjnych. Wady i zalety komutacji pakietów przedstawiono w tabeli 4.7.

JAWNE
Zastrzeżone

Tabela 4.7.

Podstawowe wady systemu KP	Podstawowe zalety systemu KP
-kanał jest zajmowany tylko na czas przesyłania informacji; -podział wiadomości na pakiety umożliwia zmniejszenie pojemności pamięci (buforów) w węzłach sieci; -system pozwala zwiększyć przepustowość sieci;	-zmienne opóźnienia poszczególnych pakietów powodujące konieczność przetwarzania przez węzły dużych ilości informacji.

Komutacja hybrydowa (KH) polega na połączeniu zalet komutacji kanałów i pakietów /wiadomości/. Część szczelin wspólnej ramki czasowej przeznacza się dla komutacji kanałów, pozostałą dla wymiany danych (stosuje się komutację pakietów, lub wiadomości). Podział ramki może być stały, lub zmienny, zależnie od konkretnej realizacji technicznej. Komutacja we wspólnej centrali odbywa się oddzielnie dla poszczególnych części ramki. Komutacja hybrydowa jest powszechnie stosowana w systemach IDN i ISDN wykorzystujących system sygnalizacji ITU SS7, gdzie w procesie przekazywania informacji użytkowych jest stosowana komutacja kanałów, natomiast informacje sygnalizacyjne są przekazywane w postaci depesz (komutacja pakietów). Komutacja hybrydowa znalazła dość szerokie zastosowanie w łącznicach cyfrowych z modulacją delta wykorzystywanych we współczesnych militarnych systemach łączności (wykorzystujących wydzielony system sygnalizacji).

Komutacja blokowa polega na tworzeniu połączenia na czas, w którym przesyłany jest sygnał niosący informację użyteczną w paczce zwanej "blokiem". Blok jest transmitowany wraz z nagłówkiem sygnalizacyjnym, podobnie jak w komutacji pakietów, przy czym nie jest on buforowany w węzłach sieci (co przypomina komutację kanałów). Komutacja blokowa łączy zalety komutacji kanałów (stałe opóźnienie sygnałów) oraz komutacji pakietów (efektywniejsze wykorzystywanie kanałów łączności).Podstawową wadą komutacji blokowej jest konieczność stosowania zaawansowanych technik i technologii.

4.8. Technologie w sieciach teleinformatycznych

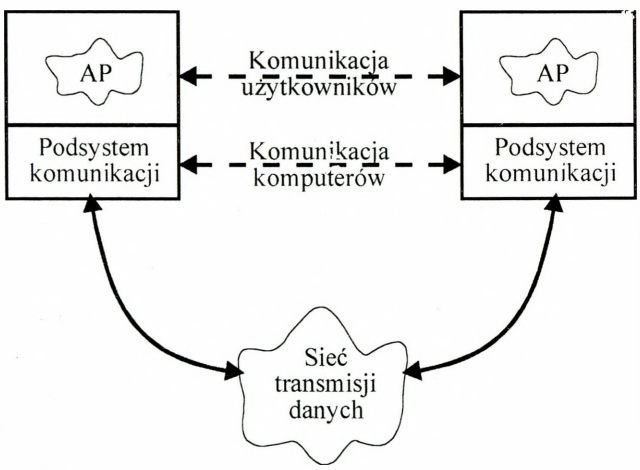
Komputery coraz szerzej wykorzystywane są w życiu zawodowym a po upowszechnieniu szerokopasmowych sieci dostępowych znajdą z pewnością zastosowanie również w życiu prywatnym. Największe możliwości wykorzystania zalet komputerów dają

sieci komputerowe (LAN – Local Area Network, MAN – Metropolitan Area Network, WAN – Wide Area Network). Sieci te umożliwiają ich użytkownikom współdzielenie rozmaitych zasobów, takich jak:

- moce obliczeniowe komputerów mainframe[26];
- drukarki, plotery, pamięci dyskowe/taśmowe.
- aplikacje[27], pliki, bazy danych posadowione na odpowiednich serwerach;

Sieci komputerowe mogą być zbudowane w różny sposób, ale zawsze w ich architekturze można wyróżnić trzy podstawowe, hierarchicznie uporządkowane elementy (Rys. 4.8):

- podsystem przetwarzania danych, dla komunikacji pomiędzy użytkownikami:
- podsystem komunikacji pomiędzy komputerami dołączonymi do sieci;
- sieć transmisji danych.



Rys. 4.8. Podstawowe elementy sieci komputerowych

Podsystem komunikacji komputerów oraz podsystem komunikacji aplikacji tworzą bardzo złożone oprogramowanie, początkowo pisane w językach symbolicznych, bez wyróżnionych struktur. Wzorując się na powstającym programowaniu strukturalnym ISO[28] zaproponowało , aby w/w oprogramowanie było tworzone w postaci niezależnych warstw współpracujących ze sobą w ograniczony sposób. W ten sposób powstał model odniesienia (model referencyjny) dla otwartych (heterogenicznych) systemów komputerowych ISO/OSI[29]. Pełna jego nazwa brzmi ISO Reference Model for Open System Interconnection.

---

26 - są to duże systemy komputerowe instalowane w specjalnie przeznaczonych klimatyzowanych pomieszczeniach, obejmujące pełny krąg zastosowań. Przykładami komputerów mainframe są IBM 360, IBM 370, seria 43xx, System 3080, 3090 itp.

27 - Liczba dostępnych aplikacji rośnie w sposób gwałtowny i ze względu na rosnące koszty z pewnością nie wszyscy użytkownicy będą je kupować.

28 - International Organization for Standarization – międzynarodowa organizacja standaryzacyjna.

Z koncepcyjnego punktu widzenia omawiane oprogramowanie pełni funkcje komunikacyjne (zorientowane sieciowo) oraz funkcje przetwarzania danych (zorientowane na aplikacje).Funkcje każdej warstwy są formalnie określone za pomocą odpowiedniego protokołu, który definiuje reguły wymiany wiadomości pomiędzy równoprawnymi jednostkami należącymi do danej warstwy. Każda warstwa dostarcza dla warstwy wyższej określonych usług, które są realizowane z wykorzystaniem usług dostarczanych przez warstwę bezpośrednio niższą.Funkcje realizowane w poszczególnych warstwach modelu przedstawia rys. 4.9.

Rys. 4.9. Funkcje realizowane przez warstwy modelu OSO/ISO

Topologie sieci LAN. Istnieją trzy podstawowe topologie, występujące również w różnych odmianach:

- topologia gwiazdy,
- topologia pierścienia,
- topologia magistrali liniowej,

w oparciu o które mogą być realizowane topologie hybrydowe np. pierścieniowo-gwiaździsta topologia drzewa itp.

29 - OSI – Open System Interconnection.

JAWNE
Zastrzeżone

Protokoły. Protokoły stosowane w sieciach LAN są opracowywane i wdrażane przez ITU (np.: X.25, X.400, X.500, X.29), ISO (np.: OSI), IEEE (np.. Project 802). Projekt 802 dotyczy dwóch najniższych warstw modelu OSI. W projekcie 802 warstwę łącza danych modelu OSI podzielono na dwie podwarstwy: wyższą – LLC – Logical Linc Control oraz niższą – MAC – Media Access Control. Projekt 802 ustalił wiele aktualnie stosowanych standardów, spośród których dwa mają podstawowe znaczenie: 802.3 – definiujący standardy dla warstwy MAC i fizycznej w sieciach magistralowych działających zgodnie z algorytmem CSMA/CD[30] oraz 802.5 - definiujący standardy dla warstwy MAC i fizycznej w sieciach pierścieniowych z przesyłaniem znaczników (token) w paśmie podstawowym[31].

Podstawowe typy sieci LAN. ***Ethernet*** – sieć typu LAN pracująca w paśmie podstawowym. Sieci te wykorzystują metodę dostępu CSMA/CD oraz mają przepustowość 10 Mb/s. Architektura Ethernet doskonale sprawdza się w sieciach w których od czasu do czasu występują przeciążenia. Inną zaletą sieci jest możliwość stosowania różnych protokołów komunikacyjnych, a zwłaszcza TCP/IP[32]. W sieciach Ethernet zasadniczo stosuje się topologię magistrali liniowej, może być również stosowana topologia gwiazdy. Stosowane są trzy rodzaje okablowania:

- wykonane za pomocą kabla grubego – Thick Ethernet;
- wykonane za pomocą kabla cienkiego – Thin Ethernet;
- wykonane za pomocą nieekranowanej skrętki – UTP – Unshieled Twisted Pair.

W standardzie 802.3 wymienione są trzy odmiany sieci , w których wykorzystuje się różne okablowanie: 10BASE2 (cienki kabel), 10BASE5 (gruby kabel), 10BASE-T (nieekranowana skrętka).Udoskonalone sieci Ethernet**:**

- sieć Ethernet komutowana pakietami,
- dupleksowa sieć Ethernet,
- sieć Fast Ethernet (sieć zgodna z 802.3 o szybkości 100 Mb/s).

Token Ring – sieć typu LAN o architekturze zgodnej ze specyfikacją 802.5. Sieć charakteryzuje:

- topologia pierścieniowo-gwiaździsta;
- uzycie techniki przekazywania znacznika;
- transmisja w pasmie podstawowym.

---

30 - Carrier Sense Multiple Access with Collision Detection – metoda dostępu stosowana w sieciach Ethernet.
31 - metody tej aktualnie używa się w architekturze Token Ring.
32 - TCP/IP - Transmission Control Protocol/Internet Protocol. Zbiór sieciowych protokołów umożliwiających komunikację pomiędzy różnymi systemami, pochodzącymi od różnych dostawców.

JAWNE Zastrzeżone

- okablowanie za pomocą skrętki nieekranowanej, lub ekranowanej;
- szybkość transmisji 4 Mb/s, lub 16 Mb/s;

W architekturze Token Ring jest stosowana deterministyczna metoda uzyskiwania dostępu do sieci za pomocą specjalnego znacznika (pakietu) krążącego w sieci (token).

ARCnet – sieć typu LAN opracowana przez Datapoint Corporation. W sieci jest stosowana technika przekazywania znacznika wzdłuż magistrali, bardzo podobna do przekazywania znacznika w pierścieniu (w sieciach Token Ring). Sieć może być skonfigurowana w topologii magistrali, lub gwiazdy, często występuje w postaci gwiazdy rozproszonej, lub drzewa. Połączenia mogą być realizowane za pomocą 93 omowego kabla koncentrycznego RG-62, lub za pomocą skrętki. W sieci mogą być stosowane huby pasywne i aktywne co powoduje, że nadaje się ona przy skomplikowanym okablowaniu.

Sieci MAN. Sieci miejskie-MAN /Metropolitan Area Network/ z historycznego punktu widzenia stały się pierwszymi komponentami przyszłych B-ISDN. Z uwagi na różne kryteria, sieci MAN można sklasyfikować jako:

- sieci świadczące jeden rodzaj usług, t.j. sieci teleinformatyczne (np. X.25, FDDI),
- sieci z integracją usług (IEEE 802.6, ISDN); ewentualnie:
- sieci prywatne
- sieci publiczne

Sieć FDDI jest typową siecią informatyczną (świadczącą jeden rodzaj usług). Głównym jej przeznaczeniem było zapewnienie możliwości wzajemnego połączenia oddalonych od siebie lokalnych sieci komputerowych LAN /Local Area Network/. Sieć FDDI pracuje zwykle w konfiguracji podwójnej pętli (pętla pierwotna i pętla wtórna). Transmisja w pętlach odbywa się w przeciwnych kierunkach z szybkością 100 Mb/s

Jako medium transmisyjne wykorzystywany jest światłowód (umożliwia on połączenie do 500 stacji przy maksymalnej długości kabla 200 km). Długość odcinka światłowodu pomiędzy sąsiednimi stacjami FDDI nie powinna przekraczać 2 km (dla światłowodu gradientowego), lub 60 km dla światłowodu jednomodowego.

Źródłem promieniowania w nadajnikach są diody elektroluminescencyjne (LED) emitujące falę o nominalnej długości 1300nm (1270-1380 nm). Normy FDDI definiują 2 klasy stacji:

- stacje klasy SAS (Single Attachment Station) – mające jedną parę obiektów warstw PMD[33] (Physical Layer Medium Dependent) i PHY[34] (Physical Layer Protocol),

[33] - niższa podwarstwa warstwy fizycznej PL (Physical Layer) modelu odniesienia ISO/OSI.
[34] - wyższa podwarstwa warstwy fizycznej PL (Physical Layer) modelu odniesienia ISO/OSI.

JAWNE
Zastrzeżone

- stacje klasy DAS (Dual Attachment Station) mające dwie pary obiektów PMD i PHY.

Fizyczna pętla FDDI może zawierać tylko stacje klasy DAS. Stacje te są nazywane koncentratorami i dzielą się na dwie grupy:

- koncentratory SAC (Single Attachment Concentrator),
- koncentratory DAC (Dual Attachment Concentrator).

Zastosowanie SAC i DAC umożliwia tworzenie wielopoziomowej struktury sieci (np. sieci o topologii podwójnej pętli z drzewami). Każda stacja prowadzi ciągły monitoring stanu sieci. Dostęp do medium transmisyjnego uzyskuje się po przejęciu uprawnienia nazywanego tokenem. Przejęciu tokena przez stację odpowiada jego usunięcie z pętli. Po uzyskaniu dostępu stacja transmituje ramki informacyjne przez określony protokołem (TTRP – Timed Token rotation Protocol) okres czasu, po czym natychmiast generuje nowy token.

Sieć FDDI-II. Stanowi rozszerzenie sieci FDDI umożliwiając transmisję danych w oparciu o dwie metody komutacji: komutację pakietów i komutację łączy. Dokonuje się tego przez podział wspólnego kanału sieci na szczeliny czasowe, przydzielane dynamicznie bądź kanałowi transmisji pakietowej, bądź kanałowi transmisji izochronicznej. Niezbędne zmiany dotyczące wprowadzenia usługi transmisji izochronicznej zawiera standard HRC (Hybrid Ring Control). Każda stacja sieci FDDI-II może pracować w trybie podstawowym (Basic Mode) – zgodnym ze standardem FDDI-I oraz w trybie hybrydowym (Hybrid Mode) – jako stacja sieci FDD-II.

Sieć oparta na protokle DQDB (Distributed Queue Dual Bus) – standardu IEEE 802.6. Jest to sieć z integracją usług (umożliwiająca . transmisję danych, szybki transfer zbiorów, transmisję głosu i obrazów). Sieć DQDB można budować w oparciu o szerokie spektrum dostępnych systemów transmisyjnych (np.G.703, SDH, SONET). Sieć DQDB może być w stosunkowo prosty sposób przyłączana do przyszłych sieci B-ISDN. Architektura sieci oparta jest na dwóch magistralach A i B, w których transmisja odbywa się w przeciwnych kierunkach. Sieć gwarantuje połączenie typu full-duplex pomiędzy dowolnymi parami węzłów.

Sieci WAN. Sieci WAN mogą obejmować swym zasięgiem obszar całego kontynentu, lub państwa. Sieć WAN może być rozwinięta jako sieć publiczna (udostępniająca swoje zasoby wszystkim użytkownikom, lub jako sieć resortowa udostępniająca swoje zasoby tylko użytkownikom jednego resortu. Obecny rynek telekomunikacyjny oferuje wiele technologii umożliwiających budowę rozległych sieci komputerowych. Każda z niżej wymienionych technologii cechuje się określonymi właściwościami.

JAWNE
Zastrzeżone

- Technologia wykorzystująca ***łącza komutowane*** (dial-up phone lines). Przykładem jest wykorzystywanie linii telefonicznych publicznej sieci telekomunikacyjnej PSTN (Plain Switched Telephone Network), lub POST (Plain Old telephone Service) do transmisji danych za pośrednictwem modemów (najbardziej popularne protokoły TD: V.32, V.32bis, V.42, V.42bis). Efektywna szybkość transmisji zależy od: jakości łączy telefonicznych, centrali telefonicznej, parametrów technicznych modemów, kompresji danych. Wysoki koszt połączeń telefonicznych oraz mała szybkość TD (zwykle nie przekraczająca 28,8 kb/s) - uniemożliwiająca realizację bardziej zaawansowanych usług multimedialnych ograniczają zakres zastosowań łączy komutowanych Linie komutowane używane są również w charakterze połączeń zapasowych (backup) dla linii dzierżawionych, X.25 czy Frame Relay.
- Technologia wykorzystująca ***łącza dzierżawione*** (leased lines). Są z założenia zestawiane na stałe na dłuższy czas określony między operatorem i klientem. Opłaty są zależne od przepustowości, a nie od ruchu. Rozróżnia się dwa rodzaje łączy dzierżawionych: analogowe, cyfrowe. W przypadku łączy cyfrowych klient dysponuje większym zakresem możliwych do uzysknia przedkości TD: od 9,6 kb/s , przez 64 kb/s (T0), n x 64 kb/s (Fractional T1-FT1), 2 Mb/s (E1), 34 Mb/s (E3). W Polsce dzięki urządzeniom NewBridge zainstalowanym w sieci TP S.A można dzierżawić kanały n x64 kb/s (maksymalnie 2 Mb/s – kanał E1). Typowym zastosowaniem łączy dzierżawionych jest połączenie dwóch odległych sieci lokalnych LAN-LAN. Najczęściej wykorzystywane są do tego mostki (bridge), lub urządzenia trasujące (routery). Z uwagi na dobrą jakość łączy (szczególnie cyfrowych) oraz możliwość szybkiej TD łącza mogą być wykorzystywane do realizacji niektórych usług multimedialnych.

ISDN (Integrated Services Digital Network). Możliwość zestawiania połączeń „każdy z każdym". Wykorzystywane dwa rodzaje standardowych styków: BRI (Basic Rate Interface) $2B_{64}+D_{16}$ (o przepływności 128 kb/s bez kompresji, lub 144 kb/s z wykorzystaniem kanału D) oraz PRI (Primary Rate Interface) $30B_{64}+D_{64}$ o przepływności 2,048 Mb/s (E1) /w systemach Ameryki Północnej oraz Japonii PRI posiada $23B_{64}+D_{64}$ o łącznej przepustowosci 1,5 Mb/s (T1)/. Styk BRI znajduje zastosowanie do podłączania np. małych biur (umożliwia podłączenie do 8-miu indywidualnie rozpoznawalnych urządzeń). Głównym zastosowaniem PRI jest możliwość agregacji wielu styków BRI umożliwiając np.połączenie wielu małych oddziałów firm z jej siedzibą główną. Bardzo ważnym aspektem technologii ISDN jest możliwość współpracy urządzeń pochodzących od różnych producentów. Urządzenia są badane pod kątem zgodności z normami ETSI.

Technologia wykorzystująca ***protokół X.25*** (opracowany w latach 70-tych). Umożliwia zestawianie kanałów wirtualnych SVC (Switched Virtual Circuit), co w porównaniu z technologią łączy dzierżawionych oznacza realizację kilku logicznych kanałów na jednym styku fizycznym (bardziej elastyczne wykorzystanie urządzeń oraz mniejsze opłaty abonentowe za dzierżawę łączy). W protokole X.25 są wbudowane silne mechanizmy korekcji błędów, które umożliwiają prawidłową pracę nawet na łączach złej jakości. Sieci pakietowe zbudowane w oparciu o protokół X.25 wykorzystuje się najczęściej do interaktywnej pracy terminalowej (np. dostęp do baz danych), aczkolwiek możliwym jest również łączenie sieci LAN. Protokół X.25 wypierany przez sieci oparte o protokoły Frame Relay i ISDN jest ciągle najtańszym sposobem realizacji niezawodnej transmisji danych.

Technologia wykorzystująca ***protokół Frame Relay*** (początek prac standaryzacyjnych 1984) jest nowoczesnym protokołem zaprojektowanym z myślą o współpracy z takimi protokołami jak TCP/IP (Tranmission Control Protocol/Internet Protocol) oraz SPX/IPX (Sequenced Packet Exchange/Internet Packet Exchange). Szybkości dostępowe do sieci Frame Relay zaczynają się od 64 kb/s, a kończą na 2 Mb/s (E1). Łącza międzywęzłowe mogą pracować z prędkością do 34 Mb/s (E3). Charakterystycznym parametrem Frame Relay jest CIR (Committed Information Rate) definiowany dla każdego statycznie zestawianego kanału logicznego PVC (Permanent Virtual Circuit) określający gwarantowaną przez operatora minimalną szybkość TD (w każdej chwili może być większa jeśli pozwalają na to zasoby sieciowe). Najnowsze implementacje umożliwiają konfigurację kanałów SVC (Switched virtual Circuit) zestawianych na żądanie w chwili zapotrzebowania na TD – analogicznie do telefonicznych łączy komutowanych, lub łączy wirtualnych X.25. Protokół Frame Relay jest preferowany do łączenia ze sobą sieci lokalnych LAN. Coraz bardziej popularnym zastosowaniem staje się przesyłanie dźwięku VOFR (Voice Over Frame Relay) co jednak wymaga zastosowania specjalnych urządzeń do kompresji i dekompresji dźwieku. Pod względem technicznym konkurencją dla sieci Frame Relay może być dobrze rozbudowana sieć ISDN, sieć cyfrowych łączy dzierżawionych, lub ATM.

Technologia wykorzystująca ***ATM*** (Asynchronous Transfer Mode). Jest określana jako docelowa technologia dla systemów telekomunikacyjnych. Może być stosowana zarówno w sieciach rozległych jak i w sieciach lokalnych. ATM umożliwia świadczenie większej ilości usług multimedialnych jak np. transmisja dźwięku i obrazu o wysokiej jakości. Obecnie dostępne szybkości transmisji zaczynaja się od 1,544 Mb/s (T1) poprzez 155,520 Mb/s (OC-3, STM-1) do 2488,320 Mb/s (OC-48, STM-16). Podobnie jak w protokole Frame

JAWNE
Zastrzeżone

Relay ATM nie gwarantuje dostarczenia informacji do węzła końcowego. ATM jest przeidziany do TD przez łącza o wysokiej jakości (światłowód, skrętka kategorii V).

4.9. Radiokomunikacja

Radiokomunikacja jest tą dziedziną łączności, która na całym świecie rozwija się najbardziej dynamicznie. Dystans jaki nas dzieli od przodujących krajów Europy jest znacznie mniejszy, niż w przypadku telekomunikacji przewodowej.

Radiodyfuzja. Jest ona usługą telekomunikacyjną, którą należy rozumieć jako dostarczanie dla wielu odbiorców jednocześnie programów radiofonicznych i telewizyjnych. Dostarczanie może odbywać się za pomocą fal radiowych lub przy wykorzystaniu sieci kablowych. Ogólnopolskie sieci telewizyjne i radiowe uzupełniane są sieciami regionalnymi i stacjami lokalnymi. Można przewidywać, że w niedalekiej przyszłości rozpocznie się wykorzystywanie sieci telewizji kablowych do świadczenia takich usług, jak: nadawanie filmów na zamówienie, telefonia, połączenia międzykomputerowe, telezakupy.

Systemy dostępu radiowego. W ostatnim okresie szereg firm zajmujących się produkcją sprzętu telekomunikacyjnego oferuje radiowe systemy dostępu. Mają one zastosowanie szczególnie na terenach wiejskich, słabo zaludnionych i o "słabej" kablowej infrastrukturze telekomunikacyjnej. Abonent takiego systemu posiada bezprzewodowy aparat telefoniczny (abonent ruchomy) lub zwykły aparat telefoniczny (sygnały od abonentów do centrali są transmitowane drogą radiową poprzez układ antenowy znajdujący się w budynku). Zalety systemu dostępu radiowego:

- konkurencyjny cenowo względem kabla system;
- wysoka jakość przekazu dorównująca tradycyjnej transmisji kablowej;
- łatwość wdrożenia systemu i jego utrzymania (odpadają koszty konserwacji studzienek, kabli telekomunikacyjnych itp.);
- możliwość utajniania przekazu cyfrowego w tym systemie;
- możliwość przekazywania danych komputerowych w systemie;
- możliwość szybkiego kontaktu z osobą funkcyjną (służbą dyżurną, patrolem) posiadającą aparat w tym systemie (tak jak w telefonii komórkowej) - pod warunkiem, że te osoby znajdują się w zasięgu centrali oferującej dostęp radiowy.

Centrale systemów dostępu radiowego są połączone z "tradycyjną kablową" centralą telefoniczną i abonent radiowy może się połączyć z dowolnym abonentem sieci kablowej i odwrotnie.

JAWNE
Zastrzeżone

System przywoławczy (pagingowy) jest to jednokierunkowy, radiowy system komunikacyjny, umożliwiający abonentowi wyposażonemu w niewielki i niedrogi odbiornik kieszonkowy (pager) otrzymywanie krótkich komunikatów przywoławczych. Standaryzacja wielu niespójnych systemów doprowadziła do określenia międzynarodowego standardu POCSAG, definiującego zasady sygnalizacji i kodowania w systemach przywoławczych, a w Unii Europejskiej przygotowano standard cyfrowego systemu przywoławczego ERMES (z ang. Europan Radio Message System) o europejskim zasięgu. Większość prywatnych systemów przywoławczych stosowanych w europie stosuje kod POCSAG, uznany przez CCIR za międzynarodowy kod przywoławczy RPC 1.

Zasadniczym elementem systemu jest centrala przywoławcza połączona bezpośrednio (zwykle przewodów) z nadajnikiem lokalnym lub z siecią nadajników rozmieszczonych na terenie kraju. Przekazywanie zleceń do systemu przywoławczego może odbywać się kilkoma sposobami, zarówno za pośrednictwem operatora jak też i bez jego udziału, w sposób całkowicie automatyczny.

Ze względu na zasięg rozróżnia się systemy przywoławcze:

- lokalne;
- o dużym zasięgu.

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

- sygnałem tonowym;
- sygnałem numerycznym;
- sygnałem alfanumerycznym.

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

Systemy trunkingowe. Radiowy system komunikacyjny polegający na automatycznym przydzielaniu i podziale ograniczonej puli kanałów radiowych (trunks) między znacznie wyższą od tej puli liczbą użytkowników. Idea trankingu opiera się na teorii prawdopodobieństwa, która zakłada, że jest małe prawdopodobieństwo, aby wszyscy abonenci w tym samym czasie chcieli korzystać z całej puli dostępnych kanałów radiowych. Kanały komunikacyjne (pasma częstotliwości radiowej) są przydzielane abonentowi na żądanie i zwalniane natychmiast po zakończeniu rozmowy, uzyskuje się wysoką efektywność wykorzystania widma częstotliwości, pozwalającą na zredukowanie liczby nośnych niezbędnych do zapewnienia wymaganej jakości usług. Technika trankingu jest szeroko

JAWNE
Zastrzeżone

stosowana do wewnętrznej łączności w przedsiębiorstwach rozległych oraz w stacjonarnej i ruchomej transmisji danych.

W Polsce pracuje wiele prywatnych i publicznych sieci trankingowych, spełniających funkcje teledacyjne. Nadzieją na standaryzację na poziomie europejskim jest TETRA (ang. Trans European Trunked Radio), będąca w zakresie systemów teledacyjnych odpowiednikiem standardu GSM. Wysokie oczekiwania odbiorców profesjonalnych w zakresie jakości komunikowania się, szybkości i bezpieczeństwa przesyłania danych oraz szybki rozwój myśli technologicznej końca XX wieku, a szczególnie w zakresie telekomunikacji, przyczyniły się do stworzenia nowej generacji cyfrowego systemu radiokomunikacji ruchomej a nazwie Tetra. Tetra, czyli Terrestial Trunked Radio, to nazwa całego zespołu otwartych standardów – interfejsów i usług – opracowanych przez ETSI – Europejski Instytut Norm Telekomunikacyjncy. Tetra to pierwszy w pełni otwarty, międzynarodowy standard cyfrowej radiokomunikacji ruchomej do zastosowań profesjonalnych.

W pracach zmierzających do opracowania specyfikacji systemu obok największych producentów terminali i systemów radiokomunikacyjnych brały także udział organizacje rządowe kilkunastu państw europejskich oraz najwięksi producenci terminali i systemów radiokomunikacyjnych, w tym firma Nokia. Dzięki temu udało się stworzyć system, który wykorzystuje możliwości najnowocześniejszej techniki i technologii potrafi spełnić wysokie oczekiwania przedstawicieli służb bezpieczeństwa i porządku publicznego (wojsko, policja, straż pożarna, pogotowie ratunkowe, służby leśne, obrona cywilna, administracja państwowa, itp.) oraz organizacji komercyjnych (firmy transportowe, energetyka, gazownictwo, stocznie, kopalnie, rafinerie, korporacje handlowe, itp.).

ETSI zarezerwowało dla standardu TETRA dwa pasma częstotliwości: 380 – 400 MHz dla służb bezpieczeństwa i porządku publicznego oraz pasmo 410 – 430 MHz dla organizacji komercyjnych. Oznacza to, że instytucje i służby oraz prywatni użytkownicy systemu Tetra z różnych państw mogą korzystać z dostępu do sieci również poza zasięgiem nadajników swojego narodowego operatora.

Technikę systemu Tetra można porównywać z analogowymi systemami trankingowymi, systemami telefonii komórkowej, a także innymi cyfrowymi systemami radiokomunikacji ruchomej.

Systemy cyfrowe mają wiele cech i oferują wiele funkcji niedostępnych w systemach analogowych. Dotyczy to np. równoczesnego przekazywania głosu i danych oraz możliwości

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

korzystania z sieci przez wielu użytkowników w zamkniętych ramach poszczególnych organizacji.

Połączenia telekonferencyjne w systemie Tetra bardzo różnią się od tradycyjnych metod łączności radiowej:

- połączenia w grupie użytkowników są kodowane;
- położenie geograficzne ani liczba kanałów nie ograniczają możliwości tworzenia grup użytkowników sieci;
- technika cyfrowa i kodowanie protekcyjne umożliwiają osiągnięcie wyższej jakości transmisji mowy w stosunku do systemów analogowych;
- dostępne pasmo częstotliwości jest wykorzystywane bardziej efektywnie – dzięki technice zwielokrotnienia czasowego TDMA zamiast jednego kanału radiowego można stosować większą liczbę kanałów logicznych;
- przynależność użytkownika do grupy wewnątrz danej organizacji można określać w sposób elastyczny z poziomu konsoli dyspozytorskiej.

System Tetra został zaprojektowany z myślą o wymagających użytkownikach profesjonalnych, co w zdecydowany sposób odróżnia go od systemu GSM, zapewniającego jedynie realizację transmisji głosu i danych. Podsumowując można stwierdzić, że system Tetra zapewnia sprawną łączność grupową, bezpieczeństwo, priorytety dostępu oraz połączenia w trybie bezpośrednim (łączność pomiędzy terminalami znajdującymi się poza zasięgiem sieci).

Kraje Unii Europejskiej na spotkaniu w Schengen w 1995 roku doszły do porozumienia, że w krajach członkowskich powinien zostać wprowadzony wspólny, otwarty standard radiokomunikacji ruchomej dla organizacji bezpieczeństwa publicznego. Propozycja stworzenia takiego systemu wraz ze szczegółowo określonymi wymogami odnośnie jego funkcjonowania została przekazana do ETSI, a ETSI w oficjalnej odpowiedzi stwierdziła, że opracowywany właśnie standard Tetra spełnia oczekiwania Unii. W 1997 roku Tetra uznana została za standard dla organizacji bezpieczeństwa publicznego, który będzie wprowadzony w krajach UE.

Do tej pory w Europie wydano już wiele licencji dla operatorów systemu Tetra. Powszechnie przyjętą jest praktyka wydawania licencji ogólnokrajowych, preferująca tworzenie zintegrowanych systemów rozległych. Takie podejście zapewnia przede wszystkim minimalizację kosztów inwestycyjnych i operacyjnych, a ponadto gwarantuje użytkownikom ten sam poziom usług niezależnie od ich lokalizacji (np. realizacja połączeń grupowych na obszarze całego kraju).

JAWNE
Zastrzeżone

Tetra poza odpornością na zakłócenia i stabilnością działania zapewnia wiele funkcji użytecznych w codziennej pracy zarówno służb bezpieczeństwa publicznego jak i organizacji i przedsiębiorstw komercyjnych – jak np. błyskawiczne zestawienie połączeń indywidualnych i grupowych, połączenia alarmowe, praca w trybie bezpośrednim, możliwość ustalania różnych priorytetów dla połączeń oraz dynamiczne tworzenie grup.

Należy podkreślić, że system Tetra w porównaniu z dotychczas użytkowanymi analogowymi systemami łączności radiowej, systemami telefonii komórkowej a także innymi cyfrowymi systemami radiokomunikacji ruchomej ma wiele istotnych zalet, a mianowicie:

- zapewnia efektywne wykorzystanie ograniczonych zasobów częstotliwości (w jednym kanale radiowym o szerokości 25 kHz dostępne są 4 kanały komunikacyjne);
- zapewnia sprawną łączność grupową oraz możliwość współdziałania pomiędzy różnymi służbami i organizacjami, co ma szczególne znaczenie w stanach zagrożenia;
- rozbudowane możliwości transmisji danych w połączeniu z kodowaniem sygnału zapewniają szybki dostęp do baz danych z dowolnego miejsca, przy jednoczesnym zachowaniu pełnej poufności przesyłanych informacji;
- poprzez kodowanie zapewnia bezpieczeństwo przesyłanych informacji;
- możliwość pracy w trybie bezpośrednim, tj. bez wykorzystania infrastruktury sieci;
- jest to system otwarty, czyli jest wielu producentów, którzy ze sobą konkurują, zapewniając poprzez to lepszy wybór, wysoką jakość systemu oraz stały rozwój standardu;
- umożliwia praktycznie natychmiastowe i pewne zestawienie połączeń (ok. 300 msek);
- jej wykorzystanie usprawnia działanie różnych organizacji poprzez efektywne zarządzanie zasobami ludzkimi i sprzętowymi.

Tetra jest szczególnie przydatna w zastosowaniach na rzecz policji, straży pożarnej, pogotowia ratunkowego i wielu innych służb oraz organizacji mających na celu zapewnienie bezpieczeństwa i porządku publicznego. Rozwiązania oparte na publicznych środkach łączności nie spełniają w wystarczającym zakresie wymagań stawianych przed systemami profesjonalnymi. Tetra, jako system z założenia przeznaczony do zastosowań profesjonalnych, od początku była opracowywana pod kątem spełnienia bardzo ostrych wymagań stawianych przez organizacje bezpieczeństwa publicznego. Natychmiastowe zestawianie połączeń, połączenia grupowe wraz z możliwością dynamicznego tworzenia grup (obejmujących w zależności od potrzeb przedstawicieli różnych służb), rozbudowane funkcje dyspozytorskie – są to przykładowe funkcje, które nie są realizowane w publicznych systemach telekomunikacyjnych.

Na rynku można spotkać rozwiązania symulujące system trankingowy na bazie sieci GSM – takie rozwiązania oferują jednak jedynie bardzo ograniczony zakres dodatkowych funkcji, zajmują także szerokie pasmo częstotliwości (np. przy połączeniu grupowym każdy abonent zajmuje jeden kanał radiowy, w przypadku zaś Tetry praktycznie nieograniczona liczba abonentów może uczestniczyć w połączeniu grupowym zajmując tylko jeden kanał radiowy).

Należy także pamiętać o tym, że w sytuacjach kryzysowych publiczne środki łączności nie gwarantują odpowiedniej niezawodności - ulegają one zablokowaniu lub uszkodzeniu. Rozwiązaniem jest tu jedynie zastosowanie wydzielonej sieci łączności radiowej opartej na systemie Tetra. Dzięki standaryzacji i możliwości budowy sieci rozległych umożliwia ona współdziałanie nie tylko w obrębie jednego regionu czy kraju, ale także pomiędzy służbami i organizacjami wielu państw.

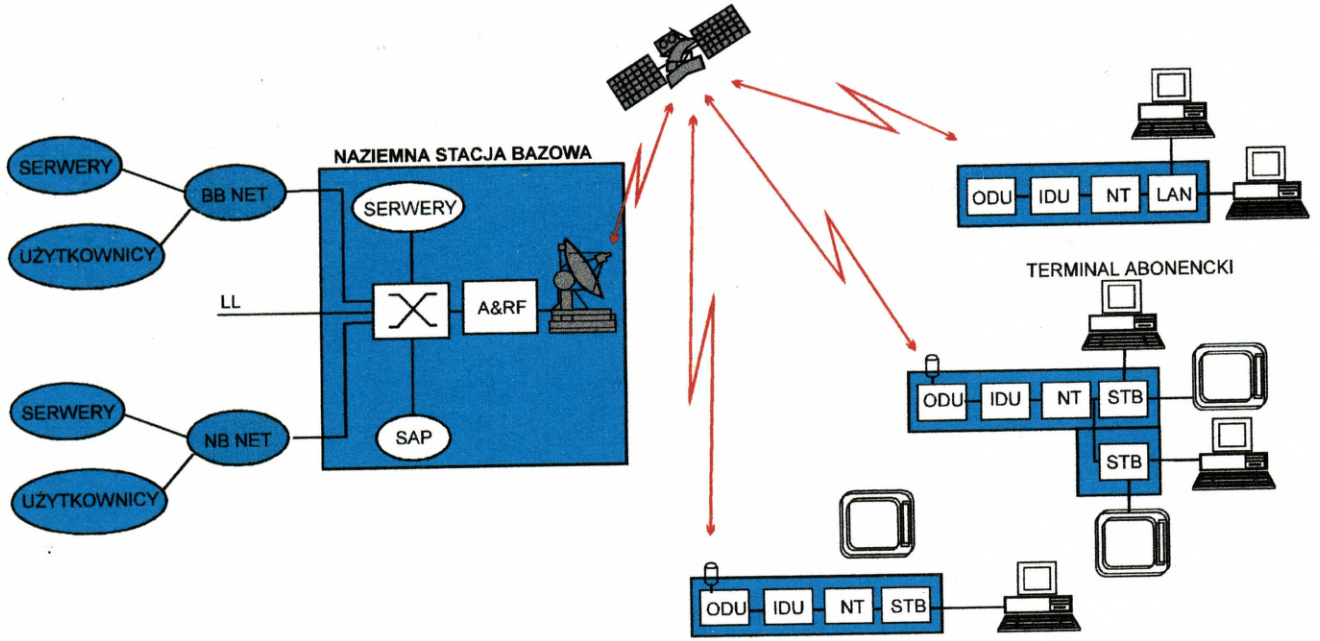
Systemy satelitarne. W kraju istnieje nowoczesny system łączności satelitarnej (na skalę europejską) w Psarach koło Kielc. Przykład takiej sieci przedstawiono na rys. 4.10.

W stacjonarnych systemach satelitarnych komunikacja między abonentami dokonuje się za pomocą satelitów telekomunikacyjnych umieszczonych na orbitach geostacjonarnych. Każdy system obejmuje jeden lub kilka aktywnych satelitów i przynajmniej jednego rezerwowego , uaktywnianego w przypadku uszkodzenia lub utraty kontroli nad satelitą aktywnym. Satelity wykorzystywane do celów telekomunikacyjnych są zwykle wyposażone w kilka (do kilkudziesięciu) transponderów, pracujących w różnych pasmach o częstotliwości od kilku do kilkudziesięciu GHz, wykorzystywanych w zależności od zastosowań, rodzaju transmisji, sposobu rezerwacji pasma i wielkości przepływności binarnej przez kanały satelitarne.

Typowymi zastosowaniami systemów satelitarnych są:

- naziemne satelitarne stacje odbiorcze TV, pracujące w zakresie 11/12 GHz;
- systemy z terminalami VSAT (z ang. Very Small Aperture Terminal), pracujące w pasmie Ku 11/12/14 GHz lub w pasmie C 4/6 GHz;
- naziemne satelitarne stacje ruchome umożliwiające transmisję danych z niewielkimi szybkościami, pracujące w zakresie 11/12/14 GHz

Niektóre pasma częstotliwości satelitarnych pokrywają się z naziemnymi liniami radiowymi do transmisji sygnałów cyfrowych działających w zakresach częstotliwości 11, 14, 23, 38, 50 GHz.



Oznaczenia:

ODU - (Outdoor Unit) część zewnętrzna terminala abonenckiego
IDU - (Indoor Unit) część wewnętrzna terminala abonenckiego
NT - (Network Termination) zakończenie sieciowe
LAN - (Local Area Network) lokalna sieć komputerowa
STB - (Set Top Box) przystawka abonencka
SAP - (Service Access Point) punkt dostępu do usług
A&RF - (Access and RF Equipment) wyposażenie radiowe i dostępowe
BB NET - (Broadband Network) sieć szerokopasmowa
NB NET - (Narrowband Network) sieć wąskopasmowa

Rys. 4.10. Schemat sieci satelitarnej (wariant)

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Przyznane są one wyłącznie dla specyficznych rodzajów służb lub wykorzystywane wspólnie przez wiele służb publicznych. Do największych światowych systemów satelitarnych należą: Intelsat, Inmarsat, Orion, Eutelsat i Panamsat. Optymalne położenie satelitów ze względu na dostęp do nich z terytorium naszego kraju systemy: Intelsat, Inmarsat i Eutelsat.

Inne systemy radiowe. W Polsce pozostało jeszcze blisko 5 tys. przestarzałych dyspozytorskich sieci radiotelefonicznych z 300 tys. terminali. Wykorzystują one bardzo dużo częstotliwości, m.in. 33 MHz, 160 MHz, 170 MHz czy 300 MHz. Mało kto wie, że oprócz trankingu i przestarzałych systemów dyspozytorskich działa w Polsce dupleksowa ruchoma łączność telefoniczna wprowadzona pod koniec lat osiemdziesiątych na częstotliwości 160 MHz. 28 kanałów tej sieci użytkuje TP S.A. Jest około 5 tys. abonentów tego systemu, który przypomina wczesne samochodowe konstrukcje radiotelefoniczne z końca lat siedemdziesiątych.

4.10. Techniki realizacji systemów i struktury sieciowe

Systemy analogowe. Istnieje jeszcze duża ilość urządzeń i systemów zrealizowanych w przestarzałej technice analogowej. W systemach analogowych sygnał zmienia się w sposób ciągły w przeciwieństwie do dyskretnych sygnałów cyfrowych. Do transmisji głosu wystarcza pasmo przenoszenia od 300 Hz do 3400 Hz. Natomiast transmisja dźwięków wysokiej jakości wymaga większej szerokości pasma przenoszenia - do 16 kHz. W systemach komutacyjnych do lat dziewięćdziesiątych w Polsce stosowano powszechnie technikę przesyłania sygnałów analogowych za pomocą kanałów telefonicznych w podstawowym paśmie przenoszenia lub poprzez kosztowne urządzenia zwielokrotnienia częstotliwościowego o niewielkiej krotności kanałów rozmównych ze względu m.in. na embargo w dostępie do najnowszych technologii. Od początku lat 90-tych są one wypierane przez nowoczesne urządzenia cyfrowe.

Systemy cyfrowe. Technika modulacji kodowo - impulsowej PCM[35] jest podstawą telefonii cyfrowej. Została opatentowana w 1926 r., jednak dopiero w 1962 r. zastosowano ten wynalazek w telekomunikacji.[36] Dążenie do maksymalnego wykorzystania możliwości przepustowych stosowanych linii transmisyjnych stało u podstaw opracowania cyfrowych

---

[35] PCM (Pulse Code Modulation) - w telekomunikacji podstawowa technika konwersji sygnału analogowego mowy do postaci cyfrowej.

[36] Pionierskim był 24-krotny system amerykański TCK-24 o przepływności 1544 kbit/s (w przybliżeniu 1.5 Mbit/s) opracowany w roku 1962. Nieco później, bo w roku 1968 opracowano w Europie 30-kanałowy system PCM-30. Wykorzystywał on metodę zwielokrotnienia, w której w sygnale wynikowym zawarte były sygnały z 30 użytkowych kanałów 64 kbit/s oraz dwu kanałów dodatkowych, służących transmisji sygnałów sterujących. Zastosowany sposób zwielokrotnienia prowadził do utworzenia strumienia o przepływności 2048 kbit/s.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

systemów wielokrotnych z wykorzystaniem sygnałów cyfrowych o dużej przepływności uzyskanych z łączenia wielu sygnałów o mniejszej przepływności przez zwielokrotnienie z podziałem czasu TDM (ang. Time Division Multiplexing). Możliwości zwiększania wykorzystywanej szerokości pasma zaowocowały opracowaniem cyfrowych systemów teletransmisyjnych o rosnących systematycznie krotnościach i szybkościach transmisji. Systemy te oparte były na technice, jaka była dostępna w czasie, kiedy rozpoczynał się ich rozwój. Techniką tą była tzw. plezjochroniczna (tzn. prawie synchroniczna) technika zwielokrotniania sygnałów cyfrowych. Przy wykorzystaniu tej techniki zwielokrotniania powstała oparta na niej hierarchia cyfrowa systemów teletransmisyjnych PDH. Ponieważ w nowo instalowanych centralach i torach transmisji danych TP S.A. stosuje się wyłącznie technikę cyfrową i w związku z tym automatycznie wzrosła jakość usług.

Technika cyfrowa w sieci abonenckiej wprowadza znaczną poprawę jakości świadczonych usług (eliminację przesłuchów, redukcję szumów, zakłóceń i zniekształceń). Jednak zdecydowanie cenniejszą korzyścią tej modernizacji jest udostępnienie użytkownikowi kanału cyfrowego, który umożliwi mu transmisję dowolnego typu informacji. Należy więc podkreślić, że rozpatrywany etap modyfikacji sieci telekomunikacyjnej niesie za sobą daleko idącą unifikację formy przesyłanych danych, niezależną od ich rodzaju i treści.

PDH (ang. Plesiochronous Digital Hierarchy) - plezjochroniczna technika cyfrowa. W systemach plezjochronicznych nie ma pełnego synchronizmu sygnałów. W poszczególnych węzłach sieci instalowane są niezależne zegary o stosunkowo dużej niestałości częstotliwości. Korekcję przesunięć fazowych i opóźnień sygnałów pochodzących z różnych źródeł bądź przychodzących różnymi drogami uzyskuje się poprzez wykorzystanie buforowania i uzupełnienie przeplotu bitowego bitami dopełnienia. Za pomocą tego typu środków uzyskuje się stan bliski synchronizmowi. Ceną jaką się zań płaci jest znaczne opóźnienie sygnałów szczególnie przy długich łączach, lub gdy wymagane jest przeprowadzenie wielu pośrednich multipleksacji i demultipleksacji, konieczność usuwania bitów dopełnienia w urządzeniu odbiorczym lub wreszcie cząstkowa utrata informacji.[37]

Do ograniczeń systemów plezjochronicznych należy zaliczyć:

- zróżnicowanie międzynarodowych standardów zwielokrotnienia (istnieją 3 standardy zwielokrotnienia: europejski, japoński i amerykański);
- konieczność multipleksacji/demultipleksacji w każdym praktycznie węźle sieci;

[37] *NetWorld. Vademecum Teleinformatyka.cz. 1 i cz. 2 - wydanie specjalne, 1998*

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

- niedostosowanie do transmisji sygnałów o przepływnościach różnych od standardowych dla poszczególnych poziomów zwielokrotnienia;
- mała elastyczność (rekonfigurowalność) sieci transmisyjnej;
- brak możliwości zautomatyzowanego zarządzania siecią;
- brak standaryzacji styku optycznego, co utrudnia stosowanie torów światłowodowych pochodzących od różnych producentów;
- duża liczba sprzętu i jego zróżnicowanie;
- wysokie koszty systemu.

Eksploatowane obecnie cyfrowe sieci telekomunikacyjne w znacznej części oparte są na plezjochronicznej hierarchii cyfrowej PDH, która powstała głównie na potrzeby telefonii i nie umożliwia realizacji połączeń wymagających dużych oraz zmiennych przepływności. Ponadto w zakresie plezjochronicznych systemów cyfrowych świat podzielił się na trzy strefy wpływów (Europa, Stany Zjednoczone i Japonia) z różnymi przepływnościami na różnych poziomach zwielokrotnienia. Sytuacja ta powoduje, że istnieją techniczne utrudnienia współpracy tych systemów, bowiem nie są one kompatybilne.

W systemie PDH wykorzystywane są sygnały (strumienie) cyfrowe o przepływności 64 kb/s uzyskiwane w modulatorach PCM poprzez dyskretyzację (w skali czasu z częstotliwością 8 kHz) i próbkowanie (liczba poziomów kwantyzacji – 256) analogowych sygnałów telefonicznych o paśmie 4 kHz, które są następnie zwielokrotniane (w krotnicach I rzędu) metodą przeplatania bajtów (metoda zwielokrotnienia z podziałem czasowym TDM - Time Division Multiplexing) w następujące strumienie grupowe I rzędu:

A/ w tzw. „systemie europejskim" (30/32 krotnym) – w strumienie o przepływności 2.048 Mb/s (kraje Europy, Azji oraz kraje Ameryki Południowej);

B/ w systemach Ameryki Płn. i Japonii (24 krotnych) – w strumienie o przepływności 1,54 Mb/s);

Zalety systemów PDH: pełna "przeźroczystość" polegająca na tym, że każdy sygnał niezależnie od jego zawartości informacyjnej zostaje przenoszony przez MUX. /wada: przetwarzane przez MUX sygnały stanowią dla nich tylko ciągi bitów, bez żadnej struktury wewnętrznej co powoduje, że na czas transmisji tracone są ważne informacje/.

Wady systemów PDH:

- niemożliwość identyfikacji pojedynczego kanału w sygnale grupowym o dużej przepływności;
- brak dostatecznego miejsca w ramkach dla przesyłania informacji służących do zarządzania siecią telekomunikacyjną;

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

- dość skomplikowany i kosztowny transfer strumieni cyfrowych o małej przepływności, ze strumienia cyfrowego o przepływności bardzo dużej. (wymagana jest znaczna różnorodność sprzętu: MUX-y, UKTL itp.);
- brak standaryzacji styku optycznego, co utrudnia (czasem uniemożliwia) łączenie systemów różnych producentów i różnych państw na tym poziomie.

SDH (ang. Synchronous Digital Hierarchy). Synchroniczne systemy teletransmisyjne SDH, stanowią odpowiedź na wady PDH. Cechą charakterystyczną systemów SDH (w odróżnieniu od systemów PDH) jest zastosowanie w systemie jednego zegara, tzw. pierwotnego zegara odniesienia PRC (ang. Primary Reference Clock) o dużej stałości częstotliwości (nie gorszej od 10^{-11}). Z niego w drzewiastej strukturze sieci synchronizacyjnej doprowadzane są sygnały synchronizujące do wszystkich zegarów systemu.[38] Pozwala to na realizację synchronizmu przesyłanych sygnałów i wykonywanych na nich operacjach, co pozwala uniknąć wad systemów plezjochronicznych. Bardzo ważny jest fakt, że systemy SDH mogą współpracować z istniejącymi systemami PDH. Współpraca ta realizowana jest poprzez łączenie ze sobą w jeden standardowy sygnał SDH sygnałów plezjochronicznych. Opracowując standard pomyślano także i o tym, aby zapewnić możliwość współpracy urządzeń pochodzących od różnych producentów. W synchronicznej hierarchii cyfrowej przyjęto jako podstawową przepływność binarną kanału 155,52 Mbit/s. Określono również wyższe poziomy synchronicznej hierarchii cyfrowej pracujące z przepływnościami 622 Mbit/s, 2.5 Gbit/s, a także 5 Gbit/s i 10 Gbit/s[39].

Systemy synchroniczne stanowią kolejny w czasie stopień w rozwoju systemów transmisyjnych. Już od początku opracowywania tych systemów wielką wagę przywiązywano do problemów standaryzacji. W ramach prac standaryzacyjnych rozwiązano również szereg problemów dodatkowych jak np.: wprowadzenie funkcji zarządzania siecią oraz zasad współpracy pomiędzy hierarchiami systemów teletransmisyjnych Europy i Ameryki Północnej. Opis SDH znajduje się w zaleceniach ITU. Opisywane w literaturze standardy SONET /USA/ są podzbiorem ogólnoświatowych standardów SDH.

Jednostką transmisyjną w systemie SDH jest Synchroniczny Moduł Transportowy rzędu N (Synchronous Transport Module STM-N). Moduł ten zwykle przedstawia się w postaci matrycy o 9-ciu rzędach oraz NX 270 kolumnach, gdzie każda komórka matrycy zawiera 8 bitów. Moduł STM-N zawiera:

---

[38] Wadą takiego rozwiązania jest wysoka cena zegarów PRC (zegary atomowe) i możliwość rozsynchronizowania sieci w przypadku ich uszkodzenia.

[39] Dąbrowski A., Kula S., *Systemy i sieci SDH*, WKiŁ, Warszawa 1996.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

- nagłówek SOH /Section Overhead/ - przenoszący wzór fazowania modułu, dwa kanały TD nadzoru, dwa kanały służbowe, bajty detekcji błędów i inne,
- N grup jednostek administracyjnych AUG /Administrative Unit Groups/. Każda AUG zawiera: jednostkę administracyjną rzędu 4 /AU-4/, lub trzy jednostki administracyjne rzędu 3-go /AU-3/. Z kolei: -każda AU-4 zawiera: kontener wirtualny VC-4 i znacznik, wskazujący, w której komórce jednostki znajduje się pierwszy bajt kontenera.

Kontener wirtualny VC-4 zawiera:

- nagłówek POH /Path Overhead/, przenoszący informacje o stanie drogi transmitującej kontener, informacje o zawartości kontenera i inne.
- zawartość kontenera /alternatywnie/: -kontener C-4, przenoszący sygnał o przepływności 140 Mb/s, -3 jednostki wejściowe TU-3 /Tributaru Unit/ o przepływnościach 34/45 Mb/s każda, -21 jednostek wejściowych TU-2 o przepływnościach 6 Mb/s każda, -63 jednostki wejściowe TU-12 o przepływnościach 2.048, lub 1.54 Mb/s każda.

Każda jednostka wejściowa TU zawiera:

- znacznik wskazujący położenie początku zawartego w jednostce kontenera C,
- kontener wirtualny VC-n.

Kontener wirtualny VC-n zawiera:

- nagłówek,
- zawartość przenoszącą sygnały PDH odpowiedniej przepływności.

Przepływności oraz nazwy sygnałów (modułów) SDHprzedstawiono w tabeli 4.8.

Zalety systemów SDH:

przeźroczystość systemu dla sygnałów PDH. Sygnały 1.5 i 2.048 Mb/s /o strukturze zdefiniowanej zal.G.702/ mogą być "rozszywane" /poprzez umieszczenie ramki tych sygnałów w ustalonych miejscach kontenerów VC-11, lub VC-12/ umożliwiając w ten sposób dostęp urządzeń SDH do pojedynczych kanałów.

- możliwość dynamicznego przydzielania abonentom żądanej przepływności /rozproszone zarządzanie przepływnością
- uproszczenie sieci związane z integracją sprzętu: zacierają się różnice pomiędzy krotnicami i traktami liniowymi /ten sam multiplekser może transmitować sygnały o różnych przepływnościach, a sygnał optyczny może być wysyłany wprost krotnicy/, transmisją i komutacją /kanały podstawowe mogą być wydzielane w krotnicy/, siecią i zarządzaniem nią /w ramkach STM-N znajduje się dostateczna liczba bitów do operacji nawet bardzo skomplikowanego zarządzania siecią/.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Tabela 4.8.

Oznaczenie (Mb/s)	SONET /USA/		SDH
	Sygnał elektr.	Sygnał optycz.	
51,84	STS-1	OC-1	STM-0
155,52	STS-3	OC-3	STM-1
466,56	STS-9	OC-9	-
622,08	STS-12	OC-12	STM-4
933,12	STS-18	OC-18	-
1244,16	STS-24	OC-24	-
1866,24	STS-36	OC-36	-
2488,32	STS-48	OC-48	STM-16
4976,94	STS-96	OC-96	STM-32*
9953,28	STS-192	OC-192	STM-64*

* - standardy są w przygotowaniu

- duża żywotność sieci. Wprowadzone funkcje zarządzania umożliwiają natychmiastową identyfikację uszkodzenia linii lub węzła, a zastosowanie tzw. samo naprawiającej architektury umożliwia automatyczną rekonfigurację sieci po wystąpieniu uszkodzenia.
- urządzenia transmisyjne SDH mają znormalizowane interfejsy do istniejących sieci plezjochronicznych. W ramkach STM-N /Synchronous Transport Module/ znajdują się kontenery /pewna liczba bitów w ramce/, w które mogą być wprowadzane strumienie cyfrowe PDH .

ATM (ang. Asynchronous Transfer Mode). Rozpowszechnione obecnie na świecie wąskopasmowe sieci telekomunikacyjne nie zapewniają jakości, wymaganej przy przekazie związanym z usługami multimedialnymi, szczególnie z transmisjami wideo i audio w czasie rzeczywistym. Wynika to głównie ze zbyt małej przepływności łączy oraz niedostosowania mechanizmów sterowania ruchem sygnałów w sieci do wspomnianych typów przekazu.[40]

Z tego powodu CCITT wybrał asynchroniczny tryb przesyłania[41] (ATM - Asynchronous Transfer Mode) jako docelową technikę transmisji B-ISDN[42]. Należy podkreślić, że ATM jest metodą przenoszenia informacji[43] i jako taka nie zależy od zastosowanej techniki transmisji. Jest techniką komutacji krótkich pakietów o skończonej długości zwanych komórkami. Głównym jej elementem są centra komutacji pakietów

[40] Pach A., Lasoń K., Współpraca sieci ATM z innymi systemami telekomunikacyjnymi, WFPT, Kraków 1995.

[41] Od zwielokrotnienia SDH i PDH różni się tym, że nie zachodzi konieczność synchronizacji zegarów centrów komutacyjnych.

[42] B-ISDN Brodband ISDN - szerokopasmowa ISDN.

[43] Materiały z warsztatów Instytutu Łączności.. Podstawy szerokopasmowych sieci telekomunikacyjnych BISDN. Warszawa - Miedzeszyn marzec 1997.

JAWNE
Zastrzeżone

połączone liniami transmisyjnymi. Zasada jest podobna jak w innych metodach komutacji pakietów. Technologia ATM umożliwia łączenie ze sobą szerokiej gamy urządzeń od telefonów do komputerów w jednej sieci. Usuwa to różnicę pomiędzy sieciami lokalnymi (LAN), miejskimi (MAN) czy rozległymi (WAN) integrując je w jednolitą strukturę. ATM może zastępować lub wspomagać konwencjonalne technologie sieciowe takie jak: Ethernet[44], Token Ring[45] czy FDDI[46]. Uniwersalność tej technologii polega na możliwości:

- przesyłania stałych porcji informacji o pojemności 53 bajty (w tym 48 bajtów informacji użytecznej), co ułatwia proces ich obróbki w węzłach sieci ATM;
- ustalania indywidualnych połączeń o dowolnej szybkości w obrębie przyjętych lub istniejących standardów (25 Mb/s, 100 Mb/s, 155 Mbit/s, 622 Mb/s, 2500 Mb/s, dzięki przyporządkowaniu dowolnej liczby komórek do konkretnego połączenia użytkownika; obsługi transmisji: głos, obraz, HDTV z opóźnieniem nie większym niż 10 ms;
- tworzenia przekazów głównie w trybie połączeniowym, co oznacza, że przed wysłaniem informacji właściwej występuje faza zestawiania łącza według parametrów deklarowanych przez abonenta (typ usługi, deklarowana przepływność, deklarowany adres), a po zakończeniu przekazu jego likwidacja;
- adaptacji komórek ATM do dowolnej przepływności medium transportowego, przez wprowadzanie komórek pustych, pomijanych w węźle docelowym;
- przypisania komórkom ATM (kanałowi, ścieżce, połączeniu między użytkownikami) konkretnej usługi, której parametry mogą być dynamicznie zmieniane, zarówno w fazie nawiązywania łącza, jak i w trakcie działania usługi komunikacyjnej;
- zapewnienie "przezroczystości" przenoszenia informacji przez sieć ATM, a więc dostosowanie pracy do sieci z różnymi protokołami komunikacyjnymi i do realizacji różnych usług.

Pojęcie techniki transmisji ATM (Asynchronous Transfer Mode) jest nierozerwalnie związane z tematem sieci B-ISDN, która ma dostarczać swoim użytkownikom szeroki zakres usług. Jest ona naturalnym rozwinięciem idei sieci ISDN i ma zapewniać:

- transmisje interakcyjne i dystrybucyjne, których przedmiotem mogłyby być szeroko pojęte multimedia;
- transmisje szeroko- oraz wąskopasmowe;

---

[44] Komputerowa sieć lokalna pracująca z szybkością 10 Mbit/s. Nowsze rozwiązania Fast Ethernet - 100 Mbit/s i . Gigabit Ethernet - - 1000 Mbit/s.

[45] Sieć komputerowa standardu IBM o szybkości transmisji 4 Mbit/s i 16 Mbit/s.

[46] Dane są przesyłane z szybkością 100 Mbit/s.

- transmisje ciągłe i impulsowe (bursty and continuous traffic) - przy czym bardzo istotnym zagadnieniem jest tutaj wykorzystanie właściwości dużej liczby transmitowanych sygnałów, które nie mają charakteru ciągłego strumienia o określonej przepływności, a raczej potrzebują sporadycznie dużej przepływności łącza;
- usługi połączeniowe i bezpołączeniowe (connection-oriented and conectionless services) - zarówno transmisję wymagającą wcześniejszych procedur ustanawiania połączenia jak i transmisję datagramów;
- implementację do przetwarzania transmitowanych sygnałów - czyli DSP (digital signal processing) - gdzie najważniejszym zagadnieniem jest kompresja sygnałów z algorytmem dostosowanym do ich charakteru, a także dostosowanie ich postaci do potrzeb i wymagań urządzeń odbiorczych;
- szeroką gamę rodzajów połączeń, z których warto wymienić:
  - połączenia punkt-punkt (w wersjach jedno i dwukierunkowych);
  - zespoły równoległych połączeń typu punkt-punkt;
  - połączenia typu punkt-wielopunkt.

Początkowo przewidywano, że odpowiednim sposobem transmisji dla tak wymagającej sieci B-ISDN będzie synchroniczny tryb transmisji STM (Synchronous Transfer Mode) wykorzystywany wcześniej w implementacji ISDN. Rozważano także struktury hybrydowe, ale ostatecznie przyjęto ATM jako technikę wolną od nie akceptowalnych ograniczeń STM. Założono również istnienie struktur hybrydowych jako form przejściowych. Zarówno ATM jak i STM opierają się na podziale zasobów (pasma) sieci i odpowiedniego przydzielania ich użytkownikowi, przy czym o ile ATM jest w istocie swego działania przykładem techniki komutacji pakietów, o tyle STM opiera się na komutacji łączy. STM w latach swojej świetności zastąpił FDM (Frequency Division Multiplexing), zaś ideą działania STM jest TDM (Time Division Multiplexing).

W odróżnieniu od STM, technologia PTM (ang. Packet Transfer Mode) bazuje na przesyłaniu porcji informacji zwanych pakietami, których przynależność do danego połączenia jest identyfikowana na podstawie przenoszonego wewnątrz tej struktury adresu. Jak sama nazwa sugeruje, PTM opiera się na komutacji pakietów i nie wymaga fazy nawiązywania połączenia, ponieważ źródło i cel transmitowanych danych jest określone jednoznacznie poprzez unikalne adresy. Technika ta jest szeroko wykorzystywana w komputerowych sieciach lokalnych, zaś dostęp do fizycznego łącza odbywa się bądź na zasadzie rywalizacji (CSMA/CD - Ethernet), bądź poprzez współgospodarowanie łączem (Token Ring). Pozwala to na elastyczne gospodarowanie zasobami sieci, z drugiej jednak

JAWNE
Zastrzeżone

strony uniemożliwia pracę w czasie rzeczywistym. W efekcie nie jesteśmy w stanie zapewnić danej usłudze określonej, choćby minimalnej, ale zawsze gwarantowanej przepływności. ATM jest technologią, która łączy najlepsze cechy poprzednio omawianych STM (prostotę i duże prędkości transmisji) i PTM (elastyczność przydzielaniu pasma). ATM charakteryzuje się następującymi właściwościami:

- użyteczna pojemność interfejsu (ang. bandwidth) jest podzielona na małe komórki o stałej długości (cell);
- przynależność danej komórki do konkretnego połączenia jest identyfikowana na podstawie informacji zawartej w nagłówku;
- ATM jest przezroczysty względem przenoszonej informacji - jest wiec przystosowany do przenoszenia różnych protokołów komunikacyjnych i usług;
- przypisanie komórki ATM konkretnej usłudze odbywa się dynamicznie poprzez nadanie jej odpowiedniego identyfikatora;
- ATM wykorzystuje multipleksowanie statystyczne poszczególnych kanałów, co pozwala na efektywne gospodarowanie łączem;
- przydzielenie identyfikatora konkretnemu połączeniu wymaga fazy nawiązania połączenia;
- jeden, stały rozmiar homogenicznej komórki ATM (rozważano możliwość wprowadzenia kilku rozmiarów komórek) ułatwia proces jej obróbki w węzłach sieci;
- każdemu połączeniu może być przyporządkowana dowolna ilość komórek (o ile pozwala na to dostępna pojemność łącza), co umożliwia realizację dowolnych prędkości transmisji;
- przepływność strumienia komórek dostosowuje się do przepływności transmisyjnej przez wprowadzenie komórek pustych, które w węźle docelowym są pomijane;
- ATM jest skalowalny - może pełnić rolę systemu transmisji zarówno dla sieci WAN, MAN, jak też LAN. W założeniach projektowych ATM uwzględniono implementacje systemów taryfikacji;
- technologia ATM przewiduje obsługę usług izochronicznych (dźwięk, video - również "High Definition TV") z opóźnieniem nie przekraczającym 10 [ms];
- duże szybkości transmisji i silna fragmentacja informacji poważnie ogranicza możliwości monitorowania przepływu danych przez osoby niepowołane, co przyczynia się do poprawy bezpieczeństwa systemu.

Dla pełnego omówienia standardu ATM niezbędne jest umieszczenie go w uniwersalnej strukturze modelu odniesienia dla współdziałania systemów otwartych

JAWNE
Zastrzeżone

(Reference Model for Open System Interconnection). Zgodnie z wcześniejszą uwagą zasadne wydaje się zarysowanie całego modelu odniesienia dla sieci B-ISDN.

Chociaż standard ATM definiuje trzy warstwy, nie jest słuszne przypuszczenie, że odpowiadają one trzem dolnym warstwom modelu odniesienia ISO OSI. Właściwsze jest traktowanie warstwy fizycznej ATM oraz warstwy ATM jako odpowiednika warstwy fizycznej w modelu OSI, natomiast warstwy adaptacji (ang. AAL) jako odpowiednika warstwy łącza danych wg OSI. Wskazuje na to porównanie usług podstawowych realizowanych przez odpowiednie warstwy. Łącze wirtualne oferowane przez warstwę ATM odpowiada warstwie fizycznej. Udostępnia ono usługę transmisji bajtów informacji w konfiguracji punkt-punkt lub punkt-wielopunkt z określoną prędkością. Warstwa AAL oferuje usługi dotyczące dostępu do łącza, przydzielania pasma, nie zapewnia natomiast procedur typowych dla warstwy sieciowej, związanych z routingiem czy adresacją końcówek sieci. Sieci oparte na technologii ATM są konfigurowane jako gwiazda lub hierarchiczna gwiazda (w przypadku połączeń miedzy komutatorami) z komutatorem (swich'em) ATM w centrum. Wyróżnia się dwa typy interfejsów:

- UNI - User/Network Interface, który łączy CPE (ang. Customer Premises Equipment) z siecią ATM czyli odpowiada za styk użytkownik-sieć publiczna. Interfejs UNI powinien zapewniać użytkownikowi podłączenie do globalnej sieci urządzenia typu:
  - terminal szerokopasmowy B-ISDN;
  - urządzenie sieci LAN/MAN przystosowane do współpracy z standardem ATM;
  - komutator - switch – ATM;
- NNI - Network/Network Interface łączący tylko porty switch'ow ATM - tzn. za ich pośrednictwem łączone są sieci i podsieci ATM.

Mówimy tutaj o styku sieć publiczna-sieć publiczna. Podział na dwa rodzaje interfejsów spowodował rozróżnienie dwóch formatów komórek ATM. Istnieje wiele specyfikacji interfejsów UNI/NNI z których każda obejmuje opis stosowanej warstwy fizycznej i charakterystykę warstwy ATM. Warto podkreślić że UNI/NNI zwierają w sobie zagadnienia związane z płaszczyzną kontroli (Control Plane): zarządzania połączeniami, sygnalizacją, itp.

ATM pozwala na osiągnięcie ekonomii skali poprzez integrację różnych rodzajów usług na bazie jednolitej infrastruktury telekomunikacyjnej. Dodatkowo statystyczna natura ATM, oraz jej umiejętność obsługi aplikacji o zmiennym zapotrzebowaniu na pasmo prowadzi do znacznie większej efektywności sieci, w porównaniu z tradycyjną technologią

JAWNE
Zastrzeżone

komutacji łączy. Udostępniając każde połączenie dla aplikacji, sieć zapewnia niezależnie parametry związane z jakością obsługi (QOS - Quality of Service):

- opóźnienie, np. wymagane małe w przypadku interaktywnej transmisji video lub głosu;
- niezawodność, np. wysoka dla obsługi systemów alarmowych, aplikacji CAD/CAM, EDI;
- przepustowość, np. wysoka dla przesyłu danych.

Parametry te pozwalają ustalić atrybuty poszczególnych aplikacji uwzględniając kolejność ich obsługi przez sieć. W przypadku istnienia wielu dróg pomiędzy użytkownikami dają one możliwość wyboru trasy optymalnej (ze względu na opóźnienie, niezawodność, czy prędkość przesyłu).

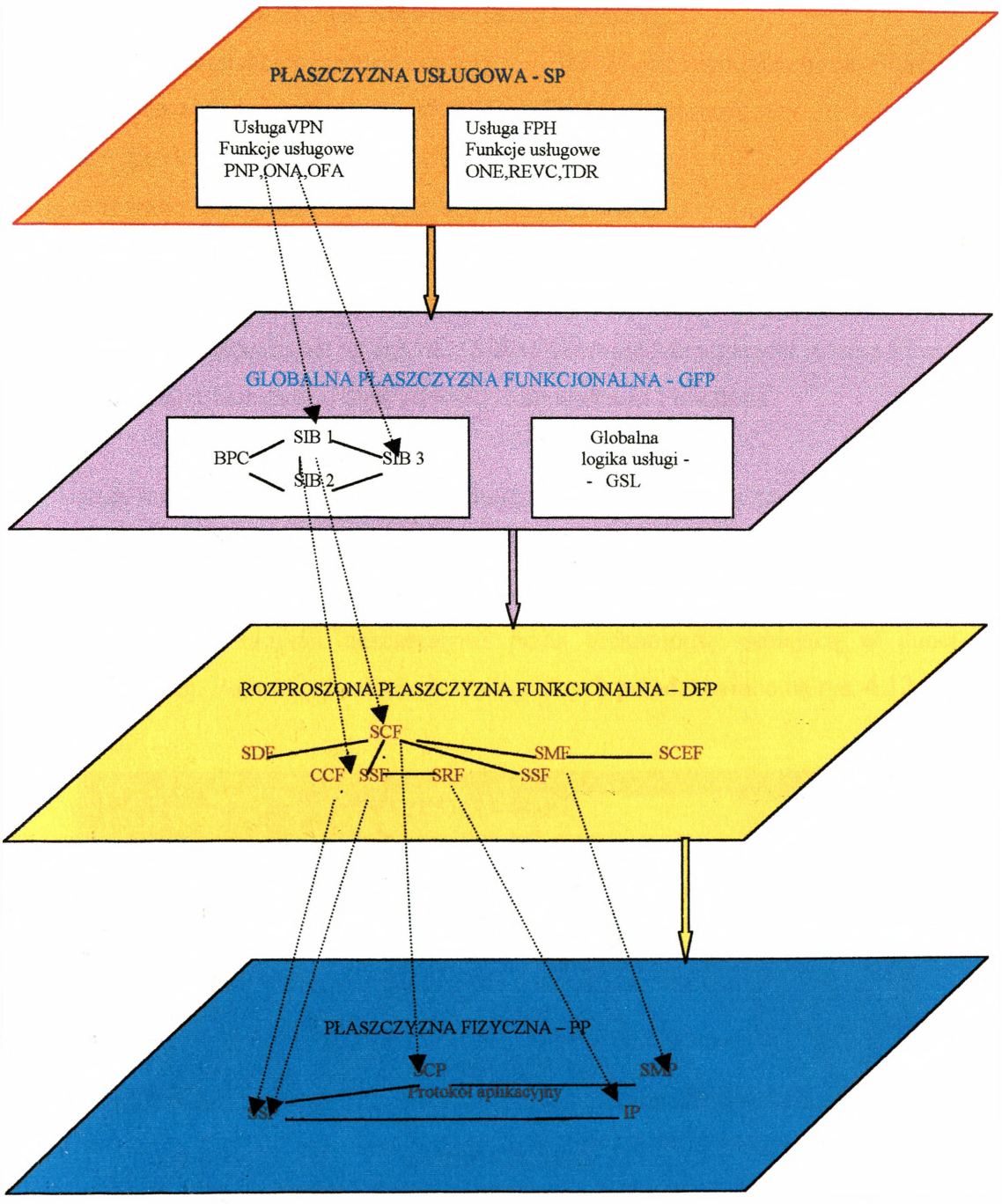
Jakość obsługi oraz zapotrzebowanie na przepustowość ustalane są w wyniku negocjacji między aplikacją użytkownika a siecią, podczas fazy nawiązywania połączenia, kiedy to aplikacja określa swoje żądane (maksymalne) oraz minimalne wymagania. Jeżeli zasoby sieciowe pozwalają spełnić minimalne wymagania użytkownika, zawierany jest kontrakt, którego przestrzeganie obowiązuje obydwie strony. W przeciwnym przypadku sieć odmawia obsługi aplikacji, bez wpływu na aktualnie istniejące połączenia.

Sieci inteligentne (IN – ang. Intelligent Network). Przez pierwsze lata historii rozwoju telefonii głównym problemem było zapewnienie dostatecznej liczby łączy telefonicznych o odpowiedniej jakości, dających możliwość nieograniczonej realizacji połączeń telefonicznych na dowolną odległość. Problem ten stał się podstawowym i na nim skupiała się uwaga wszystkich operatorów sieci telekomunikacyjnych. W miarę rozwoju sieci telefonicznych abonentom przestały wystarczać klasyczne usługi telefoniczne i pojawiło się zapotrzebowanie na coraz bardziej złożone usługi realizowane za pomocą aparatu telefonicznego. W początkowym okresie rozwoju telefonii, „inteligencja". sieci była w dużym stopniu zapewniana przez personel central, który dbał o właściwy przebieg scenariuszy realizacji usługi. Od kilkunastu lat inteligencja jest wprowadzana na wszystkich poziomach sieci, za pomocą specjalizowanych systemów komputerowych i oprogramowania, które są w różny sposób integrowane z podstawową infrastrukturą sieci telefonicznej[47] Istnieje wyróżniona koncepcja techniczna, definiująca znormalizowaną architekturę sieci, zestaw usług i zasady ich kreacji, która jest określana terminem sieci inteligentnej. Model koncepcyjny sieci inteligentnej przedstawiono na rys. 4.11. Warto zauważyć w tym miejscu, że świadczenie usług telekomunikacyjnych przebiega w zasadzie dwutorowo. Z jednej strony jest uwarunkowane postępem technologicznym (usługi dodatkowe w centralach telefonicznych, ISDN), a z drugiej strony zapotrzebowaniem rynku na usługi niestandardowe.

JAWNE
Zastrzeżone

[47] Bromirski M., *Sieci inteligentne w telekomunikacji*, IŁ – O Sz., Warszawa 1999.

JAWNE
Zastrzeżone



Rys.4.11.Przykład modelu koncepcyjnego sieci inteligentnych (IN CM) [48]

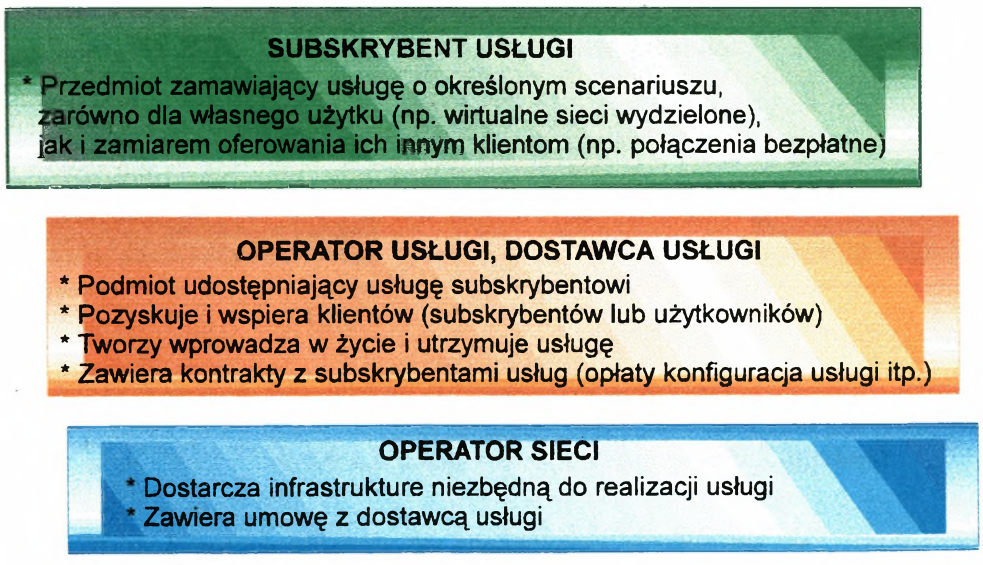
[48] Opracowano na podstawie: Średniawa M., *Sieci inteligentne*, PW - IT, Warszawa1998.

JAWNE
Zastrzeżone

Legenda:

Przedstawiony na rys. 3.9. model koncepcyjny realizuje następujące zadania:
Funkcje komutacji usług – SSF (Service Switching Function);
Funkcje zarządzania zasobami specjalizowanymi – SRF (Specialized Resources Function);
Funkcje sterowania obsługą zgłoszeń – CCF (Call Control Function);
Funkcje dostępu do sieci – CCAF (Call Control Agent Function);
Funkcje sterowania usługami SCF – (Service Control Function);
Funkcje zarządzania danymi usług – SDF (Service Data Function);
Funkcje środowiska kreacji usług – SCEF (Service Creation Environment Function);
Funkcje dostępu do zarządzania usługami – SMAF (Service Managament Access Function);
Funkcje zarządzania usługami – SMF (Service Management Function).

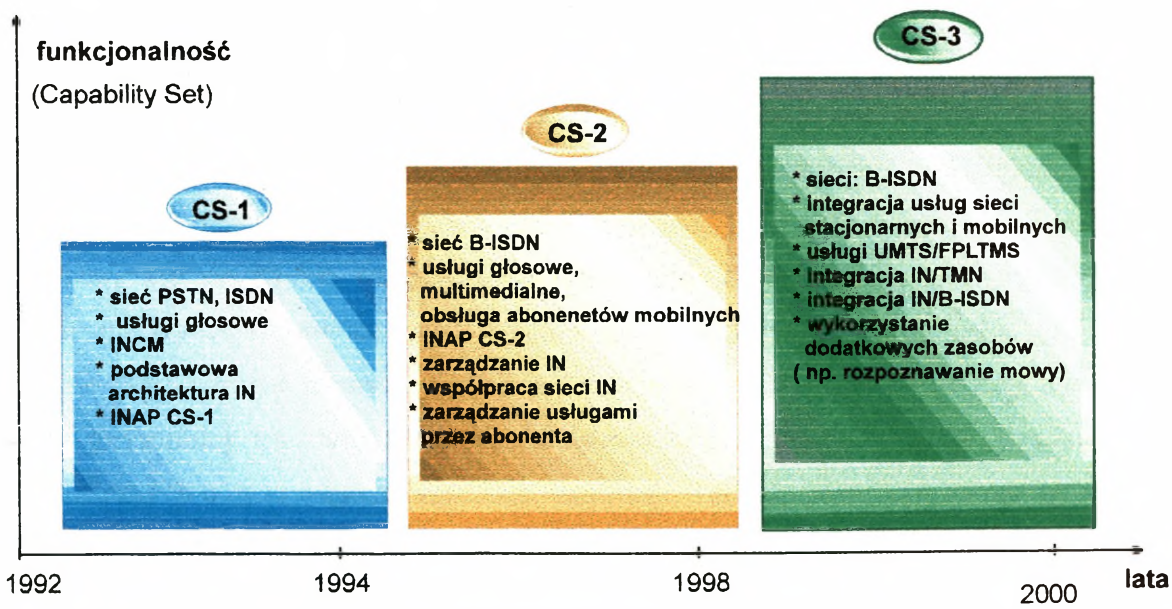
Usługi możliwe dzięki postępowi technologicznemu są ściśle związane z daną centralą i obszarem przez nią obsługiwanym. W przypadku usług niestandardowych, realizowanych na potrzeby klienta, niezwykle ważne jest zapewnienie zasięgu ogólnokrajowego i możliwość poruszania się poza ramami narzuconymi przez technologię istniejącą w danej sieci telekomunikacyjnej. Podmioty w sieciach inteligentnych przedstawiono na rys. 4.12.



Rys. 4.12. Podmioty w sieciach inteligentnych

JAWNE
Zastrzeżone

W efekcie narzuconych zebranych na świecie doświadczeń i analizy zapotrzebowań na nowe niestandardowe usługi telekomunikacyjne stworzono uniwersalną koncepcję, obejmującą rozwiązania techniczne, sposoby ich świadczenia i nadano jej nazwę sieci inteligentnej. Budowa sieci inteligentnej umożliwia operatorowi natychmiastowe reagowanie na zapotrzebowanie rynku telekomunikacyjnego i pełną otwartość na potrzeby klienta, praktycznie niezależnie od użytkowanej infrastruktury telekomunikacyjnej. Zainteresowanie usługami IN wynika przede wszystkim z ich dużego znaczenia dla zastosowań komercyjnych, które mają pośredni lub bezpośredni wpływ na wyniki działalności gospodarczej firmy (abonenta usługi). Pomagają one poprawić wyniki ekonomiczne (zwiększenie obrotu w wyniku poprawy jakości usług i ułatwienia kontaktów z klientami, możliwości telefonicznego składania zamówień, uzyskiwania informacji i pomocy, np. serwisowej, przeprowadzanie teleankiet badających zapotrzebowanie rynku itp.) Etapy rozwoju usług sieci IN na rys. 4.13.



Rys.4.13. Etapy rozwoju usług sieci inteligentnej

Zbiór usług możliwych do świadczenia z użyciem sieci inteligentnej jest bardzo bogaty. W standardach międzynarodowych zdefiniowano obecnie ok. 30 usług. Nie wszystkie usługi cieszą się jednakową popularnością na rynku telekomunikacyjnym. Najbardziej chyba powszechnymi i znanymi usługami są: usługa połączenia bezpłatnego (Freephone) tzw. Infolinia 800 czy usługi audioteksowe o prefiksie 700.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Wirtualna sieć prywatna VPN (ang. Virtual Private Network)

Koncepcja tej sieci polega na wykorzystaniu zasobów sieci publicznej do zapewnienia własności funkcjonalnych sieci wydzielonej. Sieć wydzieloną można traktować jako zamkniętą grupę użytkowników zrealizowaną w sieci publicznej. Najważniejszą własnością VPN jest rozpoznawanie prywatnego planu numeracji i jego translacja na rzeczywiste numery sieciowe. Sieci VPN zapewniają udogodnienia sieci wydzielonych, takie jak:

- prywatny plan numeracji;
- zamknięte grupy użytkowników;
- odbieranie połączeń spoza VPN;
- realizowanie połączeń na zewnątrz VPN;
- realizowanie połączeń wewnątrz VPN;
- możliwość kierowania zgłoszeń;
- możliwość rozliczeń według specjalnych taryf;
- możliwość rekonfiguracji i rozbudowy sieci.

Usługa wirtualnej sieci prywatnej może być przydatna dla potrzeb służb specjalnych i na okres stanów nadzwyczajnych ze względu na swoje unikalne właściwości. Usługa sieci prywatnych (VPN) wychodzi naprzeciw nowym potrzebom telekomunikacyjnym użytkowników współczesnych sieci telekomunikacyjnych. Rozwijane sieci prywatne charakteryzują się zwykle większymi nakładami inwestycyjnymi niż sieci publiczne oraz większymi wymaganiami ich użytkowników do jakości świadczonych usług (głównie w zakresie TD). Z drugiej strony rozwijane nieustannie sieci publiczne cechuje z reguły większy zasięg terytorialny (np. łączność międzymiastowa, międzynarodowa) oraz używanie łączy dalekosiężnych o dużo większej szybkości transmisji. Ten fakt powoduje, że operatorzy sieci publicznych coraz częściej oferują operatorom sieci prywatnych usługi VPN.

VPN zwykle tworzą zasoby sieci publicznej[49] wydzielone dla pojedynczych przedsiębiorstw, lub organizacji, najczęściej z własnym ośrodkiem zarządzania. Logiczne wydzielenie sieci VPN może być zrealizowane na poziomie portu, lub na poziomie całego modułu. VPN oparta jest na sieci publicznej, stąd jej główne cechy zależą od usług oferowanych przez tę sieć

JAWNE

49 - VPN może być logiczną częścią sieci publicznej, lub też może stanowić kombinację logicznej części sieci publicznej i fizycznej części sieci prywatnej. Przykładem sieci VPN jest sieć POLPAK-T.

Zastrzeżone

JAWNE
Zastrzeżone

Usługa VPN pozwala połączyć zalety sieci publicznych i prywatnych. VPN pozwala w sposób logiczny powiązać[50] linie dostępowe i terminale należące do danego użytkownika sieci. Opłaty za usługę VPN zależą przede wszystkim od stopnia wykorzystania ilości i rodzajów zasobów sieci publicznej (zwykle nie zależą od ilości przesyłanych informacji). Własny ośrodek zarządzania (CNM – Customer Network Management) zapewnia użytkownikowi podgląd elementów bezpośrednio wpływających na działanie i wydajność sieci VPN, jak również w pewnym zakresie (przypisanym mu przez operatora sieci publicznej) sterować tymi elementami.Użytkownik VPN może stosować własne zabezpieczenia[51] sprzętowe, lub programowe dla zapewnienia bezpieczeństwa przesyłanych danych. Bezpieczeństwo danych w sieciach VPN jest z reguły większe niż w fizycznych sieciach prywatnych. Powodem tego jest to, że znacznie trudniej jest pozyskać (podsłuchać, przechwycić) dane przesyłane w strumieniach o bardzo dużej szybkości, jak również to, że na łączach międzywęzłowych dane są kodowane (szyfrowane) przez użytkownika VPN wg własnych protokołów.

Ogólnie rzecz biorąc do podstawowych zalet sieci VPN należą:

- niski koszt inwestycyjny;
- niskie ryzyko inwestycyjne;
- pokrycie dużych obszarów (np. sieci WAN).

Do podstawowych wad sieci VPN zalicza się brak elastyczności w tworzeniu rozwiązań sieciowych dla użytkownika. Charakterystyka sieci VPN wynika wprost z charakterystyki sieci publicznej, na bazie której sieć VPN została utworzona podczas gdy sieci prywatne cechują się rozwiązaniami optymalnymi dostosowanymi do specyficznych potrzeb użytkowników.

4.11. Usługi telekomunikacyjne

Rozwój infrastruktury sieciowej jest warunkiem koniecznym do oferowania szerokiej gamy usług, poczynając od prostych usług telefonicznych, aż po usługi szerokopasmowe. Z kolei świadczenie usług telekomunikacyjnych jest podstawową działalnością operatorów telekomunikacyjnych i źródłem ich dochodu.

Definicje i charakterystyki poszczególnych typów usług, zostaną poprzedzone bardziej formalnym opisem usługi telekomunikacyjnej. Nie istnieje żadna ścisła, formalna definicja

---

50 - powiązanie logiczne może być zrealizowane przez takie cechy jak zamknięte grupy użytkowników, zarządzanie siecią klienta, dostarczanie usług specjalizowanych, specjalne rozliczanie usług itp.

51 - zabezpieczenia oferowane przez operatora publicznego z uwagi na ich powszechność, z reguły nie zapewniają właściwego stopnia bezpieczeństwa.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

usługi. Jednak dla potrzeb niniejszej pracy, można następująco zdefiniować usługę telekomunikacyjną.

Pod pojęciem usługi telekomunikacyjnej, rozumiemy zbiór wszelkich zasobów sieci, środków oraz narzędzi służących przeniesieniu informacji, oferowany użytkownikowi sieci telekomunikacyjnej dowolnego typu. Definicja ta ma charakter ogólny, jednak w wystarczający sposób precyzuje cel usługi, środki służące jej realizacji oraz jej adresata.Istnieje wiele możliwości klasyfikacji usług telekomunikacyjnych.

Usługi te mogą być dzielone ze względu na sposób przekazywania danych (np. usługi telefoniczne - głosowe, transmisja danych, przesyłanie obrazu itd.), ze względu na techniki używane do ich realizacji[52]. Jedną z możliwości jest też klasyfikacja funkcjonalna usług telekomunikacyjnych. Według niej usługi możemy podzielić na:

- usługi przenoszenia zapewniające transmisje informacji pomiędzy stykami użytkowników sieci;
- teleusługi polegające na transmisji informacji pomiędzy użytkownikami sieci, zapewniające dodatkowo wszystkie funkcje terminala, bądź stacji abonenckiej;
- usługi dodatkowe stanowiące modyfikację, bądź rozwinięcie poprzednio klasyfikowanych usług.

Z każdym typem usługi, skojarzona jest pewna liczba atrybutów, charakteryzująca daną usługę. Usługi przenoszenia mogą być charakteryzowane przez atrybuty związane z transmisją, bądź przez parametry określające sposób dostępu do fizycznego medium, protokół dostępu, typ interfejsu, parametry związane z jakością usługi itd. Na stan infrastruktury telekomunikacyjnej kraju, mają wpływ nowe techniki i technologie, których zastosowanie umożliwia dostęp do nowych usług.

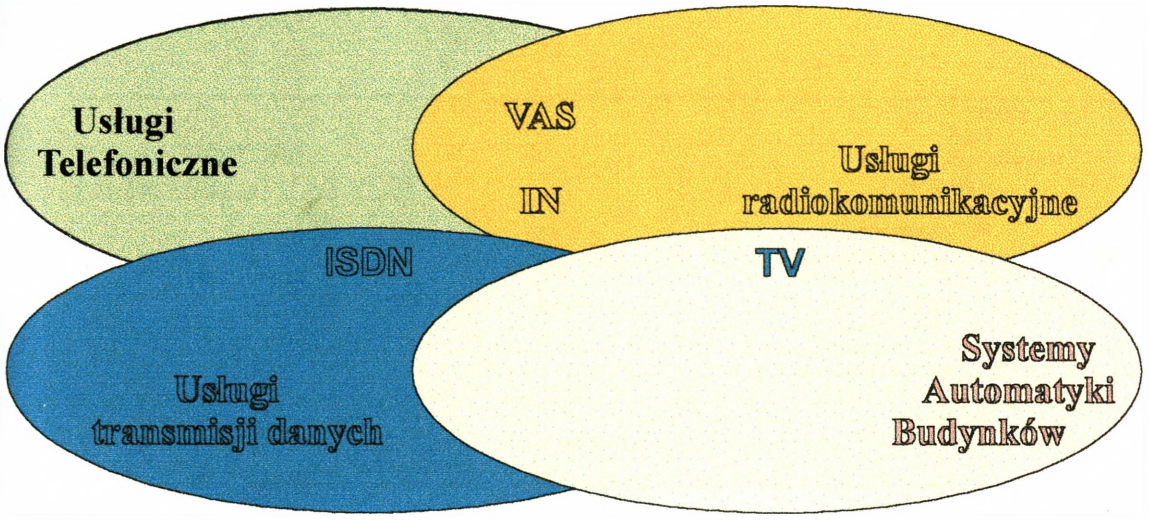
Teleusługi są ponadto charakteryzowane przez atrybuty określające styk użytkownika z urządzeniem (wyższe warstwy modelu odniesienia OSI). Na rys. 4.14. przedstawiono ogólną klasyfikację usług w sieciach publicznych. Na przykład z usługami świadczonymi przez sieć ISDN, są skojarzone atrybuty określające wymagania związane z jakością usługi. Na rys. 4.15. przedstawiono ogólną klasyfikacja usług w sieci ISDN.

Usługi oferowane przez operatorów sieci zaprezentowano podając podstawowe określenia, najpopularniejszych usług telekomunikacyjnych:

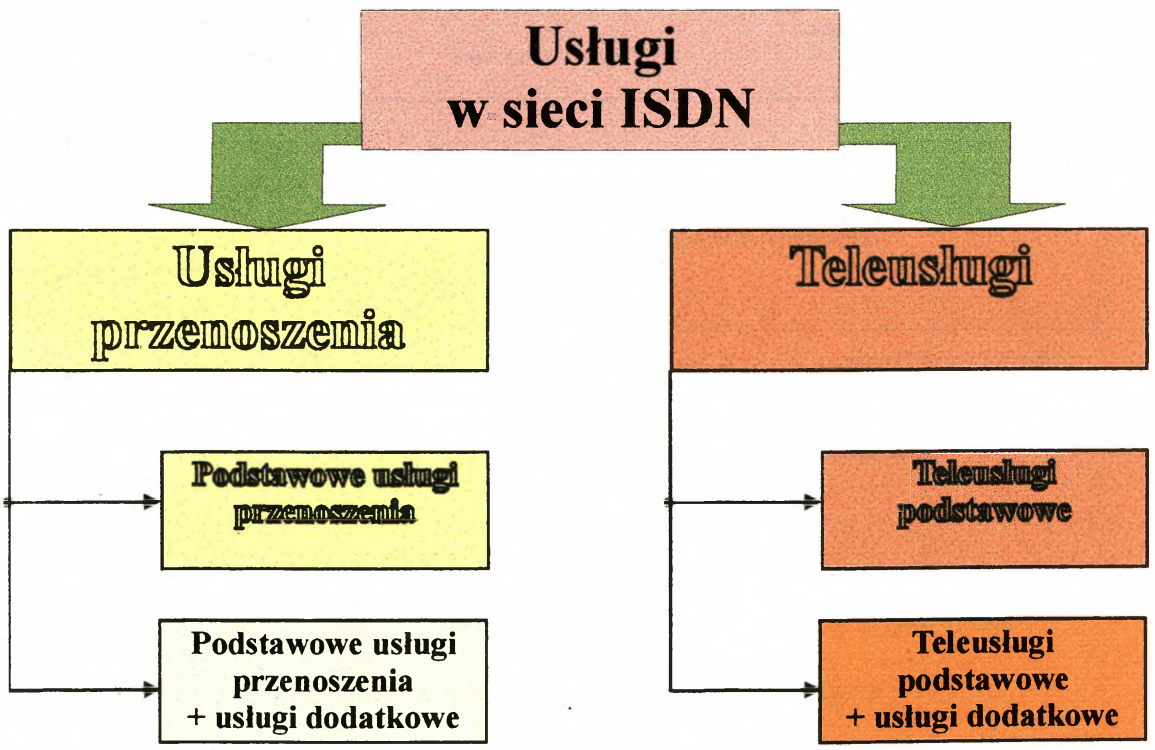
1. Telefonia - najpopularniejsza usługa telekomunikacyjna polegająca na dwukierunkowym przesyłaniu głosu w paśmie 3,1 kHz (300-3400 Hz).
2. Telefaks - transmisja tekstu lub grafiki, wykorzystująca standardowe łącza telefoniczne.

[52] Ziemski W., *Usługi sieci inteligentnej*, TP S.A. Warszawa 1998

JAWNE
Zastrzeżone



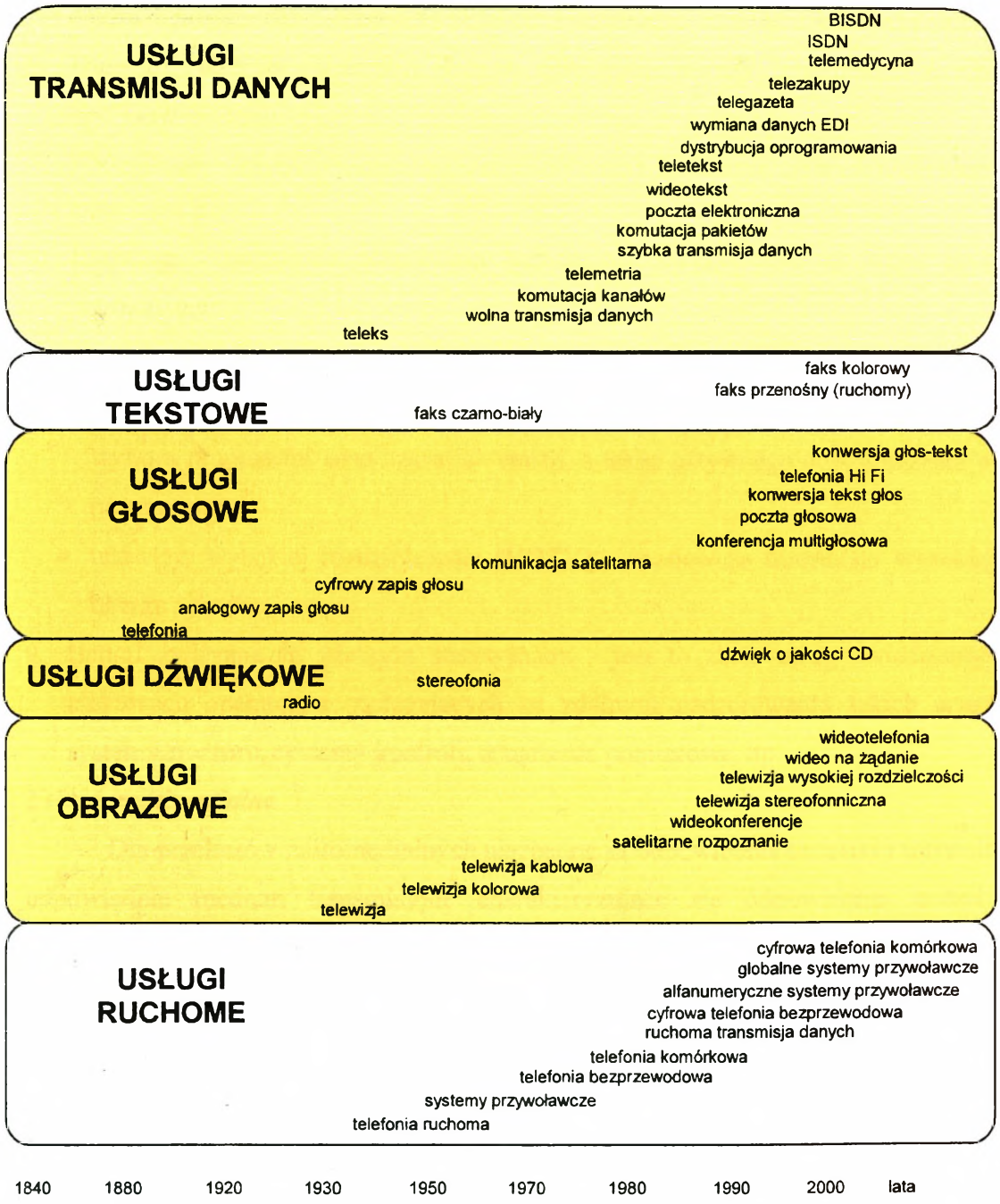
Rys. 4.14. Ogólna klasyfikacja usług oferowanych w sieciach publicznych (wariant)



Rys. 4.15. Ogólna klasyfikacja usług w sieci ISDN (wariant)

JAWNE
Zastrzeżone

Klasyfikację klasycznych usług telekomunikacyjnych przedstawiono na rys. 4.16.



Rys.4.16. Klasyczne usługi telekomunikacyjne

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

3. Teleks i teleteks - prostsza (teleks) i bardziej rozwinięta wersja (teleteks) transmisji znakowej.
4. Wideoteks - usługa umożliwiająca dostęp do oddalonych baz danych za pomocą sieci telefonicznej (usługa ta nazywana Minitel, jest bardzo popularna we Francji).
5. Poczta elektroniczna (e-mail) - przesyłanie wiadomości między użytkownikami.
6. Transmisja danych - transmisja danych cyfrowych między terminalami użytkowników sieci (komputerami).
7. Wideofonia - usługa pozwalająca na jednoczesną transmisję głosu i ruchomego obrazu rozmówców.
8. Telewizja - transmisja rozsiewcza ruchomego obrazu; poza telewizją standardową rozróżniamy:
   - telewizję kablową (CTV) - w której transmisja obrazu odbywa się przez sieć kablową;
   - telewizję interaktywną (ITV) - w której użytkownik ma dużo większą możliwość wyboru programów oraz czasu ich emisji, a także aktywnego uczestniczenia w samych programach;
   - telewizję wysokiej rozdzielczości (HDTV) - rozsiewcza transmisja wysokiej jakości obrazu i fonii.
9. Usługi związane ze zdalnym sterowaniem - jest to zbiór usług świadczonych przez niektórych operatorów, polegających na zdalnym nadzorowaniu takich urządzeń, jak systemy nadzoru, systemy kontroli, urządzenia pomiarowe, itp.

Usługi multimedialne

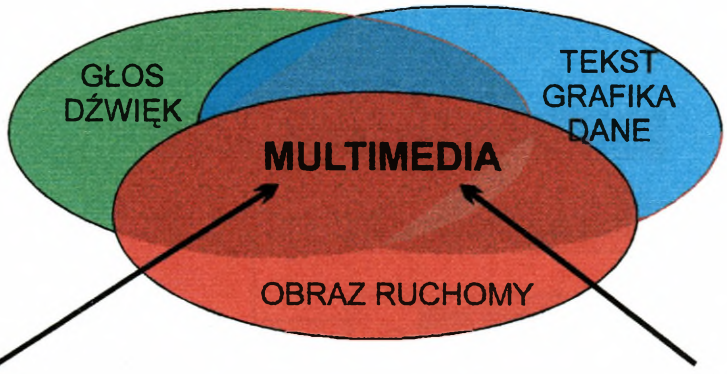
Dla przekazów multimedialnych niezbędne są odpowiednie techniki i technologie oraz odpowiednie medium transmisyjne charakteryzujące się odpowiednią przepływnością i zapewniające określone zasięgi łączności, przedstawia rys. 4.17.

Dla przekazów szerokopasmowych z wykorzystaniem technik i technologii SDH, ATM, Fast Ethernet, Gigabit Ethernet i innych wymagane jest odpowiednie medium transmisyjne zapewniające osiągnięcie dużych przepływności sygnału. Takim medium transmisyjnym jest światłowód, który zapewnia "nieograniczoną przepustowość" w stosunku do istniejących technik transmisyjnych.

Dodatkową zaletą światłowodów jest ich odporność na elektromagnetyczne zakłócenia zewnętrzne i brak emisji ujawniającej sygnału na zewnątrz. Ograniczeniem do ich stosowania są przede wszystkim wysokie jeszcze ceny elementów aktywnych okablowania światłowodowego.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone



USŁUGI	
Istniejące	- dystrybucja TV - płatna telewizja PPV - telefonia POST - wideotelefonia
Nowe	- wideo na żadanie - wideokonferencje - telezakupy - praca w domu - zdalne nauczanie - telemedycyna - usługi bankowe - reklama i marketing - interaktywna telewizja - interaktywna rozrywka (gry)

TECHNOLOGIE	
TECHNIKA	- cyfryzacja - kompresja - kodowanie - kompensacja - kasowanie echa - modulacja - komutacja
SIECI	- transportowe: ATM, SDH/ SONET - dostępowe: ISDN, ADSL, HFC, FITL (PON, APON), CATV, WLL(RLL)
NOWE WYROBY	- wideo kodery MPEG - modemy szerokopasmowe - wideoserwery - stacje czołowe TV - przełączniki ATM - przystawki multimedialne - rozgałęźniki sprzęgacze

Rys.4.17. Usługi i technologie telekomunikacyjne

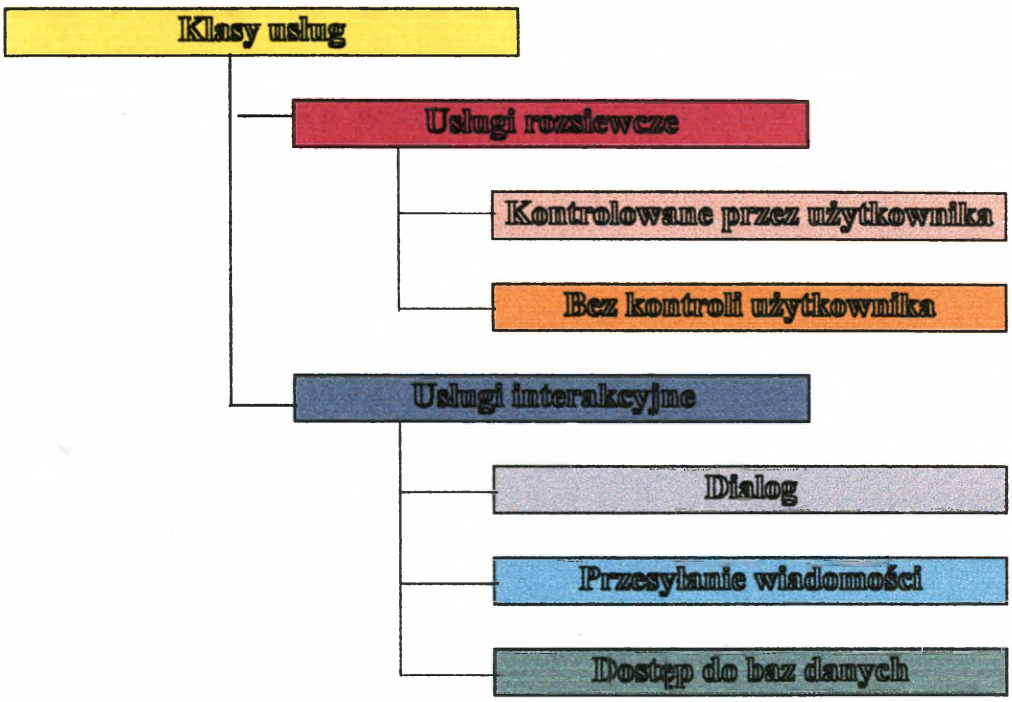
Należy również, wyróżnić ogólną klasyfikację usług telekomunikacyjnych pod względem klasy świadczonych usług a mianowicie:

- usługi rozsiewcze;
- usługi interakcyjne.

Usługi rozsiewcze polegają na jednokierunkowym przesyłaniu strumienia informacji z centralnego źródła do wielu użytkowników. W grupie usług nie kontrolowanych przez użytkownika, liczba odbiorców informacji jest dowolna, zaś użytkownik nie może wpływać na to jaka informacja jest mu przesyłana (np. telewizja). Z kolei w usługach rozsiewczych, kontrolowanych przez użytkownika odbiorcy mogą wybierać typ informacji oraz moment rozpoczęcia tej transmisji (przykładem jest telewizja na żądanie - Video on Demand).
Omawiane klasy usług przedstawiono na rys. 4.18.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone



Rys. 4.18. Klasy usług telekomunikacyjnych (wariant)

Usługi interakcyjne pozwalają na łączność dwustronną, w której komunikujące się ze sobą terminale (bądź osoby), mają podobne możliwości wysyłania informacji. Usługi te mogą być trojakiego rodzaju:

- usługi dialogowe - najczęściej telefoniczne;
- usługi umożliwiające przesyłanie wiadomości wg schematu zapamiętaj i przekaż (tzw. poczta elektroniczna);
- interakcyjny dostęp do baz danych, gdzie użytkownik może przeglądać zbiory informacji zebrane w bazach danych.

4.12. Rozbudowa infrastruktury telekomunikacyjnej kraju w aspekcie potrzeb obronności

Kierowanie podczas użycia nowoczesnych wysoce skutecznych systemów technicznych i uzbrojenia w stanach nadzwyczajnych staje się niemożliwe przy wykorzystaniu tradycyjnych dotychczasowych środków łączności /telefon, dalekopis, telefax,

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

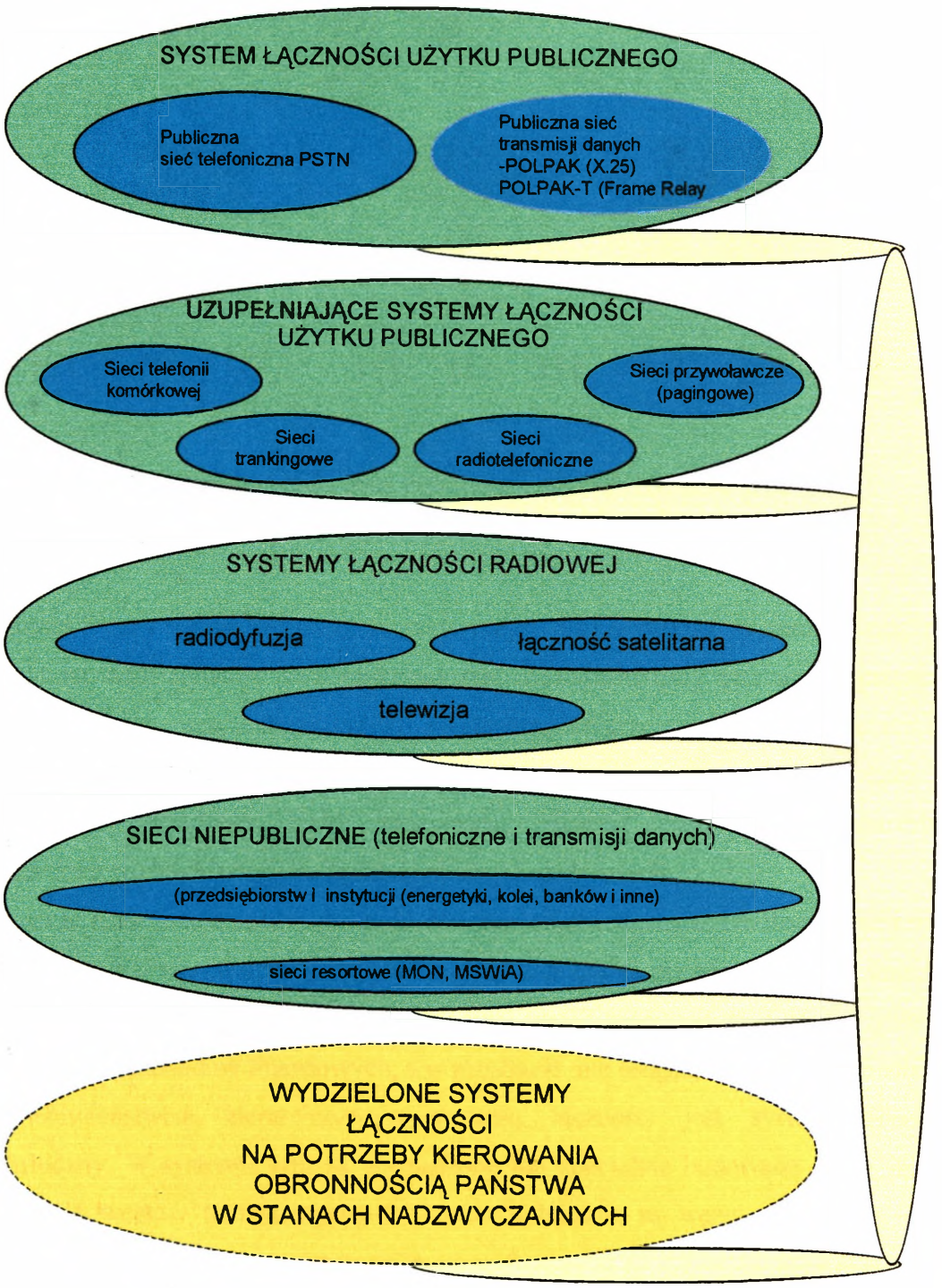
itp./. Niezbędna jest zatem automatyzacja procesów wykrywania, rozpoznania i wskazywania celów do zniszczenia oraz wypracowywania komend i przekazywania rozkazów. Duże nadzieje w pracach nad doskonaleniem dowodzenia wiąże się z szeroko pojętą komputeryzacją systemów dowodzenia. Uważa się, że komputery w połączeniu z nowoczesnymi systemami łączności /telekomunikacyjnymi/ mogą w szerokim zakresie wesprzeć pracę osób funkcyjnych organów kierowania najwyższej władzy i administracji państwa oraz sił zbrojnych, w tym dowódców i oficerów sztabu, szczególnie usprawnić i przyspieszyć większość przedsięwzięć o charakterze kalkulacyjno - biurowym i informacyjnym. Dlatego też potrzeby i wymagania wszystkich organów kierowania obronnością kraju powinien zaspokajać system telekomunikacyjny państwa. W systemie tym zachodzą istotne zmiany, zdecydowanie przyspieszono zwłaszcza proces przejścia na technikę cyfrową sieci telekomunikacyjnej kraju oraz budowę elektronicznych central telefonicznych.

Wykorzystanie sieci telekomunikacyjnej to także problem działania systemu łączności w nowych warunkach. Budowa i doskonalenie systemu łączności kierowania obronnością państwa i dowodzenia siłami zbrojnymi w celu dostosowania go do obecnych potrzeb wymaga podejścia interdyscplinarnego. Te działania stosownie do nowych warunków i przewidywanych potrzeb, stają się obecnie jednym z najważniejszych problemów obronności państwa. Miejsce w systemie łączności państwa i powiązanie systemu łączności kierowania obronnością z innymi systemami i sieciami przedstawiono na rys. 4.19.

Jest to następstwem konieczności przebudowy systemu łączności kierowania obronnością wynikającej ze zmiany warunków funkcjonowania dotychczasowego systemu, który był dostosowany do wykonywania zupełnie innych zadań przez siły zbrojne, głównie działań zaczepnych prowadzonych na froncie zewnętrznym przez siły koalicyjne.

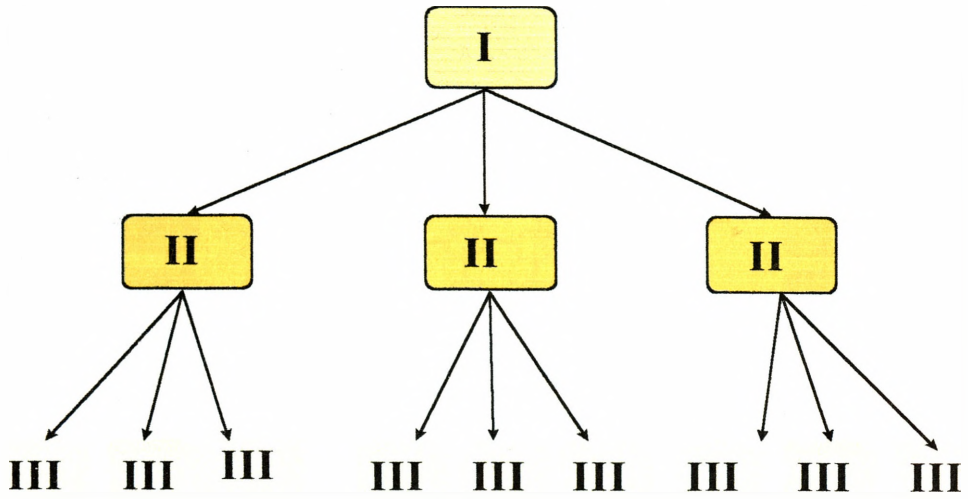
Sieć telekomunikacyjna jest rozwinięta w sposób nierównomierny. Ogólnie można stwierdzić, że jej stan nie jest zadowalający zarówno pod względem ilościowym, jak i jakościowym (niewłaściwa struktura organizacyjna, mała skuteczność obrony przed rozpoznaniem i obezwładnieniem radioelektronicznym, technika nawet z lat siedemdziesiątych i osiemdziesiątych, nawet jeszcze - analogowa). Eksploatowany system łączności jest mało spójny organizacyjnie i technicznie oraz podzielony na zbyt wiele podsystemów. Stwarza znaczne utrudnienia w przekazywaniu informacji i niedogodności w organizowaniu łączności. Obieg informacji nijednokrotnie oparty jest na przestarzałym (pochodzącym z importu) sprzęcie. Sieci łączności niektórych resortów i instytucji posiadają jeszcze strukturę hierarchiczną przedstawioną na rys. 4.20

JAWNE
Zastrzeżone



Rys.4.19. Możliwości połączenia systemu łączności na potrzeby kierowania obronnością państwa z innymi systemami i sieciami (wariant rozwiązania)

JAWNE
Zastrzeżone



Rys.4.20. Schemat hierarchicznej organizacji systemu łączności (wariant)

Hierarchiczny system łączności charakteryzuje: mała podatność na automatyzację; mała odporność na oddziaływanie radioelektroniczne; niezadowalający poziom bezpieczeństwa łączności na skutek niepożądanej emisji elektromagnetycznej; niepodatność na unifikację i miniaturyzację; stosowanie starych technologii (znaczne pobory mocy i duże masy poszczególnych urządzeń); duża awaryjność, złożona obsługa i diagnozowanie; zaangażowanie wielkich zespołów ludzi do obsługi i eksploatacji.

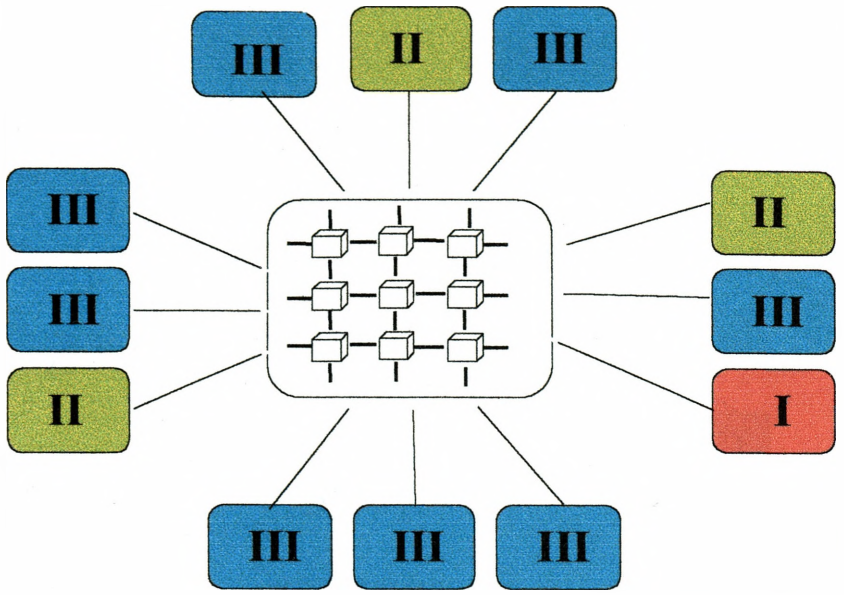
Sieci te funkcjonują opierając się na różorodnych rozwiązaniach technicznych i różnym sprzęcie (np. nowo wprowadzone urządzenia łączności nie są przystosowane do współpracy z obecnie eksploatowanymi). Stwarza to również możliwości znacznej utraty informacji, powoduje wzrost nakładów finansowych, a w rezultacie nie osiąganie zakładanych celów.

Przeciwieństwem hierarchicznego systemu łączności jest system sieciowy - nieheirarhiczny. W systemie tym są wyznaczone lub specjalnie budowane węzły łączności pełniące rolę wezłów tranzytowych, do któreh dołączane są węzły dostępowe – węzły łaczności użytkowników. W praktycznej realizacji oznacza to, że w stacjonarnym systemie łączności każdy węzeł użytkowników jest jednocześnie tranzytowom i dostępowo – końcowym. Wszystkie węzły łączności posiadają taki sam status. Systemy takie w literaturze przedmiotu nazywane są systemami sieciowymi lub kratowymi (siatkowymi).

Dlatego celowym jest utworzenie na obszarze kraju kompleksowej i zintegrowanej sieci łączności o niehierarchicznej strukturze siatkowej, pozbawionej wad systemu hierarchicznego. Sieć łączności przedstawiono na rys.4.21.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone



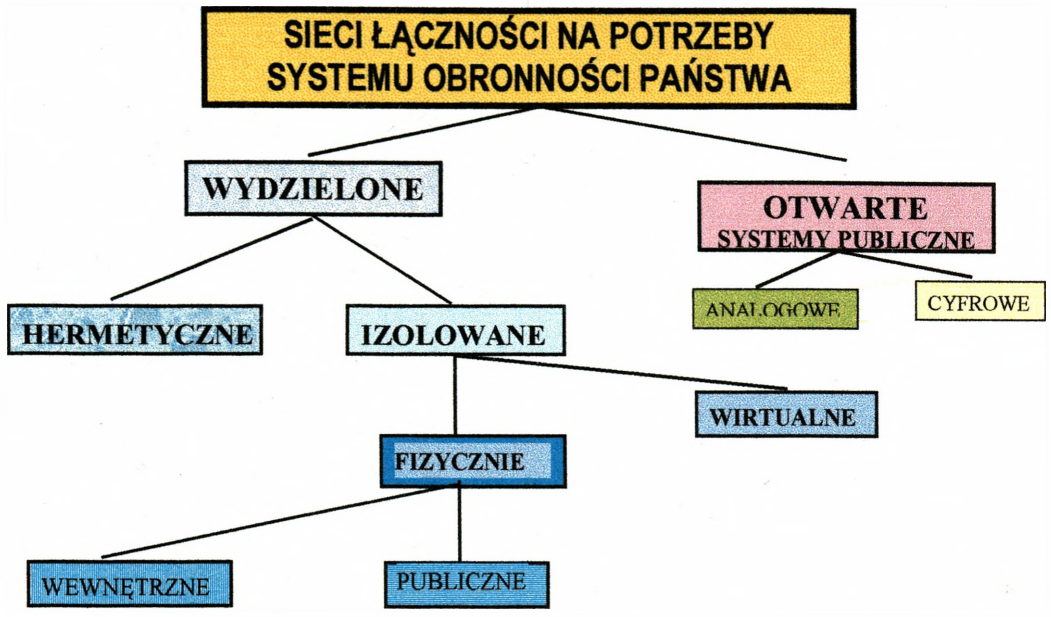
Rys.4.21. Schemat niehierarchicznej organizacji systemu łączności (wariant)

Podstawową cechą określającą stopień przydatności danego systemu telekomunikacyjnego na potrzeby administracji kraju i systemu obronności jest możliwość jego hermetyzacji czyli zapewnienia określonym abonentom priorytetowego dostępu do świadczonych usług. Stosując to kryterium dokonano próby klasyfikacji najpowszechniej stosowanych w kraju sieci łączności i przedstawiono na rys. 4.22. Wszystkie systemy zostały podzielone na dwie podstawowe grupy: systemy wydzielone i publiczne. W zależności od sposobu wydzielania z ogólnej infrastruktury telekomunikacyjnej kraju sieci, wydzielono sieci izolowane i hermetyczne.

Cechą sieci hermetycznych jest to, iż tworzą zamknięte systemy, całkowicie niedostępne dla innych abonentów. Sieci takie, poprzez powszechne stosowanie urządzeń kryptograficznych, umożliwiają użytkownikom prowadzenie tajnej korespondencji. Przedstawicielami takiego systemu jest militarny system łączności STORCZYK i planowana na potrzeby systemu obronności tzw. *sieć awaryjna.*

Została powołana Komisja ds. Planowania Łączności Cywilnej NATO (CCPC), która przewiduje istnienie w krajach członkowskich NATO narodowych systemów awaryjnych. Zaleca jednocześnie, aby systemy te ze sobą współpracowały. Sieci awaryjne realizowane są więc głównie jako cyfrowe systemy krajowe wąskopasmowe z kanałem abonenckim o przepływności 16 kbit/s z modulacją delta. Normy EUROCOM określają parametry styków i sygnalizacji tych sieci.

JAWNE
Zastrzeżone



Rys.4.22. Klasyfikacja sieci łączności (wariant)

W Polsce proponowana jest budowa cyfrowej wąskopasmowej sieci łączności spełniającej podstawowe zalecenia norm EUROCOM i pełniąca rolę krajowej sieci awaryjnej.

Sieć ta przeznaczona będzie głównie do zapewnienia bezpiecznej wymiany informacji (prowadzenia niejawnej korespondencji) pomiędzy ogniwami naczelnych i wojewódzkich organów władzy i administracji państwowej w sytuacjach wyjątkowych, w czasie kryzysu i wojny.

Do najistotniejszych cech tego systemu należy zaliczyć:

- niskie koszty eksploatacji;
- duża elastyczność konfiguracji sieci;
- kompatybilność sprzętową i programową z urządzeniami stosowanymi w specjalnych sieciach systemów militarnych, w tym również SZ RP;
- możliwość stosowania w systemie indywidualnych i grupowych urządzeń kryptograficznych;
- mobilność systemu i współpraca z urządzeniami radiodostępu z zachowaniem ciągłości utajniania;
- stosowanie wielostopniowego priorytetu dostępu abonentów do zasobów sieciowych systemu;

- w sytuacjach awaryjnych - możliwość pracy plezjochronicznej central bez konieczności ich synchronizacji z krajowym systemem dystrybucji zegara.

W celu zwiększenia efektywności ekonomicznej eksploatacji sieci awaryjnej, przewiduje się, że powinna być ona eksploatowana również w czasie pokoju, na potrzeby centralnych i wojewódzkich organów władzy i administracji państwowej[53].

Sieć użytku publicznego jest siecią o zasięgu ogólnokrajowym i nadaje się do wykorzystania dla potrzeb obronnych. Przykładem wykorzystania tej sieci może być wymieniona wcześniej usługa wirtualnej sieci prywatnej VPN, która zapewni stworzenie wydzielonej grupy użytkowników z własną taryfikacją i planem numeracji.

Systemy mogą być izolowane fizycznie lub programowo. Sieci izolowane fizycznie, bazując na dzierżawionych zasobach transmisyjnych infrastruktury kraju, posiadają własne centra komutacyjne. Przykładem wewnętrznych sieci izolowanych fizycznie jest między garnizonowy system łączności MON, system MSWiA, system kolei itp.

System łączności państwa powinien być udoskonalany i unowocześniany w zakresie:

- zwiększania żywotności i niezawodności;
- zwiększania szybkości i ilości przekazywanych informacji;
- zapewnienia łączności nowo powstałym elementom systemu kierowania;
- umożliwienia łatwego, szybkiego (kompleksowego) dowiązania i połączenia polowego systemu łączności z systemem telekomunikacyjnym kraju;
- ochrony przekazywania informacji.

Stan aktualny systemu łączności na potrzeby kierowania obronnością państwa w stanach nadzwyczajnych przedstawia się następująco.

1. Siły zbrojne i administracja państwowa nie dysponują praktycznie zintegrowanym, kopleksowym, nowoczesnym i utajnionym systemem łączności do przekazu informacji niejawnych.
2. Brak spójnych systemów utajniających stwarza poważne zagrożenia przecieków informacji będących często tajemnicą państwową bądź gospodarczą. Sytuacja taka powoduje realizowanie rozproszonego rozwoju różnych systemów łączności przez poszczególne resorty i instytucje. Poczynania te charakteryzują się dwoma zasadniczymi cechami:
   - są wymuszane specyfiką specjalnych zadań, przy jednoczesnym braku wyspecjalizowanego oferenta wymaganej usługi telekomunikacyjnej,

[53] W Szwecji - ConTakt, w Danii - Atoko D, w Wielkiej Brytanii - Ptarmingan, w USA - Tri Tack, DSN.

- nie są ze sobą kompatybilne ze względu na brak określonej koncepcji systemowej i koordynacji działań w tym zakresie.

3. Brak w kraju, określonego przepisami organu koordynującego wszelkie działania w tej materii. Ustawa o łączności z 1990 jaki i ustawa z dnia 21 lipca 2000 r. „Prawo telekomunikacyjne", stwarzają warunki przyspieszenia rozbudowy systemu telekomunikacyjnego kraju, jednak nie gwarantują w pełni interesów i potrzeb organów kierowania państwem oraz dowodzenia Siłami Zbrojnymi RP..
4. Kierowanie i zarządzanie siecią jest mało efektywne i nie spełnia właściwej roli w systemie telekomunikacyjnym kraju.
5. Nowa technika i technologia systemów łączności nie jest w pełni przystosowana do współpracy z dotychczas stosowanym sprzętem polowym resortu MON oraz MSW i A.
6. Brak synchronizacji działań inwestycyjnych w poszczególnych resortach, budowa własnych często dublujących się sieci opartych o różne rozwiązania techniczne, nie tylko nie osiąga zakładanych celów, lecz powoduje również niewspółmierny wzrost nakładów finansowych z budżetu państwa.

Taki stan łączności rzutuje również na rejony stanowisk kierowania szczególnie naczelnych oraz centralnych organów władzy i administracji państwowej.

Współczesne tendencje rozwoju sieci telekomunikacyjnych na świecie i w Polsce, związane z integracją usług, wymuszają wartościowanie takich ich cech jak niezawodność, żywotność, skuteczność, elastyczność, podatność na blokadę itp.

Wszystkie te cechy są szczególnie istotne w systemie łączności na potrzeby kierowania obroną państwa i dowodzenia siłami zbrojnymi. System ten powinien odznaczać się:

- dużą niezawodnością i wiernością transmisji danych między elementami
- zautomatyzowanego systemu dowodzenia i skomputeryzowanymi miejscami pracy osób funkcyjnych;
- gwarancją automatycznego uzyskania połączeń bezpośrednich i obejściowych;
- odpornością na przypadkowe i celowe zakłócenia radioelektroniczne;
- zdolnością przekazywania informacji niejawnych z określoną mocą kryptograficzną;
- możliwością przesyłania sygnałów alarmowych oraz zdolnością realizacji szybkiej łączności operacyjnej w formie pisemnej z automatycznym jej zobrazowaniem i dokumentowaniem możliwością zapewnienia bezpośredniej, konferencyjnej stanowisk dowodzenia i kierowania;

- możliwością wymiany informacji opracowanej w planowanych systemach zautomatyzowanego dowodzenia i kierowania;
- możliwością kontroli i automatycznej rejestracji stanu eksploatowanych łączy.

System łączności zawierający w sobie wszystkie te cechy, to nowoczesny cyfrowy system teletransmisyjny i komutacyjny, który mógłby spełniać równolegle funkcje systemu komercyjnego i specjalnego. W związku z powyższym konieczna jest koncentracja wysiłków państwa, skupiona na budowie zintegrowanej sieci telekomunikacyjnej, która ujęta w określony system, pozwoli na zabezpieczenie niezawodnej, utajnionej łączności, niezbędnej do realizacji wszystkich procesów związanych z zarządzaniem państwem, jego bezpieczeństwem zewnętrznym i wewnętrznym zarówno w czasie pokoju jak i wszelkich sytuacjach kryzysowych. System ten, pod nazwą Narodowy lub Krajowy System Łączności, oparty byłby na istniejącej i rozbudowywanej cyfrowej sieci telekomunikacyjnej kraju, powinien zapewnić użytkownikom specjalnym łączność telefoniczną, telegraficzną, telefaksową i teleinformatyczną w systemie utajnionym, zgodnie z najnowocześniejszymi standardami światowymi w oparciu o krajową myśl techniczną.

Skoordynowane działania organizacyjno-techniczne umożliwią:

- budowę sieci transmisyjnej o znacznie większej przepustowości. Uzyskany w ten sposób większy współczynnik wykorzystania linii pozwoli obniżyć sumaryczną przepustowość sieci, zmniejszając jednostkowe koszty jej eksploatacji;
- organizację systemu o dużej elastyczności, stwarzając w ten sposób warunki do dowolnego powiązania użytkowników specjalnych zarówno w relacjach międzymiastowych jak i międzynarodowych;
- uzyskanie większej żywotności sieci, zwiększając przez to odporność zarówno na czynniki zewnętrzne jak i ekstremalne wahania obciążeń systemu;
- wykorzystanie jednego operatora systemu, odpowiedzialnego za eksploatację całej sieci oraz świadczenie usług na rzecz jej użytkowników zarówno w czasie pokoju jak i wojny.

Nie bez znaczenia jest również fakt połączenia wszystkich potencjalnych użytkowników w ramach jednego systemu, umożliwi to:

- wykorzystanie baz danych poszczególnych instytucji w momencie realizacji zadań państwowych;
- scentralizowane kierowanie wszystkimi służbami realizującymi określone zadania w danym regionie lub na terenie całego kraju;

JAWNE
Zastrzeżone

- tworzenie wydzielonych warstw sieci, w ramach ogólnego systemu, z pełną gwarancją ochrony ich zasobów informacji.

4.13. Bezpieczeństwo systemów telekomunikacyjnych

W ostatnich latach nastąpił w Polsce gwałtowny rozwój infrastruktury telekomunikacyjnej. Sytuacja ta umożliwiła szerokie wykorzystywanie w procesach zarządzania, kierowania i dowodzenia nowoczesnych technik przekazu i przetwarzania informacji. Znaczenie obiegu informacji w instytucji państwowej, przedsiębiorstwie, organizacji militarnej, czy też koncernie działającym na rynku globalnym, porównać można do znaczenia krwioobiegu w organizmie ludzkim. Każda organizacja dysponująca informacjami, wykorzystuje do ich przechowywania, przetwarzania i przesyłania systemy teleinformacyjne.[54]

Przyszli użytkownicy systemów, urządzeń czy też oprogramowania, które mają służyć do przechowywania, przetwarzania i przesyłania informacji o charakterze niejawnym, muszą mieć pewność, że wyrób który zamierzają kupić spełnia wymagania bezpieczeństwa teleinformacyjnego. Wiara w werbalne zapewnienia producentów czy dealerów o bezpieczeństwie teleinformacyjnym tej kategorii wyrobów jest niewystarczająca. Użytkownik powinien polegać na wynikach formalnej i bezstronnej oceny, dokonanej przez uprawniony do tego organ.

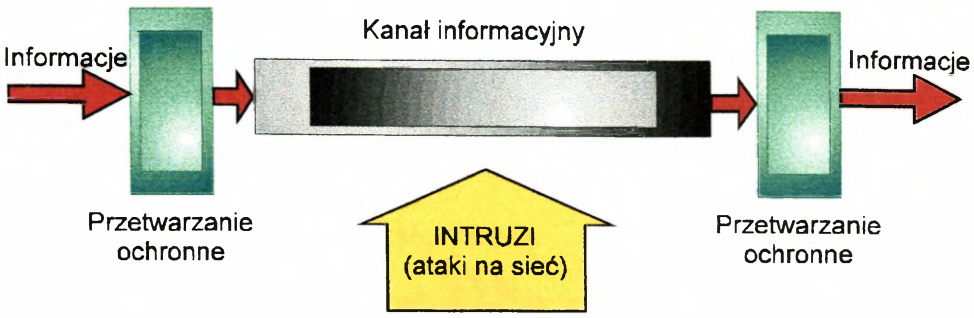
Ocena wyrobu wymaga dobrze zdefiniowanego kryterium oceny zabezpieczenia oraz istnienia jednostki certyfikującej, uprawnionej do wydania potwierdzenia, że oceny dokonane przez laboratorium badawcze zostały przeprowadzone właściwie. Ocena możliwości zabezpieczających systemu może być rozpatrywana jako część większej formalnej procedury przyjęcia systemu teleinformacyjnego do stosowania w konkretnym środowisku.

Bezpieczeństwo sieci to pojęcie obejmujące zarówno bezpieczeństwo informacji krążących pomiędzy węzłami tej sieci, jak i tych zgromadzonych w bazach danych dostępnych za pośrednictwem sieci (Rys. 4.23).

---

[54] Informacja - jakakolwiek wiedza, która może być przechowywana, przetwarzana lub przesyłana. Informacja niejawna - informacja, która wymaga ochrony przed nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem, oznaczona odpowiednią klauzulą tajności. System teleinformacyjny - urządzenia, narzędzia, metody postępowania, procedury oraz personel zorganizowany w taki sposób, aby zapewnić funkcje przechowywania, przetwarzania i przesyłania informacji.

JAWNE
Zastrzeżone



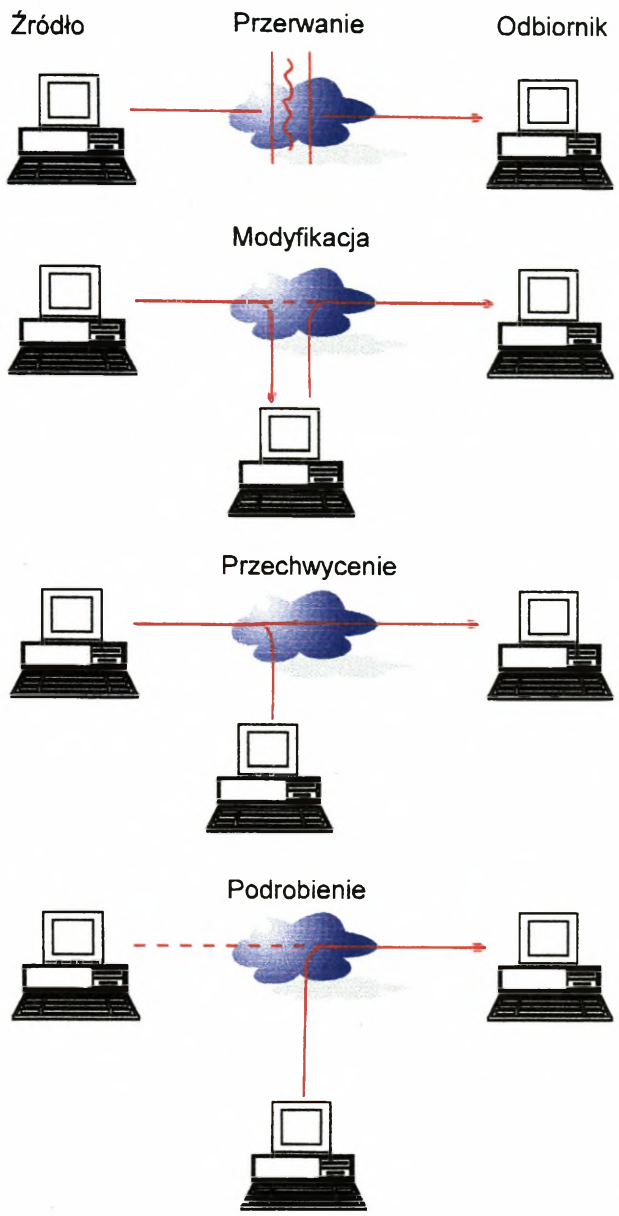
Rys.4.23. Model ochrony danych w sieci (wariant)

Znane dzisiaj metody ochrony informacji nie gwarantują absolutnego bezpieczeństwa i dalekie są od ideału, a zjawiska włamań do sieci nie dają się wyeliminować. Włamania do systemów informatycznych przynoszą znaczne straty finansowe i często utratę zaufania do instytucji, której powierzono poufne informacje. Środki ochrony, zmniejszające ryzyko uzyskania dostępu do danych przez osoby nieupoważnione, można ogólnie podzielić na dwie kategorie:

- kodowanie informacji (utajnianie) za pomocą metod kryptograficznych;
- ograniczenie dostępu do zasobów systemu zgodnie z ustaloną polityką ochronną organizacji.

Podstawowe pojęcia z zakresu ochrony danych to: atak na bezpieczeństwo danych, mechanizm zabezpieczający i usługa ochrony danych. Ataki na bezpieczeństwo sieci komputerowych przedstawiono na rys. 4.24, mogą być przeprowadzane w sposób pasywny lub aktywny. Atak pasywny polega na podsłuchiwaniu (szeroko pojętym) i monitorowaniu przesyłanych informacji. Celem ataku pasywnego może być dążenie do ujawnienia treści wiadomości lub uzyskanie informacji o samym ruchu informacji.

Atak aktywny dąży do modyfikowania strumienia informacji lub tworzenia fałszywych informacji. W działaniach tych mieszczą się: podszywanie się pod osobę uprawnioną i blokowanie działania. Istnieją różne metody zablokowania systemu teleinformacyjnego. Jedną z najprostszych do przeprowadzenia metod jest atak polegający na tak silnym przeciążeniu działania systemu wówczas praca w nim okazuje się niemożliwa. Ten rodzaj sabotażu może sparaliżować pracę organizacji w takim stopniu, że nie będzie ona mogła normalnie funkcjonować.



Rys.4.24. Ataki na bezpieczeństwo sieci komputerowych (wariant)

Napastnik zaleje system falą komunikatów, listów elektronicznych, połączeń modemowych i żądań usług sieciowych w tak dużym stopniu, że system nie będzie praktycznie robił nic poza próbami wykonania tych wszystkich zleceń. Bardziej wyrafinowane ataki polegają na przekierowywaniu żądań usług systemu w inne, zupełnie niewłaściwe miejsca. Znany jest przykład takiego przeprogramowania połączeń modemowych, że każde połączenie było kierowane na przypadkowy błędny numer.

Szczególną bolączką jest fakt, że ochrona przed blokadą usług systemu jest bardzo trudna – w praktyce wiąże się z izolowaniem systemu od otoczenia sieciowego.

Warunkiem koniecznym wprowadzenia urządzeń kryptograficznych powinno być zapewnienie pełnego bezpieczeństwa podczas prowadzenia wymiany informacji. Pewną część tych zadań można zrealizować przez utajnianie (szyfrowanie) informacji. Chcąc jednak uzyskać kryptograficznie bezpieczny i spójny system łączności należy oprócz eksploatacji tych urządzeń zrealizować inne przedsięwzięcia techniczno-eksploatacyjne.

Eksploatacja sieci łączności bez systemu ochrony informacji może umożliwić przeciwnikowi (wykorzystującemu istniejące luki w systemie ochrony) dostęp do informacji niejawnych, a działając w sposób aktywny może spowodować zniszczenie zasobów informacji i zdezorganizowanie funkcjonowania sieci. Funkcje zaimplementowane w urządzeniach utajniających powinny realizować wiele różnych zadań kryptograficznych. Dla poprawnej pracy tych urządzeń niezbędne jest dostarczenie określonej ilości danych kluczowych, ich wymiana w określonym czasie i bieżący nadzór nad eksploatacją. Funkcje te możliwe są do zrealizowania przez odpowiednie zaprojektowanie i wykonanie urządzeń utajniających. W systemie łączności eksploatowanych jest szereg różnych urządzeń i kanałów. Elementy te tworzą kilka podstawowych, zasadniczych podsystemów telekomunikacyjnych. W każdym z tych podsystemów występuje potrzeba określenia jednoznacznych i ścisłych wymagań dotyczących ochrony kryptograficznej.

Do podsystemów tych zaliczyć należy:

- podsystem łączności;
- podsystem informatyczny;
- podsystem kierowania i zarządzania siecią łączności;
- podsystem dystrybucji.

Jednocześnie z zasadniczymi funkcjami użytkowymi na te podsystemy powinny być nałożone elementy realizujące podsystem ochrony informacji.

Podsystem ten powinien spełniać następujące wymagania:

- powinien być szczelny, spójny i chronić informację przed nielegalnym ujawnieniem, modyfikacją, przekształceniem i zniszczeniem;
- powinien zapewniać ochronę informacji od momentu jej powstania u użytkownika do momentu jej wykorzystania i celowego legalnego zniszczenia;
- powinien spełniać wymagania użytkownika w zakresie ochrony i być przez użytkowników w pełni akceptowany;
- środki i metody ochrony powinny uwzględniać przewidywany charakter zagrożeń bezpieczeństwa.

Podsystem ten powinien być modyfikowalny. Do budowy podsystemu ochrony informacji należy stosować środki techniczne, programowe i organizacyjno - administracyjne. Użytkownikom należy zostawić swobodę w stosowaniu dodatkowych środków ochrony ich własnej informacji pod warunkiem, że uzyskają odpowiedni atest. Przy projektowaniu i wdrażaniu podsystemu ochrony należy uwzględnić koszty jego budowy i eksploatacji. Ochrona informacji w sieciach łączności obejmuje aspekty zabezpieczania fizycznego, organizacyjnego, przesyłania i przetwarzania danych. Jeśli informacja przesyłana między elementami sieci jest utajniana, lecz nie ma fizycznych ograniczeń w dostępie do systemu, to utajnianie może okazać się bezcelowe. W sieci łączności ochrony wymagają:

a) informacje i dane (łącznie z oprogramowaniem i danymi związanymi z zabezpieczeniami, np.: klucze, uprawnienia dostępu, itp.);
b) usługi komunikacyjne i przetwarzanie danych;
c) urządzenia.

Dla elementów tych istnieją następujące zagrożenia:

a) zniszczenie informacji i/lub innych zasobów (nieświadome lub złośliwe);
b) fałszowanie lub modyfikacja informacji;
c) kradzież, usunięcie lub zgubienie informacji;
d) ujawnienie informacji niejawnych;
e) przerwanie usługi;
f) zmiana uprawnień.

Zagrożenia mogą być przypadkowe i umyślne, pasywne i aktywne (czynne). Zagrożenie zrealizowane umyślnie określane jest jako atak na system. Zagrożenia pasywne, jeśli nawet zostały zrealizowane umyślnie, nie mają wpływu na modyfikację informacji w systemie łączności, nie zmieniają jego stanu i wykonywanych operacji. Zagrożenia umyślne pasywne popularnie nazywane są podsłuchem. Zagrożenia aktywne wprowadzają zmianę informacji w systemie lub zmieniają stan jego działania. Systemy informatyczne są szczególnie wrażliwe na ten typ zagrożeń.

Specyfika eksploatacji systemu łączności powoduje występowanie szeregu czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji. Poznanie ich pozwala prawidłowo projektować strukturę systemu, oraz konstrukcję i funkcje urządzeń utajniających. Do czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji w omawianym systemie zaliczyć należy:

- rozproszenie zasobów informatycznych na dużym terenie;
- eksploatowanie niewłaściwego sprzętu komputerowego;

- eksploatowanie "pirackiego" oprogramowania (systemowego i użytkowego);
- stosowanie do ochrony informacji nieetatowych środków ochrony (mechanizmów programowych i urządzeń technicznych);
- stosowanie sprzętu i oprogramowania nie sprawdzonego na obecność tzw. "pluskiew" programowych i sprzętowych;
- niechęć użytkowników i projektantów do stosowania środków ochrony informacji;
- niedocenianie zagrożeń bezpieczeństwa informacji przez użytkowników.

Ponadto zagrożeniami bezpieczeństwa informacji mogą być następujące elementy:

- ujawniająca emisja elektromagnetyczna komputerów, terminali i aparatury kanałowej oraz wrażliwość tych elementów na zakłócenie elektromagnetyczne;
- możliwość zdalnej penetracji zasobów informatycznych systemu;
- dołączanie podsłuchowych urządzeń rejestrujących;
- dołączanie niesankcjonowanych terminali;
- nielegalne wykorzystanie terminali użytkowników;
- stosowanie nielegalnego oprogramowania;
- czynniki losowe - zaniki napięcia, przesłuch, błędy w komutacji, zakłócenia w transmisji, powodzie, pożary;
- awarie urządzeń;
- niesolidność personelu wywołana niedoszkoleniem, bezmyślnością lub spowodowana szantażem.

Istnieje szereg różnych metod i środków ochrony informacji. Do podstawowych z nich zaliczyć należy:

- metody organizacyjno - administracyjne:
  - ograniczenie dostępu do informacji niejawnych;
  - ograniczenie uprawnień osób funkcyjnych w systemie zarządzania;
- metody i środki programowe:
  - hasła dostępu do zbiorów;
  - uprawnienia;
  - uwierzytelnienie i identyfikacja;
  - zamknięte grupy użytkowników;
- środki techniczne:
  - osłony ekranujące;
  - kabiny ekranujące;

- ekranowanie pomieszczeń;
- urządzenia o obniżonym poziomie ujawniającej emisji elektromagnetycznej;
- światłowody;
- środki ochrony przed nieuprawnionym dostępem do sprzętu;
- środki ochrony przed nieuprawnionym dostępem do programów;
- szyfrowanie informacji:

• szyfrowanie kanałowe;

- szyfrowanie baz danych;
- uwierzytelnianie użytkownika.

Usługi ochrony danych zapewniają uzyskanie pewnych gwarancji w zakresie wiarygodności systemu komputerowego:

- poufność - ochrona przed atakiem pasywnym;
- uwierzytelnienie - zapewnienie autentyczności informacji i osób: zagwarantowanie, że informacja pochodzi z takiego źródła, które jest przy niej wymieniane lub też osoba jest tą, za którą się podaje;
- nienaruszalność - zapewnienie integralności komunikacji, tzn. tego, że informacja jest odbierana w takiej postaci, w jakiej została wysłana;
- niezaprzeczalność - niemożliwość zaprzeczenia faktowi wysłania lub odebrania informacji;
- kontrola dostępu - możliwość kontrolowania dostępu do informacji (systemów) drogą identyfikacji i uwierzytelniania;
- dyspozycyjność - ograniczanie skutków ataku w sferze dostępności informacji.

Mechanizmy zabezpieczające obejmują następujące działania:

- szyfrowanie informacji;
- uwierzytelnianie informacji (podpisy cyfrowe);
- ochrona antywirusowa;
- identyfikacja i uwierzytelnianie osób uprawnionych.

Etapy realizacji podsystemu bezpieczeństwa i ochrony w systemach teleinformatycznych.

Ocena zagrożeń jest pierwszym etapem pracy przy analizie bezpieczeństwa łączności, obejmuje ona:

a) identyfikację słabych punktów systemu;

b) analizę prawdopodobieństwa występowania zagrożeń z uwzględnieniem słabych punktów systemu;

c) ocenę konsekwencji wykorzystania każdego zagrożenia indywidualnie oraz w powiązaniu z innymi zagrożeniami;

d) oszacowanie kosztów każdego ataku (w tym ocenę na ile udany atak ułatwia następne);

e) oszacowanie kosztów potencjalnych środków przeciwdziałania, w tym również ewentualnego pogorszenia parametrów funkcjonalnych systemu.

Następnym etapem realizacji ochrony powinno być zrealizowanie przedsięwzięć organizacyjno-administracyjnych. Opracowane powinny być one z uwzględnieniem następujących zasad:

1. Informacja powinna być przekazana, udostępniona lub przedstawiona do oceny tylko tym użytkownikom, którzy są do tego odpowiednio uprawnieni.
2. Użytkownicy powinni mieć dostęp do zasobów tylko w zakresie swojego uprawnienia.
3. Każda próba nieuprawnionego działania w systemie powinna być wykrywana, rejestrowana i sygnalizowana służbom nadzoru.
4. Działania użytkowników systemu łączności, mające wpływ na żywotność systemu, powinny być rejestrowane w dzienniku kontrolnym z podaniem danych identyfikujących użytkownika, rodzaju i terminu wykonywanej operacji. O prowadzeniu dziennika użytkownicy powinni być poinformowani, ale nie powinni mieć do niego dostępu. Dostęp do dziennika powinien być zagwarantowany dla służb nadzoru.

Do ochrony systemów łączności przed atakami zarówno wewnętrznymi, jak i zewnętrznymi jako jeden z podstawowych elementów ochrony - powszechnie wykorzystywane są metody kryptograficzne. Odpowiednio zaprojektowane i wdrożone eliminują możliwości wykonania w sposób skuteczny dowolnego z ogólnie znanych ataków, nawet przez bardzo wyrafinowanego przeciwnika. Następnym etapem powinien być więc wybór odpowiednich urządzeń utajniających. W celu zrealizowania ww. założeń, w urządzeniach tych powinny być zainstalowane następujące niezbędne elementy:

- ściśle sprecyzowane algorytmy obsługi, uwzględniające wprowadzenie hasła;
- konieczność pracy z identyfikatorem osobistym, wykorzystywanym m.in. do tworzenia grup użytkowników;
- segmenty realizujące funkcje archiwizacji podstawowych zdarzeń;
- segmenty realizujące procedury zdalnej dystrybucji;
- procedury transmisyjne;
- algorytmy zabezpieczające dane kluczowe przechowywane w urządzeniach.

Zaproponowana konstrukcja urządzeń utajniających powinna umożliwić wdrożenie modułu do wielu urządzeń podsystemu łączności. Przyjęta technologia powinna pozwolić na ciągły rozwój urządzeń już opracowanych, wdrożonych i eksploatowanych. Kolejne wersje urządzenia lub określone ich funkcje mogą być wprowadzane przez upoważnione osoby u użytkownika, po dołączeniu dowolnego urządzenia telekomunikacyjnego lub informatycznego.

Bezpieczeństwo sieci to nie tylko środki techniczne i programowe systemów ochrony. Bezpieczeństwo to zarówno problem środków ochrony, jak i zarządzania zasobami oraz informacją. Jest ono w rzeczy samej pochodną dobrej organizacji i właściwej polityki ochrony wprowadzanej na wszystkich szczeblach organizacyjnych. Problem ochrony sieci przedsiębiorstwa należy rozpatrywać na wszystkich szczeblach jego struktury organizacyjnej nie wyłączając z tego ścisłego zarządu. Polityka ochrony musi być jednoznaczna i przejrzysta, a każdy pracownik firmy powinien być z nią zaznajomiony.

Podstawowym etapem w organizowaniu systemu ochrony jest rozpoznanie obszaru ochrony. Przede wszystkim trzeba określić, z czego składa się sieć: jak wygląda schemat sieci, punkty dostępu do sieci i kto z nich korzysta. Ponadto należy dokonać oceny wartościowej informacji. Jakie zasoby informacyjne są na tyle ważne, aby je chronić, i gdzie są zlokalizowane? Szkolenie personelu w zakresie ochrony informacji jest sprawą poza wszelką dyskusją, choć często zaniedbywaną. Niezbędna jest ciągła współpraca personelu zajmującego się ochroną z komórkami organizacyjnymi przedsiębiorstwa, jak również wspomaganie, zrozumienie i elastyczność wobec użytkownika końcowego. Proces edukacyjny dla całego personelu powinien być dostosowany do oczekiwań i potrzeb każdej grupy pracowniczej, w przeciwnym razie ochrona będzie pomijana, wyłączana lub ignorowana. Ustalenie polityki ochrony i przeszkolenie personelu są wstępem do wprowadzenia w życie planu ochrony - realizacja tego zadania powinna być w miarę "bezbolesna" i płynna.

Znanych jest wiele wariantów problemu ochrony informacji, mających wpływ na całą architekturę systemu ochrony. Nie są to rozwiązania idealne, ponieważ żaden system nie jest w stanie spełnić wszystkich wymagań.

Jakość podsystemu bezpieczeństwa i ochrony zależy od prawidłowego opracowania założeń, wyboru odpowiednich urządzeń utajniających oraz zrealizowania przedsięwzięć organizacyjno-administracyjnych. Sama technologia nie może zapewnić pełnego bezpieczeństwa. Ochrona to przede wszystkim właściwe zarządzanie i organizacja.

JAWNE
Zastrzeżone

4.14. Wskaźniki oceny systemów łączności

System łączności działa w niezwykle złożonych warunkach. Łączność powinna więc spełniać szereg kryteriów, do których należy zaliczyć wskaźniki jej oceny tj. terminowość, wierność i skrytość łączności, natomiast do kryteriów oceny systemu łączności należy zaliczyć: gotowość obronną, przepustowość, mobilność, trwałość (do której zalicza się: żywotność, odporność na zakłócenia i niezawodność) oraz bezpieczeństwo łączności. [55] System łączności podsystemu kierowania obronnością państwa realizowany był głównie przy wykorzystaniu hierarchicznego analogowego systemu łączności.

Specyfiką analogowego systemu była konieczność tworzenia bezpośrednich relacji łączności (kanałów łączności) pomiędzy współpracującymi stanowiskami kierowania, a nawet i poszczególnymi miejscami pracy osób funkcyjnych. W efekcie powstawała skomplikowana struktura połączeń, odzwierciedlająca, w sposób niemal wierny, hierarchiczny system kierowania obronnością państwa. W strukturze hierarchicznej, na której opierał się analogowy (przestarzały) system łączności nie jest już możliwe spełnienie wymogów między innymi mobilności. Natomiast struktura niehierarchicznych systemów łączności oparta jest na systemie siatkowym. W strukturze tej zmiana dyslokacji lub przeznaczenia poszczególnych węzłów nie powoduje zmian w strukturze całego systemu. Zmiana funkcji węzła związana ze zmianą działania obsługiwanego przez nią stanowiska kierowania obronnością związana jest ze zmianą numeracji węzła i wykonywana jest bezzwłocznie. Prawdopodobieństwo terminowej zmiany konfiguracji struktury połączonej ze zmianą dyslokacji końcowego mobilnego węzła łączności, jak wcześniej wspomniano, z uwagi na małą liczbę realizowanych relacji i praktycznie brak procedur alokacji w systemie jest bardzo wysokie.

Postęp w telekomunikacji polegający głównie na zastosowaniu techniki cyfrowej w procesach komutacji i transmisji, został tu już nazwany postępem rewolucyjnym - rewolucją techniczną. Zresztą słusznie gdyż, konsekwencje tego postępu, zwłaszcza jego wpływ na militarne systemy łączności jest ogromny. Dotychczas stosowana technika, w większości analogowa, umożliwiała realizację prostych hierarchicznych systemów łączności opartych na kanale fonicznym komutowanym w ręcznych centralach telefonicznych. Niskie krotności systemów zwielokrotniających zmuszały do stosowania ograniczeń wielkość wiązek międzycentralowych i zestawiania kanałów bezpośrednich między użytkownikami. W ramach sieci tworzono dodatkowe podsystemy wydzielone w celu realizacji usług specjalnych, np. transmisji danych, telegrafu czy związanych z utajnianiem

JAWNE
Zastrzeżone

itp. Tworzenie wydzielonych systemów uniemożliwiało prowadzenie racjonalnej polityki wykorzystywania posiadanego potencjału, zwłaszcza w jego warstwie transmisyjnej i to transmisji międzywęzłowej. Trudności w realizacji efektywnego systemu łączności polegające głównie na permanentnym braku możliwości realizacji ruchu abonenckiego w określonym czasie i o żądanym natężeniu, wymusiły stworzenie specyficznych wskaźników jego oceny. Wskaźniki te, w pełni odzwierciedlające specyfikę i charakter analogowego systemu łączności, tworzyły kompletny specyficzny język opisu jego sytuacji problemowych. Język ten, umożliwiający sformułowanie sądów wartościujących systemów analogowych, stał się mało przydatny do oceny procesów zachodzących w systemach opartych na urządzeniach techniki cyfrowej.

Terminowość łączności - zdolność do przekazywania i dostarczania informacji oraz prowadzenia bezpośrednich rozmów w określonym czasie. W systemach analogowych terminowość była definiowana generalnie, jako prawdopodobieństwo zestawienia połączenia w określonym czasie. Dla systemów łączności w pełni cyfrowych, opartych głównie na bezobsługowych urządzeniach komutacyjnych oraz stosowaniu węzłów tranzytujących ruch i dużych wiązek łączy transmisyjnych, pojęcie terminowości utożsamia się z prawdopodobieństwem odnalezienia drogi, po której zostanie zestawione żądane połączenie, przy czym czas samego zestawiania połączenia nie odgrywa specjalnej roli. Prawdopodobieństwo realizacji połączenia będzie więc zależeć nie tylko, jak w systemach analogowych, od wielkości wiązek łączy i natężenia ruchu w określonej relacji, lecz głównie od sposobu realizacji procedur poszukiwania drogi połączeniowej w sieci (realizacji routingów) i zakresu stosowania odpowiednich preferencji i ograniczeń ruchu. Zakłada się przy tym, że dla abonenta o największym priorytecie obsługi, poprawnie opracowany system powinien być zawsze zdolny do odszukania i zestawienia żądanego połączenia, z innym aktualnie istniejącym abonentem systemu.

Wierność łączności określa stopień zgodności informacji odebranej z informacją nadaną, przy istniejących liniach łączności, zakłóceniach i zniekształceniach. W odniesieniu do kanałów analogowych wierność definiowana była jako zrozumiałość logotomowa i jako prawdopodobieństwo skażenia znaku kombinacji kodowej w odniesieniu do kanałów teledacyjnych. W systemach cyfrowych wskaźnik ten należy rozpatrywać dwuaspektowo w odniesieniu do kanału sygnalizacji międzycentralowej i w odniesieniu do transmisji sygnałów w kanale abonenckim. W pierwszym wypadku producent określa maksymalną

[55] Metody oceny systemów łączności na potrzeby obronności państwa pk. "WENA-1". AON, Warszawa 1995.

JAWNE
Zastrzeżone

jednostkową stopę błędów akceptowaną przez centrale, powyżej której kanał jest uznawany jako niesprawny i wyłączony z obsługi. Udostępnienie abonentom jednorodnego kanału cyfrowego tranzytowanego przez wiele węzłów komutacyjnych i zakończonego obustronnie przetwornikami analogowo - cyfrowymi powoduje, że jakość kanałów abonenckich zależy od jednostkowej stopy błędów poszczególnych traktów cyfrowych. Wpływ wartości elementarnej stopy błędów na jakość kanału fonicznego jest ściśle określony i zależny od stosowanej metody kodowania mowy. Jak wynika z badań, modulacja delta jest najbardziej odporna na zakłócenia występujące w kanale transmisyjnym. W wypadku transmisji danych w kanałach cyfrowych stosowane procedury kontrolne czy też kody korekcyjne, uzależniają jej jakość od elementowej stopy błędów. W systemach cyfrowych istnieje możliwość kontroli stanu traktów transmisyjnych a w razie ich uszkodzeń, zdalnego ich eliminowania.

Skrytość łączności jest to zdolność przeciwstawiania się rozpoznaniu przeciwnika w zakresie ujawnienia treści przekazywanych informacji oraz wykrycia faktu, miejsca i przynależności obiektu nadawania. W systemach analogowych skrytość była definiowana jako współczynnik utajniania kanałów lub jako prawdopodobieństwo wykrycia obiektu (węzła).

W cyfrowych systemach łączności stosuje się najczęściej obligatoryjne utajnianie wszystkich międzycentralowych kanałów grupowych jako pierwszy stopień utajniania. Jako drugi stopień utajniania stosuje się, dodatkowo dla wybranych abonentów, indywidualne systemy utajniania typu punkt - punkt, instalowane bezpośrednio u użytkowników. Miarą skrytości systemu będzie więc głównie nie współczynnik utajniania kanałów a wprost skuteczność urządzeń utajniających definiowana jako ich moc kryptograficzna. Skrytość w rozumieniu prawdopodobieństwa wykrycia obiektu, np. węzła komutacyjnego, z uwagi na niehierarchiczność struktury oraz stosowanie kratowej struktury powiązań węzłów, miniaturyzację urządzeń i zmniejszenie liczby samodzielnych elementów, uległa znacznemu przewartościowaniu Zapewnienie odpowiednio niskiego prawdopodobieństwa wykrycia w odpowiednim czasie węzła cyfrowego jest dużo łatwiejsze niż w wypadku analogicznego węzła analogowego. Niehierachiczność struktury systemu spowodowała dodatkowo zmniejszenie roli poszczególnych węzłów w systemie, a więc i zminimalizowanie negatywnych skutków ich uszkodzenia (eliminacji))

Gotowość obronna systemu łączności jest to zdolność do terminowego przejścia z danego stanu w inny, niezbędny do zapewnienia kierowania systemem obronności. Powinna ona wyprzedzać gotowość obronną samego systemu obronności państwa. Nowoczesny stacjonarny cyfrowy system łączności, będący w stałej gotowości obronnej jest dostosowany,

JAWNE
Zastrzeżone

z przyczyn ekonomicznych, do realizacji z określonym prawdopodobieństwem ruchu abonenckiego, mierzonego np. w erlangach. Zwiększenie stanu gotowości obronnej systemu będzie związane głównie z jego rozbudową spowodowaną:

- koniecznością realizacji zwiększonego natężenia ruchu abonenckiego;
- rozbudowaniem struktury połączeń międzywęzłowych;
- włączeniem polowych elementów systemu.

Zmiana struktury systemu, polegająca na rozbudowie struktury powiązań, będzie uwarunkowana praktycznie jedynie czasem zestawiania nowych traktów cyfrowych. Włączenie polowych elementów systemu z punktu widzenia istniejącego w stałej gotowości systemu łączności będzie odbierane jako pojawienie się dodatkowych źródeł generacji ruchu abonenckiego, czyli zwiększenia natężenia ruchu. Z uwagi na ograniczenie liczby zestawianych relacji i zminimalizowanie procedur nawiązywania łączności, czas włączenia do systemu elementów polowych zdeterminowany będzie głównie jego czasem dyslokacji.

Przepustowość systemu łączności charakteryzuje potencjalną możliwość sieci w przekazywaniu ilości informacji w jednostce czasu. Powinna ona odpowiadać potrzebom kierowania i dowodzenia w tym zakresie. Można ją określać dla każdego kierunku łączności, odcinka lub całości systemu łączności. W cyfrowych systemach łączności zdolność przepustowa jest określana jako przepływność cyfrowych strumieni grupowych łączących poszczególne węzły komutacyjne sieci. Wartość ta, w skali lokalnej, również określa liczbę bezpośrednich kanałów łączności. W skali makro, czyli całego systemu, wielkość ta jest jedynie elementem pomocniczym umożliwiającym ocenę zdolności przepustowej całego systemu. Automatyczna komutacja połączeń oparta na dynamicznym wyznaczaniu dróg połączeniowych umożliwia praktycznie wykorzystywanie całego potencjału sieci czyli wszystkich dostępnych dróg połączeniowych.

Trwałość systemu łączności określana jest jej zdolnością do pracy przy oddziaływaniu na niego wszystkich czynników rażenia przeciwnika, czy innych narażeń, związanych z klęskami żywiołowymi, kataklizmami i atakami terrorystycznymi, wyraża się żywotnością, odpornością na zakłócenia oraz niezawodnością środków i elementów sieci.

Żywotność sieci i jej elementów określa zdolność do wykonywania postawionych zadań w warunkach oddziaływania przeciwnika lub innych destrukcyjnych czynników związanych z wystąpieniem klęsk żywiołowych itp.

Odporność na zakłócenia sieci i jej elementów charakteryzuje zdolność do wykonywania zadań w określonym czasie w warunkach radioelektronicznego oddziaływania przeciwnika, szczególnie zaś wszelkiego rodzaju środków zakłócających.

JAWNE
Zastrzeżone

Niezawodność sieci i jej elementów charakteryzuje zdolność do wykonywania postawionych zadań w określonym czasie przy odpowiednim (zadanym) poziomie parametrów taktyczno - technicznych sprzętu łączności, przyjętych w warunkach jego eksploatacji oraz pożądanym poziomie wyszkolenia stanów osobowych i odpowiednim wsparciu logistycznym.

Trwałość cyfrowego systemu łączności z uwagi na wielowariantowość realizacji połączeń jest mało zależna od stanu sprawności określonej relacji łączności między poszczególnymi węzłami. Trwałość będzie zależna od ogólnej struktury systemu globalnej sprawności systemu transmisyjnego i od stabilności pracy podsystemu sygnalizacji systemowej (międzycentralowej).

Mobilność systemu łączności jest to zdolność do terminowego rozwijania, rozbudowy i przebudowy (*adaptacji*) struktury sieci, odpowiednio do kształtującej się sytuacji operacyjno- strategicznej oraz związanych z tym potrzeb systemu kierowania i dowodzenia.

Struktura niehierarchicznych cyfrowych systemów łączności oparta jest na systemie siatkowym. W strukturze tej zmiana dyslokacji lub przeznaczenia poszczególnych węzłów nie powoduje zmian w strukturze całego systemu. Zmiana funkcji węzła związana ze zmianą funkcji obsługiwanego przez nią stanowiska kierowania obronnością związana jest ze zmianą numeracji węzła i wykonywana jest bezzwłocznie. Prawdopodobieństwo terminowej zmiany konfiguracji struktury połączonej ze zmianą dyslokacji końcowego mobilnego węzła łączności, jak wcześniej wspomniano, z uwagi na małą liczbę realizowanych relacji i praktycznie brak procedur alokacji w systemie jest bardzo wysokie.

Bezpieczeństwo systemu łączności jest to zdolność przeciwstawienia się wszystkim rodzajom rozpoznania przeciwnika oraz próbom wprowadzenia fałszywej informacji. Jest ono określane przez odporność na rozpoznanie oraz niedostępność elementów systemu łączności (niedostępność do informacji przesyłanych w systemie). Osiąga się ją poprzez terminową realizację przedsięwzięć organizacyjnych i technicznych polegających głównie na fizycznej ochronie elementów i środków łączności, ograniczaniu poziomu elektromagnetycznej emisji ujawniającej i szyfrowaniu przesyłanych informacji. [56]

W systemach niehierarchicznych struktura systemu jest praktycznie skryta. Drogi połączeniowe są zapisane w tablicach routingów procesorów sygnalizacyjnych poszczególnych węzłów komutacyjnych. Wiadomości te są fragmentaryczne i nie informują

---

[56] Gawlikowski W., *Zagrożenia systemu telekomunikacyjnego w czasie pokoju, kryzysu i wojny*. Zeszyty Naukowe nr 3/97. AON 1997.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

o strukturze całego systemu. Dodatkowo, najczęściej w sposób obligatoryjny dokonuje się utajniania wszystkich traktów grupowych, co uniemożliwia włączenie się do systemu osób postronnych.

Analiza przydatności wskaźników oceny analogowych systemów łączności po ich niewielkiej modyfikacji wykazuje przydatność do oceny niehierarchicznych systemów cyfrowych. [57]

Wskaźniki te przyjmowane w sposób obligatoryjny były weryfikowane za pomocą symulacji modeli komputerowych oraz przez praktyczną realizację, podczas badań określających specyficzne cechy systemu. Do wskaźników tych należy zaliczyć:

- prognozowanie ruchu;
- wybór stosowanej metody kodowania mowy;
- ustanowienie gradacji abonentów w postaci odpowiednich priorytetów realizacji połączeń;
- wprowadzenie limitowanego dostępu abonentów do sieci;
- ograniczenie czasu trwania niektórych połączeń;
- określenie procedur zestawiania połączeń (algorytmu komutacji poszukiwania abonentów w sieci);
- algorytm szyfrowania sygnałów.

Jak wcześniej wspomniano, efektem właściwego doboru ww. wskaźników jest możliwość wykorzystania przez abonentów, przy realizacji połączeń, całego dostępnego im potencjału komutacyjnego i transmisyjnego sieci. Jednocześnie, przy wystąpieniu rozległych uszkodzeń struktur, jest zagwarantowana możliwość realizacji połączeń dla najważniejszych abonentów systemu. Oddzielną grupę stanowią wskaźniki uwarunkowane cechami eksploatacyjnymi systemów niehierarchicznych.

W krajach NATO do praktycznej oceny wskaźników eksploatacyjnych systemów łączności stosowane są zautomatyzowane procedury oparte na systemach komputerowych, będące jednocześnie ich systemem zarządzania.[58] Wszystkie te procedury można podzielić na cztery podstawowe grupy związane z procesami:

- planowania systemu i kontroli realizacji;
- nadzoru - zarządzania istniejącymi zasobami;

---

[57] Metodyka badania Krajowego Systemu Łączności KSŁ-P Kryterium techniczne, Wykorzystanie technik komputerowych, Kryterium ekonomiczne, Kryterium eksploatacyjno-techniczne, Kryterium oceny systemu, Kryterium operacyjne, Kryterium technik komputerowych, Kryterium uwarunkowań organizacyjno-prawnych i techniczno-eksploatacyjnych, Kryterium bezpieczeństwa łączności. AON, Warszawa 1996.

[58] *Naczelny Komitet ds. Planowania Zagrożeń Cywilnych NATO, SCEPC-struktura i cele*, Materiały NATO, Bruksela 1998.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

- kontroli jakości świadczenia usług;
- bezpieczeństwa sieci.

Planowanie jest zespołem czynności dokonywanych przed podjęciem zasadniczych manewrów siłami i środkami technicznymi. Planowanie ma na celu dokonanie wstępnej oceny tworzonego (nowego lub rozbudowywanego) systemu łączności. Proces planowania jest zintegrowany z siecią zautomatyzowanego zarządzania zasobami łączności oraz z specjalistycznymi bazami danych i programami umożliwiającymi dokonanie wstępnej oceny wskaźników rozbudowywanych systemów. Planowanie dokonywane jest w czterech fazach jako:

- planowanie wstępne;
- planowanie działań;
- planowanie manewrów;
- kontrola realizacji zaplanowanych działań i manewrów.

Planowanie wstępne polega na przyjęciu założeń dotyczących realizacji systemu w zakresie generalnych założeń operacyjnych i ma na celu dostosowanie systemu do spełniania konkretnych funkcji. Polega ono głównie na ustalaniu konfiguracji węzłów, doborze odpowiednich transkoderów umożliwiających współpracę z innymi systemami. Efektem tego planowania jest powstanie bazy danych będących podstawowym materiałem do wykonania następnych czynności planistycznych. Opracowana baza danych określa liczbę i parametry poszczególnych węzłów, ich systemów komutacyjnych, transmisyjnych i radiodostępu.

Planowanie działań należy traktować jako praktyczne globalne podejście do oceny takich wskaźników systemu, jak gotowość bojowa, mobilność, terminowość, trwałość czy też zdolność przepustowa. Za podstawę fazy procesu planowania przyjmuje się, jako warunki brzegowe, aktualną strukturę systemu z uwzględnieniem stanu technicznego jego poszczególnych elementów. Podstawą procesu planowania są cyfrowe mapy terenu przyszłych działań, w powiązaniu z którymi tworzy się bazę danych o istniejącej infrastrukturze terenu pod kątem projektowanego systemu. Bazy danych takich stałych punktów dowiązania obejmują głównie wiadomości z zakresu:

- lokalizacji węzłów stacjonarnych;
- wielkości powiązań transmisyjnych węzłów stacjonarnych z innymi węzłami;
- lokalizacji i możliwości punktów transmisyjnych systemów publicznych (stacji regeneratorowych);

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

- możliwości udostępnienia przez dany węzeł infrastruktury logistycznej w postaci energii elektrycznej, wody oraz możliwości dojazdu.

Gotowe proponowane rozwiązania są archiwizowane w postaci banków danych i wykorzystywane w wypadku ponownego planowania działań na tym terenie. Planowanie wspomagane komputerowo umożliwia opracowanie grafu sieciowego czyli praktycznej listy zdarzeń określających proces przejścia systemu do żądanego stopnia gotowości bojowej wraz z wyznaczeniem ścieżek krytycznych i parametrów czasowych procesu. W planowaniu tym wyróżnia się procesy technologiczne polegające na sprecyzowaniu:

- asortymentu i ilości sprzętu;
- lokalizacji konkretnego węzła;
- powiązań z innymi węzłami i systemami;
- świadczonych usług.

Przy planowaniu sprzętu dokonuje się kontroli konfiguracji węzła pod kątem jego praktycznej aplikacji i wprowadzenia niezbędnych korekt, a wniesione zmiany zapisuje się w bazach danych. Proces lokalizacji węzła dokonuje się bezpośrednio na mapach cyfrowych terenu uwzględniając możliwości terenu i powiązania go z systemem.

Powiązanie rozwiniętego węzła z systemem łączności planowaną w nim jego rolę oraz profile terenu pod względem realizacji systemów radioliniowych.

Powiązanie węzła z innymi systemami uwzględnia dyslokację odpowiednich translatorów umożliwiających współpracę z systemami innych krajów.

Planowanie usług polega na ustaleniu lokalizacji elementów radiodostępu abonenckiego w celu zapewnienia pokrycia terenu oraz na przydziale odpowiednich częstotliwości. Planowanie manewrów polega na przewidywaniu kolejnych miejsc przemieszczeń węzłów oraz czasu ich realizacji. Wykonuje się je jako działania:

- planowane w celu dostosowania struktury systemu do konkretnych potrzeb operacyjnych i wykonuje się je przy stabilnej sytuacji bojowej (najczęściej kilku węzłami jednocześnie);
- doraźne w celu odtworzenia uszkodzonych elementów systemu;
- uprzedzające mające na celu uodpornienie eksploatowanego systemu i wykonywane jest w najbardziej dogodnym czasie.

Kontrola realizacji zaplanowanych działań jest istotnym elementem procesu planistycznego. Kontrola taka jest dokonywana na bazie zautomatyzowanego systemu zarządzania zasobami łączności i umożliwia bieżący nadzór nad procesem rekonfiguracji sieci oraz wprowadzanie niezbędnych korekt. Kontrola jakości świadczenia usług, czyli praktyczne

JAWNE
Zastrzeżone

monitorowanie systemu i zarządzanie jego eksploatacją jest realizowane najczęściej wielostopniowo poprzez centra zarządzania zasobami łączności. Kontrola ta jest wykonywana w sposób automatyczny przy wykorzystaniu pakietowych sieci transmisji danych i umożliwia kontrolowanie następujących parametrów:

- sprawności grupowych łączy międzycentralowych;
- aktualnej stopy błędów grupowych łączy;
- natłoku w sieci poprzez nadzór zajętości szczelin łączy grupowych;
- sprawności poszczególnych urządzeń systemu np. centrali urządzeń radiodostępu, radiolinii itp.;
- poprawności wybierania numerów przez abonentów;
- innych mających bezpośredni wpływ na jego wskaźniki efektywności.

Wszystkie dane wraz z aktualną konfiguracją systemu są archiwizowane i stanowią podstawę do dokonywania późniejszych analiz oraz są wykorzystywane w procesach planistycznych,

Bezpieczeństwo systemu realizowane jest poprzez stosowanie systemów utajniania cyfrowych traktów grupowych oraz indywidualnych kanałów abonenckich. Połączenia z systemami innych krajów wykonuje się poprzez odpowiednie bramy (gateway), w których następuje między innymi zmiana systemów utajniania na systemy krajowe. Dostęp do systemu zarządzania operatorów, jego zasobów i procedur, jest zróżnicowany oraz wielostopniowy i obwarowany indywidualnymi hasłami.

Uzyskiwanie żądanych wskaźników efektywności systemu jest więc procesem interakcyjnym realizowanym w sposób permanentny w powiązaniu z konkretną jego aplikacją.

Wykorzystywanie zdobytych wcześniej doświadczeń w postaci odpowiednich banków danych, z procesem planistycznym, kontrolą realizacji zamierzeń i aktualnym stanem sieci, umożliwia optymalizację działań i racjonalne gospodarowanie dostępnymi siłami i środkami.

4.15. Wymagania stawiane systemom łączności

W systemie obronnym państwa łączność występuje jako podstawowy środek kierowania państwem i dowodzenia siłami zbrojnymi. Podmiotem procesów kierowania są najwyższe organa kierownicze państwa, a ich bazę organizacyjno-techniczną stanowią stanowiska kierowania i dowodzenia wyposażone w techniczne środki wspomagania oraz

zabezpieczenia kierowania (dowodzenia), sprzężone w spójny system za pomocą środków łączności.

Wymagania systemu kierowania obronnością państwa wobec telekomunikacji i informatyki w zakresie poziomów gotowości obronnej są szczególne i dotyczą:

- zapewnienia przekazywania terminowo, wiernie i skrycie informacji w wymaganych postaciach, w obiegu wewnętrznym i między strukturami organizacyjnymi;
- żądania pełnej gotowości systemu w każdej sytuacji kryzysowej w okresie pokoju, zagrożenia wojennego i wojny;
- bezpieczeństwa i ochrony systemu;
- szybkiej reakcji systemu;
- integracji rozwiązań;
- efektywności ekonomicznej rozwiązań.

Współczesny, a zwłaszcza perspektywiczny, system łączności cyfrowej powinien posiadać cechy, pozwalające spełnić szereg wymagań, między innymi:

a) w sferze organizacyjnej:

- wyprzedzająca gotowość łączności do działania w stosunku do systemu kierowania obronnością państwa i działania wojsk;
- wysoki poziom żywotności oraz stabilności systemu bez względu na powstałą sytuację bojową;
- gwarantowany poziom utajniania i bezpieczeństwa łączności;
- duża mobilność i elastyczność systemu.

b) w sferze technicznej:

- duża niezawodność i wierność transmisji danych;
- automatyczne uzyskanie połączeń bezpośrednich i obejściowych;
- możliwość zestawiania priorytetowych połączeń dalekosiężnych;
- odporność na zakłócenia radioelektroniczne;
- zdolność przekazywania informacji z określoną mocą kryptograficzną;
- możliwość przesyłania sygnałów alarmowych oraz szybka łączność operacyjna w formie pisemnej z automatycznym jej zobrazowaniem i dokumentowaniem;
- współdziałanie z systemami różnych operatorów sieci telekomunikacyjnych;
- zapewnienie bezpośredniej, konferencyjnej i indywidualnej łączności między osobami funkcyjnymi;

JAWNE
Zastrzeżone

- wymiana informacji opracowanej w planowanych systemach zautomatyzowanego wspomagania procesu kierowania i dowodzenia;
- możliwość kontroli i automatycznej rejestracji stanu eksploatowanych łączy.

Wymagania, które musi spełniać system telekomunikacyjny, to między innymi:

- świadczenie usług telekomunikacyjnych z zadaną normami, sprawnością usługową;
- zapewnienie wiarygodności przekazywanych informacji tj. wymaganego stopnia zgodności treści wiadomości odebranej z nadaną;
- zapewnienie wysokiej żywotności systemu;
- przesyłanie wiadomości według określonych priorytetów i stopni pilności;
- właściwa reakcja systemu na nierównomierność obciążenia ruchem;
- duża niezawodność wiązek łączy i węzłów komunikacyjnych;
- zapewnienie odpowiedniej szybkości transmisji, stosownie do potrzeb i oczekiwań użytkowników;
- możliwość utajniania informacji.

Ten sposób podejścia do oceny systemów łączności nie uwzględnia wszystkich, zwłaszcza celowych narażeń, którym może być poddany system łączności.

Zdaniem autorów pracy studyjnej do najistotniejszych wymagań, jakie powinien spełniać system łączności na potrzeby obronności, należy zaliczyć między innymi:

- wyprzedzającą gotowość w stosunku do systemu kierowania obronnością;
- dużą mobilność i elastyczność umożliwiającą zmianę struktury systemu;
- wysoki poziom żywotności i stabilności pracy bez względu na sytuację operacyjną;
- odporność na rozpoznanie i niszczenie przez przeciwnika;
- jednorodność wynikającą ze stosowania cyfrowych jednorodnych kanałów abonenckich;
- możliwość stosowania radiodostępu abonenckiego z zachowaniem jednorodności kanału;
- zapewnienie ciągłości utajniania w całym łańcuchu telekomunikacyjnym (nie wyłączając radiodostępu);
- możliwość stosowania systemu kryptograficznego umożliwiającego przekazywanie informacji o najwyższych klauzulach tajności;
- zdolność przekazywania informacji (w tym również transmisji danych) w czasie zbliżonym do rzeczywistego;
- możliwość stosowania automatycznego ruchu abonenckiego;
- możliwość realizacji cyfrowych zintegrowanych kanałów abonenckich umożliwiających naprzemienne przesyłanie sygnałów mowy i danych;

JAWNE
Zastrzeżone

- zapewnienie priorytetowego dostępu najważniejszych abonentów do zasobów sieciowych;
- możliwość automatycznego poszukiwania abonenta w sieci, niezależnie od miejsca przebywania abonenta;
- możliwość stosowania systemów zarządzania zasobami transmisyjnymi i komutacyjnymi sieci;
- możliwość przekazywania informacji w trybie komutacji pakietów i kanałów.

Jest oczywistym, że organizowany na obszarze kraju system łączności powinien spełniać te wymagania, aby móc świadczyć usługi telekomunikacyjne najwyższym organom władzy i administracji państwa, jednostkom wojsk operacyjnych, obrony terytorialnej, obrony regionalnej itp., mieć zdolność zmiany konfiguracji oraz wydzielenie określonego podsystemu łączności zapewniającego kierowanie w stanach nadzwyczajnych i dowodzenie określonymi siłami przeznaczonymi do działania na wskazanym kierunku.

Wnioski

Wymagania najwyższych organów władzy, administracji państwowej i sił zbrojnych wobec telekomunikacji są szczególne. Zaliczyć do nich należy:

- żądanie wyprzedzającej gotowości systemu w każdej sytuacji, a przede wszystkim w stanach nadzwyczajnych;
- bezpieczeństwo przekazywanych informacji i ochrona systemu;
- adaptacyjność i mobilność systemu;
- integracja rozwiązań technicznych - współdziałanie wszystkich elementów systemu informacyjnego;
- efektywność ekonomiczna rozwiązań systemowych.

W realizacji przedstawionych wymagań i zadań powinny sprzyjać:

- jednoznacznie sformułowane i skoordynowane potrzeby organów władzy i administracji w zakresie usług teleinformatycznych;
- wyraźne określenie założeń technicznych i organizacyjnych dotyczących wszystkich elementów systemu;
- możliwość wyboru najkorzystniejszych rozwiązań spełniających powyższe wymagania ogólne integrujące potrzeby użytkowników z uzwzględnieniem ich specyfiki, np. sił zbrojnych, policji, straży pożarnej, urzędów ochrony państwa, celnego, itp.

Podstawową cechą określającą stopień przydatności danego systemu telekomunikacyjnego na potrzeby najwyższych organów władzy i administracji państwa jest możliwość hermetyzacji czyli zapewnienia najważniejszym abonentom priorytetowego dostępu do świadczonych usług. Cechą sieci hermetycznych jest to, iż tworzą zamknięte systemy całkowicie niedostępne dla innych abonentów. Sieci takie, poprzez powszechne stosowanie urządzeń kryptograficznych, umożliwiają użytkownikom prowadzenie niejawnej korespondencji.

Spełnienie wymagań i potrzeb najwyższych organów władzy i administracji państwa stawianych w czasie sytuacji kryzysowych było podstawą uchwały Rady Ministrów nr 73/94 z 11.10.1994 r. w sprawie utworzenia Krajowego Systemu Łączności na potrzeby państwowe. Na mocy tej uchwały powołany został Zespół Międzyresortowy do Koordynacji Spraw Utworzenia i Eksploatacji Krajowego Systemu Łączności. Zespół ten otrzymał szereg zadań i uprawnień związanych z utworzeniem w terminie do 2005 r. niezawodnego i bezpiecznego systemu łączności do przekazywania informacji jakim powinien być Krajowy System Łączności (KSŁ). Rada Ministrów uchwałą nr 73/94 uznała także, za celowe budowę systemu Pilotowego Krajowego Systemu Łączności (KSŁ – P) jako podstawę krajowej sieci awaryjnej.

Sieć ta była planowana do zapewnienia bezpiecznej wymiany informacji (prowadzenia niejawnej korespondencji) pomiędzy ogniwami naczelnych i wojewódzkich organów władzy i administracji państwowej w sytuacjach wyjątkowych, w czasie kryzysu i wojny.

Wykonania tej uchwały podjęła się Akademia Obrony Narodowej. W pionie naukowym Akademii został powołany interdyscyplinarny zespół naukowo – badawczy z różnych placówek naukowych i instytucji centralnych.

Do realizacji tego zamierzenia wybrano wąskopasmowy system łączności z modulacją delta i cyfrowym kanałem abonenckim o przepływności 16 kb/s ze względu na jego szereg cech. Do najistotniejszych cech należy zaliczyć: kompatybilność sprzętową i programową z urządzeniami stosowanymi w Siłach Zbrojnych RP (system „STORCZYK"), elastyczność konfiguracji sieci, możliwość współpracy z urządzeniami radiodostępu z zachowaniem utajniania.

W celu zwiększenia efektywności ekonomicznej eksploatacji krajowej sieci awaryjnej planowano jej wykorzystanie również w czasie pokoju, na potrzeby centralnych i wojewódzkich organów władzy państwowej.

W wyniku prowadzonych prac został opracowany projekt i zbudowany model Pilotowego Krajowego Systemu Łączności (KSŁ-P), a następnie wdrożony przez TP S.A. do systemu telekomunikacyjnego kraju. Prowadzone pzez zespół AON prace badawcze KSŁ-P przyniosły bardzo pomyślne wyniki oraz potwierdziły celowość i potrzebę budowy tego systemu, jako jedynego spełniającego dotychczas wymagania sytuacji kryzysowych.

Jednak od realizacji tego projektu jako inwestycji centralnej ujętej w ustawie budżetowej na 1996 rok odstąpiono jesienią 1996 r. pomimo pozytywnych wyników badań i utworzonego przez TPS.A. systemu pilotowego KSŁ-P.

Doświadczenia wyniesione z powodzi 1997 roku potwierdziły pilną konieczność kontynuowania prac nad utworzeniem specjalnych systemów łączności na potrzeby obronności, bezpieczeństwa i administracji państwa oraz przystosowania krajowego systemu telekomunikacyjnego również w celu zapewnienia łączności dla zarządzania i kierowania w różnorodnych sytuacjach kryzysowych okresu pokojowego, w tym w przypadku klęsk żywiołowych i katastrof.

W tym celu Rada Ministrów uchwałą nr 86/97 z 15 października 1997r. w sprawie opracowania koncepcji systemów łączności specjalnej na potrzeby obronności, bezpieczeństwa i administracji państwa zobowiązała ministrów obrony narodowej, spraw wewnętrznych i administracji w uzgodnieniu z szefem Urzędu Ochrony Państwa do opracowania w ciągu 6 miesięcy odrębnych koncepcji łączności specjalnej, a w porozumieniu z ministrem łączności projektu nowej uchwały w sprawie utworzenia systemów realizujących te koncepcje.

Na obecnym etapie prac, wobec braku decyzji o kierunku rozwoju systemu łączności na potrzeby kierowania obronnością państwa a szczególnie stanów nadzwyczajnych, trudno rozważać szczegóły eksplotacyjno-techniczne systemu oraz podejmować kompleksowe i kosztowne prace badawczo-rozwojowe nad Krajowym Systemem Łączności.

W krajach członkowskich NATO na rzecz obronności bardzo szeroko wykorzystuje się sieć telekomunikacyjną państwa, a niezależnie od tego istnieją narodowe systemy awaryjne, realizowane głównie jako cyfrowe systemy tzw. wąskopasmowe z podstawowym cyfrowym kanałem abonenckim o przepływności 16 kbit/s.

Rolę systemu łączności kierowania obronnością państwa powinien pełnić **Krajowy System Łączności**. System ten, rozwinięty w niezbędnym zakresie w czasie pokoju, powinien być wykorzystywany przez najwyższe organa władzy i administracji państwa do przekazywania niejawnych wiadomości. Rozbudowywany głównie pod względem transmisyjnym, w stanach nadzwyczajnych realizowałby uprzywilejowany dostęp do najważniejszych abonentów i byłby podstawowym systemem łączności systemu obronnści państwa.

Zaspokojenie ciągle rosnących potrzeb użytkowników, systemów łączności w zakresie usług teleinformatycznych, będzie możliwe poprzez wykorzystanie nowych technik i technologii telekomunikacyjnych przedstawionych w podrozdziałach 3.1 – 3.15.

Technologie te zapewnią organom kierującym sytuacjami kryzysowymi niespotykane dotychczas możliwości usługowe dotyczące: szybkiej wymiany danych, transferu dużych zbiorów informacji, rozproszonego przetwarzania danych, wymiany danych w czasie rzeczywistym, przekazywanie obrazów ruchomych itp.

Społeczeństwo staje się społeczeństwem informacyjnym, gdy osiąga stopień rozwoju oraz skali i skomplikowania procesów społecznych i gospodarczych wymagający zastosowania nowych technik gromadzenia, przetwarzania, przekazywania i użytkowaniaolbrzymiej masy informacji generowanej przez owe procesy.[59] W takim społeczeństwie informacja i wynikająca z niej wiedza oraz technologie są podstawowym czynnikiem wytwórczym a wszechstronnym czynnikiem rozwoju jest wykorzystywanie teleinformatyki.

Szybsze docieranie do pełniejszych, bardziej wiarygodnych informacji ułatwia podejmowanie lepszych decyzji, szczególnie w okresie stanów nadzwyczajnych oraz szybsze zaspokajanie potrzeb społecznych i obsługę niezbędnych podmiotów gospodarczych.

Budowane podobne systemy w krajach będących członkami Unii Europejskiej i NATO charakteryzują się się wykorzystywaniem technik szerokopasmowych: ATM, ISDN, IP oraz komercyjnych systemów trankingowych. Niezależnie od stosowania nowych technologii, każdy kraj w swoich projektach budowy nowych systemów, uwzględnia istniejącą infrastrukturę telekomunikacyjną.

Dla bezkolizyjnej współpracy tych systemów dąży się do stosowania urządzeń wykonanych wg standardów ITU.

---

[59] Koncepcja krajowej i międzynarodowej infrastruktury informacyjnej przyjętej za cel wspólnych działań przez konferencję Grupy G-7 nt. społeczeństwa informacyjnego w Brukseli (luty 1995 r.).

Do współpracy z innymi systemami np. militarnym, wykonanymi wg standaryzacji STANAG i EUROCOM powinny być stosowane specjalne interfejsy (gatway'e) międzysystemowe. Z dokonanego krótkiego przeglądu nowych technik i technologii teleinformatycznych wynika, że umożliwiają one tworzenie wydzielonych sieci dla zamkniętych grup użytkowników ze specjalizowanymi usługami, co jest istotne dla tego typu zastosowań.

Przedstawiona charakterystyka mobilnych systemów radiotelefonicznych wskazuje na możliwości łatwego i wygodnego ich zastosowania w różnych uwarunkowaniach operacyjnych. Podyktowane to jest głównie zgodnością standaryzacyjną z innymi systemami, elastycznością wyboru pasma częstotliwości (dla systemów trankingowych) oraz łatwością zastosowania w koniecznych miejscach użycia systemu.

Urządzenia wykonane wg nowych technik i technologii teleinformatycznych są podatne na zarządzanie a tym samym można dokonywać rekonfiguracji systemu dopasowując go do określonych wymagań i potrzeb stanów nadzwyczajnych.

W związku z członkostwem w NATO i bliską perspektywą wejścia w struktury UE, istnieje pilna potrzeba, a wręcz konieczność kontynuacji tych prac i rozbudowy systemu łączności - teleinformatycznego (informacyjnego) kraju.

JAWNE
Zastrzeżone

WNIOSKI KOŃCOWE

Społeczeństwo informacyjne tworzy warunki wysokiej sprawności administracji publicznej, obniżenia z czasem jej kosztów, zintegrowania różnych jej części za pośrednictwem technik przetwarzania i przekazywania informacji we współpracujący ze sobą system.

Społeczeństwo informacyjne tworzy nowe formy demokracji dzięki zwiększonemu dostępowi obywateli do informacji oraz zwielokrotnionym możliwościom wyrażania i badania opinii publicznej, powstawaniu kanałów poziomej komunikacji społecznej oraz łatwości organizowania się i uczestnictwa jednostek i grup w społecznym obiegu informacji[60]. Pełne wykorzystanie potencjału demokratyzacyjnego nowych technik informacyjno-komunikacyjnych wymaga zagwarantowania prawa dostępu do informacji, w tym tworzonej i przechowywanej przez administrację publiczną.

Technologicznym fundamentem społeczeństwa informacyjnego jest proces konwergencji telekomunikacji i informatyki z radiem i telewizją, powstawanie nowoczesnej infrastruktury telekomunikacyjnej, szerokopasmowych sieci multimedialnych opartych w znacznym stopniu na instalacjach światłowodowych o ogromnej przepustowości (autostrad informacyjnych lub infostrad) - oraz przenikanie wynikaj±cych z tego technik informacyjno-komunikacyjnych do wszystkich dziedzin życia. Towarzyszy temu kapitałowa i gospodarcza integracja tych dziedzin w obrębie korporacji multimedialnych, w ramach których różne dziedziny działalności wspierają i uzupełniają się nawzajem.

W systemach telekomunikacyjnych większości państw zachodzą istotne zmiany. Zdecydowanie przyspieszono proces cyfryzacji sieci telekomunikacyjnej kraju i budowę elektronicznych central telefonicznych. Wykorzystanie tej infrastruktury teletechnicznej to także problem globalnej oceny efektywności działania systemu łączności w nowych warunkach.

System jest skuteczny jeśli dysponując określonym potencjałem, osiąga w danych warunkach i pożądanym stopniu - zamierzony cel główny. Oznacza to nie tylko ocenę możliwości systemu łączności, ale także stopnia jego wykorzystania do wykonania zadań. Sieć telekomunikacyjna państwa w okresie stanów nadzwyczajnych powinna być rozwinięta na bazie węzłów stacjonarnych jak i polowych.

---

60 Społeczeństwo informacyjnew Polsce.Założenia polityki Państwa. Krajowa Rada Radiofonii i Telewizji. Warszawa, lipiec 1996 r.

JAWNE
Zastrzeżone

W zależności od potrzeb węzły stacjonarne i polowe będą pełnić tylko różne funkcje[61] np. węzły sieci bazowej lub pomocnicze. Sieć bazowa (podstawowa) powinna być powiązana z innymi systemami tworzącymi otoczenie systemowe, w tym:

- z systemem łączności przełożonego , którym może być system łączności ND SZ RP;
- system łączności rodzajów sił zbrojnych;
- system łączności dowództwa subregionalnego NATO;
- rozwinięta sieć łączności Wielonarodowych Połączonych Sił Zbrojnych (CJTF – Combined Joint Task Force) uczestniczących w misji pokojowej.

Sieć łączności powinna być dowiązana do systemu łączności przełożonego co najmniej dwiema, niezależnymi przestrzennie liniami łączności, do co najmniej dwóch, niezależnych przestrzennie węzłów (stacjonarnych, lub polowych) systemu łączności przełożonego. Przepływność linii dowiązania do systemu łączności przełożonego powinna zapewnić terminową wymianę pełnej ilości (objętości) wymaganej informacji w obydwu relacjach, tj. : „przełożony-podwładny" i „podwładny - przełożony". Należy przyjąć, że przepływność linii dowiązania do systemu przełożonego powinna wynosić nie mniej niż 2 Mbit/s lub więcej – w przypadku wykorzystywania kanałów o niższej jakości. W przypadku wykorzystywania kanałów o niższej jakości, powinny być stosowane urządzenia wstępnej korekcji błędów, z systemami łączności podległych punktów kierowania. Zakłada się przy tym, że systemy podległe mogą być wykonane w różnych technologiach np.:

- zgodnych z technologiami wykorzystanymi np. ISDN, ATM, TCP/IP;
- w technologii cyfrowej z modulacją „delta";
- w technice analogowej.

Przepływność linii dowiązania bazowej sieci łączności do podległych systemów powinna mieścić się w przedziale 2048 kbit/s– 8 Mbit/s, z systemami łączności współdziałających (sąsiednich) oraz systemami łączności rodzajów SZ (MW, WLOP). W tym przypadku również zakłada się możliwość współpracy z systemami wykonanymi w różnych technologiach, np.: w technologii zgodnej z technologiami zastosowanymi w MSSŁ (ISDN, ATM, TCP/IP); w technologii cyfrowej z modulacją „delta" (modulacją CVSD); w technice cyfrowej z modulacją PCM oraz usługami IDN; w technice analogowej z systemem telekomunikacyjnym państwa.

[61] Sposób wykorzystania węzłów stacjonarnych i polowych jest różny w zleżności od potrzeb kolejnych etapów wdrażania systemu łączności.

JAWNE

Zastrzeżone

Współdziałanie z systemem telekomunikacyjnym państwa warunkuje zapewnienie łączności z osobami funkcyjnymi jednostek administracji państwowej funkcjonujących na obszarze objętym działaniami kryzysowymi. Należy przyjąć, że abonenci najwyższych organów władzy i administracji państwa będą w najbliższej przyszłości abonentami krajowej sieci specjalnej, która będzie posiadać dużą zgodność techniczną i technologiczną z siecią telekomunikacyjną państwa.

Wyraźne określenie roli organów administracji państwowej i ich kompetencji w budowie zintegrowanego systemu telekomunikacyjnego na potrzeby obronności państwa, a szczególnie stanów nadzwyczajnych staje się pilną koniecznością.

Już dziś jest jasne, że stowarzyszenie Polski z Unią Europejską oraz perspektywa ścisłej współpracy z NATO wymuszą na nas konieczność posiadania systemu specjalnego, kompatybilnego z systemami tych organizacji. Wynika stąd potrzeba konsultacji i wymiany doświadczeń w dziedzinie organizacji i zabezpieczenia funkcjonowania systemu łączności specjalnej z przedstawicielami państw Europy Zachodniej.

Wszystkie systemy specjalne państw UE posiadają następujące cechy:

a) są cyfrowe o kanale podstawowym 16 kbit/s i hierarchii zwielokrotnienia od 3 kanałów (48 kbit/s) do 120 kanałów (2048 kbit/s);
b) typowymi strumieniami traktowymi są 128, 256, 512, 1024 i 2048 kbit/s (USA wykorzystują także 4096 kbit/s),
c) w węzłach sieci wykorzystują automatyczne łącznice kanałów podstawowych 16 kbit/s o pojemnościach 120, 240 i 480 kanałów,
d) jako media teletransmisyjne eksploatują cyfrowe i analogowe zasoby sieci stacjonarnych, głównie dzierżawione od operatorów państwowych (również od prywatnych).

Z zasobów cyfrowych głównie dzierżawione są:

* podstawowe grupy cyfrowe 2048 kbit/s PCM (łącznice tworzą na ich bazie strumienie 120 kanałowe),
* kanały 64 kbit/s PCM (łącznice tworzą na ich bazie strumienie 4 kanałowe),

d) niezależnie od zasobów stacjonarnych wykorzystują także okresowo rozwijane polowe środki radioliniowe o przepływnościach 128...2048 kbit/s,
e) kanały podstawowe 16 kbit/s doprowadzane do abonenta, są wykorzystywane uniwersalnie do rozmów telefonicznych (przy użyciu modulacji delta) oraz do rozmaitych transmisji danych z szybkościami do 16 kbit/s. Sieć krajowa stanowi bowiem bazę rozmaitego typu
f) rządowych systemów informatycznych i zautomatyzowanego kierowania,
g) sieć charakteryzuje się dwoma poziomami zabezpieczeń (utajniania):

JAWNE

Zastrzeżone

JAWNE
Zastrzeżone

* bezpośrednio u abonenta za pomocą indywidualnych urządzeń utajniających kanału 16 kbit/s. Kanał ten jest odtajniany dopiero u adresata (zasada ciągłości utajniania),
* wszystkich traktów grupowych (międzycentralowych) za pomocą grupowych urządzeń utajniających.

Niezależnie od powyższych dwu poziomów do transmisji danych wykorzystuje się dodatkowe utajnianie programowe (w komputerach osobistych abonentów).

W ramach aktualnych tendencji rozwojowych zautomatyzowanych stanowisk kierowania i dowodzenia, wymienia się trzy grupy wymagań stawianych przed systemami łączności:

1) trwałości - a więc odporności na zakłócenia, dużej niezawodności i żywotności, co wiąże się z budową sieci o strukturze rozproszonej (siatkowej);
2) skrytości - utajnianie z wymagana mocą kryptograficzną;
3) mobilności - to jest zachowania ciągłości łączności w czasie przemieszczania się stanowisk kierowania i dowodzenia.

System łączności (teleinformatyczny) powinien umożliwiać przesyłanie tych informacji do korespondentów w sposób bezpieczny (utajniony). Rekonfiguracja systemu polegająca na dynamicznej zmianie funkcji i aktywności poszczególnych stanowisk, dokonywana w celu dostosowanie struktury kierowania obroną państwa do aktualnej sytuacji bojowej, możliwości realizacyjnych i potrzeb pociągać będzie za sobą rekonfigurację systemu łączności.

System łączności powinien nadążać za dynamicznymi zmianami ich struktury organizacyjnej. Realizacja zadań stawianych nowoczesnemu systemowi kierowania obroną państwa będzie integralnie związana z permanentną dynamiczną rekonfiguracją jego struktury. Rekonfiguracja struktury polegać będzie głównie na zmianie funkcji poszczególnych stanowisk kierowania spowodowanej aktualną sytuacją.

System łączności budowany na potrzeby systemu kierowania, przy zapewnieniu wysokiej niezawodności działania, powinien zapewnić jej ciągłość oraz umożliwić wymianę informacji między poszczególnymi stanowiskami w postaci różnego typu wiadomości i baz danych.

Spełnienie tych wymagań możliwe jedynie w nowoczesnych systemach organizacji łączności w których wszystkie ogniwa (węzły komutacyjne) połączone ze sobą na zasadzie równorzędności tworzą strukturę niehierarchiczną. Stosowanie dynamicznego poszukiwania abonenta w sieci czyni taki system łączności odpornym na zniszczenia i podatnym na dynamiczną rekonfigurację całej sieci.

JAWNE
Zastrzeżone

Docelowo system łączności (teleinformatyczny) na potrzeby kierowania obronnością i bezpieczeństwem państwa według przyjętych założeń, powinien stanowić zintegrowany pod względem organizacyjnym i technicznym zespół węzłów, traktów i linii łączności (stałych i budowanych środkami polowymi), urządzeń komutacyjnych oraz końcowych zapewniających korzystanie z niezbędnych usług telekomunikacyjnych wszystkim organom kierowania i dowodzenia funkcjonującym w ramach tego systemu.

Szybki postęp w telekomunikacji w dziedzinie transmisji głównie zaś szerokie wykorzystanie techniki cyfrowej i światłowodowej umożliwia stworzenie jednolitych systemów teleinformatycznych opartych w całości o cyfrowe kanały łączności.

Dla realizacji przedstawionej, ogólnej wizji systemu koniecznym będzie:

- opracowanie szczegółowej koncepcji systemu łączności (informacyjnego) uwzględniającej potrzeby organów zarządzających kryzysami;
- poddanie koncepcji opiniowaniu odpowiednim środowiskom zajmującym się zbieżnymi projektami;
- opracowanie założeń techniczno-operacyjnych z uwzględnieniem opinii w/w środowisk;
- opracowanie projektu wstępnego systemu łączności i zbudowanie sieci pilotowej;
- weryfikacja koncepcji i założeń;
- opracowanie projektu technicznego reprezentatywnego modułu systemu łączności;
- przeprowadzenie badań wstępnych i końcowych modelu systemu łączności.

Wydaje się, że zaproponowany sposób realizacji tego projektu zminimalizuje ryzyko jego opracowania.

Przedstawiciele z różnych sektorów muszą zatem uczestniczyć w projektowaniu i integrowaniu sieci teleinformatycznej do przekazywania informacji w stanach nadzwyczajnych. Wybór docelowej struktury narodowego (krajowego) systemu łączności - teleinformatycznego musi być poprzedzony wnikliwą analizą oraz pracami koncepcyjnymi i badawczymi.

BIBLIOGRAFIA

1. Adamczewski P. Zintegrowane systemy informatyczne, Mikon, Warszawa 1998.
2. AUTOKO 90: roll-out into the age of digital communications. Defence Report Nr 42 1/96. SIEMENS.
3. Balcerowicz B., Strategia. Kwestie nie tylko terminologiczne, Zeszyty Naukowe AON 1/97, Warszawa 1997.
4. Balcerowicz B., Wybrane problemy obronności państwa - materiał studyjny, AON, Warszawa 1997.
5. Barczak A., Inteligentne sieci telekomunikacyjne – aspekty metodologiczne i techniczno – projektowe, WSOWŁ, Zegrze 1994.
6. Biuro Prasy i Informacji MON, Strategia obronności Rzeczpospolitej Polskiej, Studia i materiały nr 53,Warszawa 2000.
7. M.Bromirski. Systemy łączności wojskowej. Perspektywy rozwoju. Czas telekomunikacji Nr 9/1998.
8. CTM 300 Tactical. Line of Sight Radio for Tactical and Strategic Applications. Materiały firmowe SIEMENS.
9. Czarnecki P., Jajszczyk A., Lubacz J., Standardy zarządzania sieciami OSI/NM, TMN, WEFP, Poznań 1995.
10. Department of the Army. C4I Technical Architecture. Version 3.1. 31 March 1995.
11. Dąbrowski A., Kula S. Systemy i sieci SDH, WkiŁ, Warszawa 1996.
12. Drost M. , Siły niemilitarne w obronie RP, Rozprawa habilitacyjna, AON, Warszawa, 1998.
13. Dudek Z.T., Zagrobelny T., Ewolucja sieci telekomunikacyjnych od analogowych do szerokopasmowych, Przegląd Telekomunikacyjny nr 6, Warszawa 1992.
14. Dworecki S., Od konfliktu do wojny, BUWIK, Warszawa 1996.
15. Ericsson's scalable frame relay/ATM solution. By Alessandro Badiale. The Telecommunications Technology Journal – Internet Access Services, 1998.
16. Gąsiorek K., Skobel W., Rola i zadania województwa w systemie obronnym państwa w czasie pokoju, zagrożenia (kryzysu) i wojny, AON, Warszawa 1998.
17. Glasgall J. Połowniak A. Perspektywiczny model systemu łączności kierowania obronnością państwa w stanach nadzwyczajnych. Rozprawa doktorska. AON,

JAWNE
Zastrzeżone

Warszawa 1998.

18. Hołubowicz W., Płóciennik P., Różański A., Systemy łączności bezprzewodowej, Holkom, Poznań 1997.
19. Information technology solutions for EUROPE'S Security and Economic Growth. Euro Comm 2000. Munich, Germany 17-19 May, 2000.
20. J.Jach. Łączność wojskowa. System uwarunkowany ograniczeniami pasm i wymaganiami bezpieczeństwa. CZAS TELEKOMUNIKACJI Nr 9/1998.
21. Kabala E., Kompetencje i zadania organów władzy ustawodawczej i wykonawczej w zakresie bezpieczeństwa i obronności państwa, AON, BBN, Warszawa 1998.
22. Kalinowski R., Obrona cywilna w Rzeczypospolitej Polskiej, Rozprawa habilitacyjna, AON, Warszawa, 1998.
23. Kamiński F., Prawo telekomunikacyjne a prawo o konkurencji, KST'98, Bydgoszcz 1998.
24. Kitler W., Obrona narodowa. Konieczność nowego podejścia., Myśl Wojskowa 4/1997, Warszawa 1997.
25. Konstytucja Rzeczypospolitej Polskiej, Warszawa, 2 kwietnia 1997.
26. Kościelnik D., ISDN-cyfrowe sieci zintegrowane usługowo. WKŁ, Warszawa. 1996.
27. Koziej S., Wołkowicz F., Podstawowe założenia polityki bezpieczeństwa i strategii obronnej, AON, DSO MON, Warszawa 1998.
28. Laszczkowski Cz., Kształtowanie bezpieczeństwa narodowego RP, BBN, Warszawa 1993.
29. Marczak J., Dworecki S., Piedziuk E., Duda W., Operacyjne przygotowanie obszaru kraju do obrony. Wiedza Obronna nr 2/181/, Warszawa 1997.
30. Materiały z Konferencji Systemów Obronnego i Łączności - KSOŁ, AON, Warszawa 1994÷97.
31. Naczelny Komitet ds. Planowania Zagrożeń Cywilnych NATO, SCEPC-struktura i cele, Materiały NATO, Bruksela 1996.
32. Organizacja Traktatu Północnoatlantyckiego, NATO Vademecum, Bellona 2000
33. Ostrowski P., Lubacz J., Przegląd zagadnień ISDN, IT PW, Warszawa 1991.
34. Pawłowski J., Marczak J., O obronie militarnej Polski przełomu XX-XXIw., Bellona, Warszawa 1995.
35. Piedziuk E., Podstawowe dane Krajowego Systemu Łączności – pilota, AON,

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Warszawa 1996.

36. Piedziuk E., - kier. nauk. Słownik pojęć z zakresu telekomunkacji w zastosowaniach cywilnych i wojskowych. AON, Warszawa 1996.
37. Piedziuk E., System łączności w stanach nadzwyczajnych z punktu widzenia potrzeb obronnych państwa. AON, Warszawa 1998.
38. Piedziuk E., Telekomunikacja na potrzeby obronności państwa. AON, Warszawa 1997.
39. Praca zbiorowa pod kier. Balcerowicza B. Przygotowanie i prowadzenie wojny obronnej przez Polskę po 2000 roku. "Kappa". AON, Warszawa 1998. .
40. Praca zbiorowa pod kierunkiem Zdzisława Papira. Sieci z komutacją pakietów od X.25 do Frame Relay i ATM. Wydawnictwo Fundacji Postępu Telekomunikacji. Kraków 1996.
41. Praca zbiorowa pod redakcją Krzysztofa Wajdy. Budowa sieci komputerowych w technologii ATM. Wydawnictwo Fundacji Postępu Telekomunikacji. Kraków 1997.
42. Praca zbiorowa, zitegrowane systemy łączności, WAT ISŁ WEL, Warszawa 1998.
43. Seminaria specjalistyczne Instytutu Łączności, Łączność w stanach nadzwyczajnych zagrożeń. Insytut Łączności, Warszawa 2000.
44. Sienkiewicz P.-red. nauk., Wystarczalność obronna, Bellona, Warszawa 1996.
45. Steibrink B., Multimedia u progu technologii XXI wieku. Robomatic Wrocław 1993.
46. Stępak J., Potencjały militarne państw sąsiadujących z Polską (Analiza porównawcza), AON, Warszawa 1998.
47. Stoner James A.F., Carles Wankel, Kierowanie. PWE, Warszawa 1994.
48. Systemy i sieci SDH. Praca zbiorowa pod redakcją A.Dąbrowskiego i S.Kuli. Wydawnictwa Komunikacji i Łącznosci. Warszawa 1996.
49. Średniawa M. Sieci inteligentne, IŁ Pol.it. W-wska, Warszawa 1998.
50. J. Świdziński. Bezpieczeństwo, mienie, życie łączność. CZAS TELEKOMUNIKACJI Nr 9/1998.
51. Tadeusiak Z.Koncepcja i wykorzystanie systemu łączności o strukturze sieciowej na potrzeby kierowania obroną państwa.Rozprawa doktorska.AON.Warszawa.1997.
52. Tarasiuk B., Czarniecki A., Suwiński W., Kierowanie obronnością państwa w czasie pokoju, kryzysu i wojny, Materiał studyjny, AON, Warszawa 1998 .

JAWNE
Zastrzeżone

ZAŁĄCZNIKI

Załącznik nr 1

WYCIĄG
Z KONSTYTUCJI RZECZYPOSPOLITEJ POLSKIEJ ZAWIERAJĄCY ARTYKUŁY DOTYCZĄCE OBRONNOŚCI PAŃSTWA

Rozdział I

RZECZPOSPOLITA

Art.5.

Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju.

Art.8.

1. Konstytucja jest najwyższym prawem Rzeczpospolitej Polskiej.
2. Przepisy Konstytucji stosuje się bezpośrednio, chyba że Konstytucja stanowi inaczej.

Art.26.

1. Siły Zbrojne Rzeczpospolitej Polskiej służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic.
2. Siły Zbrojne zachowują neutralność w sprawach politycznych oraz podlegają cywilnej i demokratycznej kontroli.

Rozdział II

WOLNOŚĆ, PRAWA I OBOWIĄZKI
CZŁOWIEKA I OBYWATELA
ŚRODKI OCHRONY WOLNOŚCI I PRAW

Art.85.

1. Obowiązkiem obywatela polskiego jest obrona Ojczyzny.
2. Zakres obowiązku służby wojskowej określa ustawa.
3. Obywatel, któremu przekonania religijne lub wyznawane zasady moralne nie pozwalają na odbywanie służby wojskowej, może być obowiązany do służby zastępczej na zasadach określonych w ustawie.

Rozdział III

ŹRÓDŁA PRAWA

Art. 87.

1. Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia.
2. Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są na obszarze działania organów, które je ustanowiły, akty prawa miejscowego.

Art. 89.

1. Ratyfikacja przez Rzeczpospolitą Polską umowy międzynarodowej i jej wypowiedzenie wymaga uprzedniej zgody wyrażonej w ustawie, jeżeli umowa dotyczy:
pokoju, sojuszy, układów politycznych lub układów wojskowych.

Art.91.

1. Ratyfikowana umowa międzynarodowa, po jej ogłoszeniu w Dzienniku Ustaw Rzeczypospolitej Polskiej, stanowi część krajowego porządku prawnego i jest bezpośrednio stosowana, chyba że jej stosowanie jest uzależnione od wydania ustawy.

Rozdział IV

ORGANIZACJA I DZIAŁANIE

Art. 116.

1. Sejm decyduje w imieniu Rzeczypospolitej Polskiej o stanie wojny i o zawarciu pokoju.
2. Sejm może podjąć uchwałę o stanie wojny jedynie w razie zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umów międzynarodowych wynika zobowiązanie do wspólnej obrony przeciwko agresji. Jeżeli Sejm nie może zebrać się na posiedzenie, o stanie wojny postanawia Prezydent Rzeczypospolitej.

Art.117.

Zasady użycia Sił Zbrojnych poza granicami Rzeczypospolitej Polskiej określa ratyfikowana umowa międzynarodowa lub ustawa. Zasady pobytu obcych wojsk na terytorium Rzeczypospolitej Polskiej i zasady przemieszczania się ich przez to terytorium określają ratyfikowane umowy międzynarodowe lub ustawy.

Rozdział V

PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

Art.126.

2. Prezydent Rzeczypospolitej czuwa nad przestrzeganiem Konstytucji, stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium.

Art.134.

1. Prezydent Rzeczypospolitej Polskiej jest najwyższym zwierzchnikiem Sił Zbrojnych Rzeczypospolitej Polskiej.
2. W czasie pokoju Prezydent Rzeczypospolitej sprawuje zwierzchnictwo nad Siłami Zbrojnymi za pośrednictwem Ministra Obrony Narodowej.
3. Prezydent Rzeczypospolitej mianuje Szefa Sztabu Generalnego i dowódców rodzajów sił zbrojnych na czas określony. Czas trwania kadencji, tryb i warunki odwołania przed jej upływem określa ustawa.
4. Na czas wojny Prezydent Rzeczypospolitej, na wniosek Prezesa Rady Ministrów, mianuje Naczelnego Dowódcę Sił Zbrojnych. W tym samym trybie może on Naczelnego Dowódcę Sił Zbrojnych odwołać. Kompetencje Naczelnego Dowódcy Sił Zbrojnych i zasady jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej określa ustawa.
5. Prezydent Rzeczypospolitej Polskiej, na wniosek Ministra Obrony Narodowej, nadaje określone w ustawach stopnie wojskowe.
6. Kompetencje Prezydenta Rzeczypospolitej, związane ze zwierzchnictwem nad Siłami Zbrojnymi, szczegółowo określa ustawa.

Art. 135.

Organem doradczym Prezydenta Rzeczypospolitej w zakresie wewnętrznego i zewnętrznego bezpieczeństwa państwa jest Rada Bezpieczeństwa Narodowego.

Art. 136.

W razie bezpośredniego, zewnętrznego zagrożenia państwa Prezydent Rzeczypospolitej, na wniosek Prezesa Rady Ministrów, zarządza powszechną lub częściową mobilizację i użycie Sił Zbrojnych do obrony Rzeczypospolitej.

Art. 141.

1. W sprawach szczególnej wagi Prezydent Rzeczypospolitej może zwołać Radę Gabinetową. Radę Gabinetową tworzy Rada Ministrów obradująca pod przewodnictwem Prezydenta Rzeczypospolitej.
2. Radzie Gabinetowej nie przysługują kompetencje Rady Ministrów.

JAWNE
Zastrzeżone

Art. 144.

1. Prezydent Rzeczypospolitej, korzystają ze swoich konstytucyjnych i ustawowych kompetencji, wydaje akty urzędowe.
2. Akty urzędowe Prezydenta Rzeczypospolitej wymagają dla swojej ważności podpisu Prezesa Rady Ministrów, który przez podpisanie aktu ponosi odpowiedzialność przed Sejmem.

Przepis ust. 2 nie dotyczy:

- zwoływania Rady Gabinetowej,
- powoływania i odwoływania członków Rady Bezpieczeństwa Narodowego.

Rozdział VI

RADA MINISTRÓW I ADMINISTRACJA RZĄDOWA

Art. 146.

1. Rada Ministrów prowadzi politykę wewnętrzną i zagraniczną Rzeczypospolitej Polskiej.
2. Do Rady Ministrów należą sprawy polityki państwa nie zastrzeżone dla innych organów państwowych i samorządu terytorialnego.
3. Rada Ministrów kieruje administracją rządową.
4. W zakresie i na zasadach określonych w Konstytucji i ustawach Rada Ministrów w szczególności:

7) zapewnia bezpieczeństwo wewnętrzne państwa.

8) zapewnia bezpieczeństwo zewnętrzne państwa.

11) sprawuje ogólne kierownictwo w dziedzinie obronności kraju oraz określa corocznie liczbę obywateli powoływanych do czynnej służby wojskowej.

Art. 152.

1. Przedstawicielem Rady Ministrów w województwie jest wojewoda.

Rozdział VII

SAMORZĄD TERYTORIALNY

Art. 164.

1. Podstawową jednostką samorządu terytorialnego jest gmina.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Rozdział IX
STANY NADZWYCZAJNE

Art. 228.

1. W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej.
2. Stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości.
3. Zasady działania organów władzy publicznej oraz zakres, w jakim mogą zostać ograniczone wolności i prawa człowieka i obywatela w czasie poszczególnych stanów nadzwyczajnych określa ustawa.
4. Ustawa może określić podstawy, zakres i tryb wyrównywania strat majątkowych wynikających z ograniczenia w czasie trwania stanu wyjątkowego wolności i praw człowieka i obywatela.
5. Działania podjęte w wyniku wprowadzenia stanu nadzwyczajnego muszą odpowiadać stopniowi zagrożenia i powinny zmierzać do jak najszybszego przywrócenia normalnego funkcjonowania państwa.

Art. 229.

W razie zewnętrznego zagrożenia państwa, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić stan wojenny na części lub na całym terytorium państwa.

Art. 230.

1. W razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić, na czas oznaczony, nie dłuższy niż 90 dni, stan wyjątkowy na części lub na cały terytorium państwa.

Art. 231.

Rozporządzenie o wprowadzeniu stanu wojennego lub wyjątkowego Prezydent Rzeczypospolitej przedstawia Sejmowi w ciągu 48 godzin od podpisania rozporządzenia.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Sejm niezwłocznie rozpatruje rozporządzenia Prezydenta Rzeczypospolitej. Sejm może je uchylić bezwzględną większością głosów w obecności co najmniej połowy ustawowej liczby posłów.

Art. 232.

W celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia Rada Ministrów może wprowadzić na czas oznaczony, nie dłuższy niż 30 dni, stan klęski żywiołowej na części lub na całym terytorium państwa. Przedłużenie tego stanu może nastąpić za zgodą Sejmu.

Art. 234.

1. Jeżeli w czasie stanu wojennego Sejm nie może zebrać się na posiedzenie, Prezydent Rzeczypospolitej na wniosek Rady Ministrów wydaje rozporządzenia z mocą ustawy w zakresie i granicach określonych w art. 228 ust. 3-5. Rozporządzenia te podlegają zatwierdzeniu przez Sejm na najbliższym posiedzeniu.
2. Rozporządzenia, o których mowa w ust. 1, mają charakter powszechnie obowiązującego prawa.

JAWNE
Zastrzeżone

JAWNE
Zastrzeżone

Załącznik nr 2.

MOŻLIWE STANY W STOSUNKACH MIĘDZYPAŃSTWOWYCH I MIĘDZYNARODOWYCH. (wariant)*

L.p.	Klasa stanu	Charakterystyczne cechy
1	2	3
1	Bezpieczeństwo	• suwerenne traktowanie podmiotów we wzajemnych stosunkach międzypaństwowych i międzynarodowych; • poszanowanie integralności terytorialnej; • partnerska współpraca wielodziedzinowa (polityczna, społeczna, ekonomiczna, wojskowa itp.; • stabilność konstruktywnych stosunków międzynarodowych i międzypaństwowych; • wola politycznego i pokojowego rozstrzygania wszelkich spornych problemów; • zawieranie sojuszy (umów, porozumień, traktatów itp.); • integralność (spójność) społeczeństwa,
2	"zimny pokój"	• suwerenne traktowanie podmiotów we wzajemnych stosunkach międzypaństwowych i międzynarodowych; • poszanowanie integralności terytorialnej; • ograniczanie współpracy (przynajmniej w niektórych dziedzinach); • niechęć do nawiązywania lub kontynuowania współpracy; • brak zaangażowania (neutralność lub obojętność); niechęć lub odmowa zawierania porozumień itp.),
3	Kryzys	• suwerenne traktowanie podmiotów we wzajemnych stosunkach międzypaństwowych i międzynarodowych; • poszanowanie integralności terytorialnej; • zawieszenie współpracy; • zawieszenie wcześniej zawartych porozumień; • odmowa negocjacji w spornych problemach; • "nagłaśnianie" (upowszechnianie) sprzecznych interesów, dążeń i aspiracji; • nasilanie nieprzyjaznych działań i zachowań; • stawianie ultymatywnych warunków;
4	"zimna" wojna	• ograniczanie suwerenności we wzajemnych i międzynarodowych stosunkach oraz izolowanie na arenie międzynarodowej; • nierówno prawne traktowanie podmiotów we wzajemnych i międzynarodowych stosunkach (ograniczanie współpracy, zwiększanie zobowiązań, wymuszanie ustępstw, stosowanie restrykcji itp.) • ingerowanie w wewnętrzne sprawy innego podmiotu pod dowolnym pretekstem; • brak woli do partnerskiego traktowania w stosunkach międzynarodowych ; • odmowa poszukiwania kompromisowych rozstrzygnięć w spornych problemach; • "zamrożenie" współpracy oraz wcześniej zawartych porozumień i umów; • nasilenie dywersji politycznej; • podsycanie sprzeczności narodowych, etnicznych i religijnych; • podtrzymywanie napięcia i poczucia zagrożenia militarnego; • dążenie do uzyskania przewagi militarnej (wymuszony wyścig zbrojeń); • izolacja gospodarcza (embargo na dostawy surowców, nowoczesnych technologii, myśli technicznej itp.); • zawarcie rozejmu (czasowe i warunkowe zawieszenie działań zbrojnych); • nieformalne wspieranie "ruchów" destabilizujących sytuację wewnętrzną;

* Opracował zespół autorski pod kier. gen. B. Balcerowicza. Przygotowanie i prowadzenie wojny obronnej przez Polskę po 2000 roku, praca n-b „KAPPA". AON W-wa 1996 r.

JAWNE
Zastrzeżone

1	2	3
5	Zagrożenie pozamilitarne	• ograniczanie suwerenności we wzajemnych i międzynarodowych stosunkach; • ingerowanie w wewnętrzne sprawy innego podmiotu pod dowolnym pretekstem; • nierówno prawne traktowanie podmiotów we wzajemnych i międzynarodowych stosunkach (ograniczanie współpracy, zwiększanie zobowiązań, wymuszanie ustępstw, stosowanie restrykcji, wycofanie klauzuli najwyższego uprzywilejowania, zwiększanie opłat celnych, zerwanie wymiany handlowej itp.); • brak woli do partnerskiego traktowania w stosunkach międzynarodowych; • odmowa poszukiwania kompromisowych rozstrzygnięć w spornych problemach; • zerwanie współpracy i wcześniej zawartych porozumień sojuszniczych; • eskalacja żądań, wymuszanie ustępstw kosztem interesów drugiej strony; • incydentalne stosowanie przemocy fizycznej (zbrojnej) niezinstytucjonalizowanej;
6	Zagrożenie militarne	• jednostronne wymówienie lub zerwanie wcześniej zawartych porozumień i traktatów międzypaństwowych; • akty naruszenie suwerenności i integralności terytorialnej innego podmiotu (państwa); • zastraszanie militarne (demonstrowanie siły militarnej, manewry wojskowe w strefie przygranicznej, blokada militarna, szantaż militarny itp.); • napady, akcje i incydenty zbrojne na obiekty graniczne i w strefie przygranicznej; • sabotaż i dewastacja obiektów strategicznych na obszarze innego podmiotu; • akty dywersji i napady bojówek, prowokacja militarna itp. Formy fizycznego wywierania nacisku; • zbrojne wspieranie przez siły innego państwa, w formie niezinstytucjonalizowanej, konfliktu wewnętrznego (przewrotu, puczu, zamachu stanu, wojny domowej itp.).
7	Konflikt zbrojny	• konflikt wewnętrzny (wojna domowa) o podłożu społecznym, ekonomicznym, politycznym, narodowościowym, etnicznym, religijnym itp.; • interwencja zbrojna obcych wojsk na obszarze suwerennego państwa w celu udzielenia pomocy władzom legalnym lub wsparcia działań podmiotów nielegalnych (przewrót, pucz, zamach stanu itp.) • inwazja (napaść) zbrojna na państwo suwerenne z zamiarem wyegzekwowania swoich żądań; • incydent zbrojny graniczny lub w strefie przygranicznej na tle praw mniejszości narodowościowych lub roszczeń terytorialnych sąsiedniego państwa; • konflikt lokalny na tle jw.; • konflikt międzypaństwowy o podłożu ekonomicznym, terytorialnym, etnicznym, narodowościowym itp.; • konflikt regionalny o podłożu jw.
8	Wojna	• działania zbrojne międzypaństwowe, regionalne, kontynentalne lub światowe, o podłożu jw., w zabezpieczeniu materialnym w których uczestniczy przynajmniej część gospodarki narodowej stron biorących w nich czynny udział.

Wykonano w 3 egz.
Egz. nr 1÷3 – Dz.Z.N. B.G. AON
RWD 10/86 Z-1 /P/
Sporządził: E. Piedziuk
Wykonała: U. Jaraszek

BIBLIOTEKA NIEJAWNA Akademii Obrony Narodowej Nr ewid. 2-9/5
2-608/5 II 1