



AKADEMIA OBRONY NARODOWEJ

Do użytku służbowego

Egz. Nr



Płk dr inż. Eugeniusz PIEDZIUK

TELEKOMUNIKACJA NA POTRZEBY OBRONNOŚCI PAŃSTWA

Biblioteka Główna
Akademii Obrony Narodowej
S/3730



05-003730-004-0

WARSZAWA

53589

1997

AKADEMIA

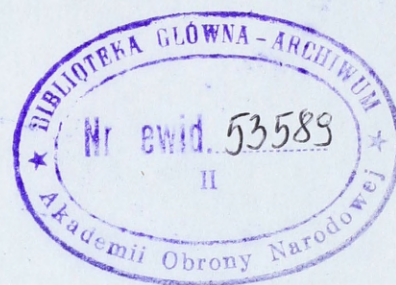
OBRONY

NARODOWEJ

ZAKŁAD ZARZĄDZANIA SYSTEMAMI INFORMACYJNYMI

Do użytku służbowego

Egz. nr



Płk dr inż. Eugeniusz PIEDZIUK

**TELEKOMUNIKACJA
NA POTRZEBY
OBRONNOŚCI PAŃSTWA**



Praca została wykonana na podstawie opracowań teoretycznych Biblioteki Głównej AON oraz materiałów:

- Biura Spraw Obronnych Ministerstwa Łączności;
- Departamentu Systemu Obronnego Ministerstwa Obrony Narodowej;
- Wojskowej Akademii Technicznej;
- Wojskowego Instytutu Łączności;
- Instytutu Łączności;
- Biura Spraw Obronnych i Ochrony TP S.A.

SPIS TREŚCI

I. BEZPIECZEŃSTWO PAŃSTWA. POJĘCIA I KATEGORIE.....	4
II. SYSTEM OBRONNY RP.....	6
1. STRUKTURA SYSTEMU OBRONNEGO.....	6
1.1. Układ militarny.....	7
1.2. Układ pozamilitarny.....	9
1.3. System kierowania obronnością (obroną narodową).....	11
2. ZADANIA SYSTEMU OBRONNEGO.....	11
2.1. Przygotowania obronne w czasie pokoju.....	11
2.2. Kierowanie obronnością w czasie zagrożenia i wojny.....	13
2.3. Stanowiska kierowania.....	14
III. ŁĄCZNOŚĆ W OPERACYJNYM PRZYGOTOWANIU OBSZARU KRAJU DO OBRONY	15
1. RYS HISTORYCZNY	15
2. PRZEDSIĘWZIĘCIA PRZYGOTOWANIA SYSTEMU TELEKOMUNIKACYJNEGO NA RZECZ OBRONNOŚCI	18
IV. INFRASTRUKTURA TELEKOMUNIKACYJNA KRAJU. KIERUNKI ROZWOJU	23
1. STAN INFRASTRUKTURY TELEKOMUNIKACYJNEJ KRAJU.....	23
1.1. Operatorzy telekomunikacyjni.....	23
1.2. Systemy radiowe.....	25
2. KIERUNKI ROZWOJU TELEKOMUNIKACJI W OPARCIU O NOWE TECHNIKI I TECHNOLOGIE.....	28
2.1. Tendencje rozwojowe systemów teletransmisyjnych PDH, ISDN, SDH, ATM.....	29
2.2. Sieci telekomunikacyjne.....	35
V. POTRZEBY TELEKOMUNIKACJI W CELU DOSTOSOWANIA DO UNII EUROPEJSKIEJ I NATO.....	39
1. WSKAŹNIKI OCENY ŁĄCZNOŚCI I SYSTEMÓW ŁĄCZNOŚCI.....	40
2. WSPÓŁDZIAŁANIE SYSTEMÓW ŁĄCZNOŚCI.....	45
3. ZMIANY W SYSTEMIE TELEKOMUNIKACYJNYM PROPONOWANE PRZEZ KOMPENDIUM ŁĄCZNOŚCI CYWILNEJ	48
3.1. Koordynacja działań w sytuacjach kryzysowo - wojennych.....	49
3.2. Działania i środki do uwzględnienia w procesie planowania obronnego	50
3.3. Eksploatacja sieci.....	52
4. NORMY PROPONOWANE PRZEZ NATO.....	55
VI. ZAGROŻENIA SYSTEMU TELEKOMUNIKACYJNEGO W CZASIE POKOJU, KRYZYSU I WOJNY ORAZ METODY OCHRONY	57
1. ZAGROŻENIA ZEWNĘTRZNE SYSTEMU TELEKOMUNIKACYJNEGO.....	57
1.1. Zagrożenia w czasie pokoju.....	57
1.2. Zagrożenia w czasie kryzysu i wojny.....	60
2. SKUTKI ODDZIAŁYWAŃ W CZASIE KRYZYSU I WOJNY	68
2.1. Oddziaływanie klęsk żywiołowych i katastrof ekologicznych	69
2.2. Oddziaływanie celowe w czasie kryzysu i konfliktu zbrojnego	70
3. ZASADY PRZYGOTOWANIA OBRONNEGO SIECI TELEKOMUNIKACYJNEJ.....	73
3.1. Uodpornienia.....	75
3.2. Bezpieczeństwo informacji.....	80
BIBLIOGRAFIA	87

I. BEZPIECZEŃSTWO PAŃSTWA. POJĘCIA I KATEGORIE

Bezpieczeństwo narodowe nazywane również bezpieczeństwem państwa - obejmuje problematykę przeciwstawiania się wszelkim zagrożeniom dla istnienia i rozwoju narodu, zarówno zewnętrznym jak i wewnętrznym. Obecnie na świecie dąży się do integracji systemów bezpieczeństwa narodowego i międzynarodowego. Wraz ze zmianami politycznymi i militarnymi ostatnich lat istotnym stało się dążenie Polski do zapewnienia sobie bezpieczeństwa w ramach NATO.

Integracja z NATO nie jest celem samym w sobie, jest to jedynie etap na drodze do zapewnienia sobie możliwości osiągnięcia celu nadrzędnego - zagwarantowania suwerenności i nienaruszalności terytorialnej oraz rozwoju gospodarczego.

W tym celu Rzeczpospolita Polska utrzymuje i doskonali swój system bezpieczeństwa, a w tym głównie system obronny państwa.

Jak we wszystkich dziedzinach życia, tak również w dziedzinie bezpieczeństwa ważna jest jednolita interpretacja podstawowych pojęć.

- 1) **bezpieczeństwo polityczne** - obejmuje przygotowanie naczelných organów władzy i administracji państwowej do przeciwstawienia się zagrożeniom politycznym państwa (zarówno wewnętrznym, jak i zewnętrznym);
- 2) **bezpieczeństwo ekonomiczne** - obejmuje przygotowanie naczelných organów władzy i administracji państwowej do przeciwstawienia się zagrożeniom ekonomicznym;
- 3) **obronność (bezpieczeństwo obronne lub wojenne)** - przygotowanie zwłaszcza sił zbrojnych do skutecznego przeciwstawienia się zagrożeniom wojennym;
- 4) **bezpieczeństwo cywilizacyjne, w tym ekologiczne** - obejmuje na przykład likwidację skutków katastrof ekologicznych;
- 5) **bezpieczeństwo publiczne** - dotyczy przeciwstawiania się wszelkim zagrożeniom struktur państwa, porządku publicznego, ochrony życia i zdrowia obywateli.

W tym miejscu celowym byłoby zwrócić uwagę na zagrożenia, zwłaszcza zagrożenia wojenne. Zagrożenia wojenne są szczególnym rodzajem zagrożeń państwa, skierowane są bowiem w podstawy jego istnienia. Jest to zestaw różnorodnych zagrożeń występujących

jednocześnie, wśród których główną rolę odgrywa zagrożenie militarne. Wojna współczesna, obejmuje nie tylko działania zbrojne, ale także różnorodne działania poza zbrojne (społeczne, ekonomiczne itp.). Z tego względu zagrożenie wojenne jest pojęciem szerszym niż zagrożenie militarne.

Specyficzną odmianą zagrożeń wojennych, w chwili obecnej dostrzeganych jako jedne z najbardziej prawdopodobnych, są zagrożenia kryzysowe, będące następstwem kryzysu polityczno-militarnego w otoczeniu państwa, czyli w sytuacji, w której nie występuje bezpośrednia groźba agresji, ale która stwarza zagrożenia pośrednie.

Obronność - dotyczy przeciwstawiania się zagrożeniom wszelkimi posiadanymi środkami, a przede wszystkim militarnym, stanowiącym sedno zagrożeń wojennych.

Kształtowanie obronności 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 w konsekwencji oznacza, że polityka i strategia bezpieczeństwa państwa składa się z polityki i strategii obronnej, polityki i strategii bezpieczeństwa: polityczno-społecznego, ekonomicznego, publicznego itp.

1. Polityka obronna - część polityki bezpieczeństwa państwa

2. Strategia obronna - jest częścią polityki obronnej (jednocześnie część szerszej strategii bezpieczeństwa narodowego). Zajmuje się ona sposobami realizacji polityki obronnej.

3. Doktryna obronności - stanowi zestaw obowiązujących w danym czasie celów obronnych i sposobów ich osiągania (jest jednocześnie częścią szerszej doktryny bezpieczeństwa narodowego). Doktryna obronności - zawarta w oficjalnych dokumentach państwowych zawiera w swej istocie strategiczną decyzję realizacji polityki obronnej.

Skonkretyzowanie i uszczegółowienie strategii i doktryny obronnej to strategia i doktryna militarna. Ich wyróżniającą cechą jest rodzaj środka obronnego, jakim są siły zbrojne. Strategia militarna zajmuje się przygotowaniem i użyciem sił zbrojnych, doktryna militarna - stanowi koncepcję przygotowania i użycia sił zbrojnych.

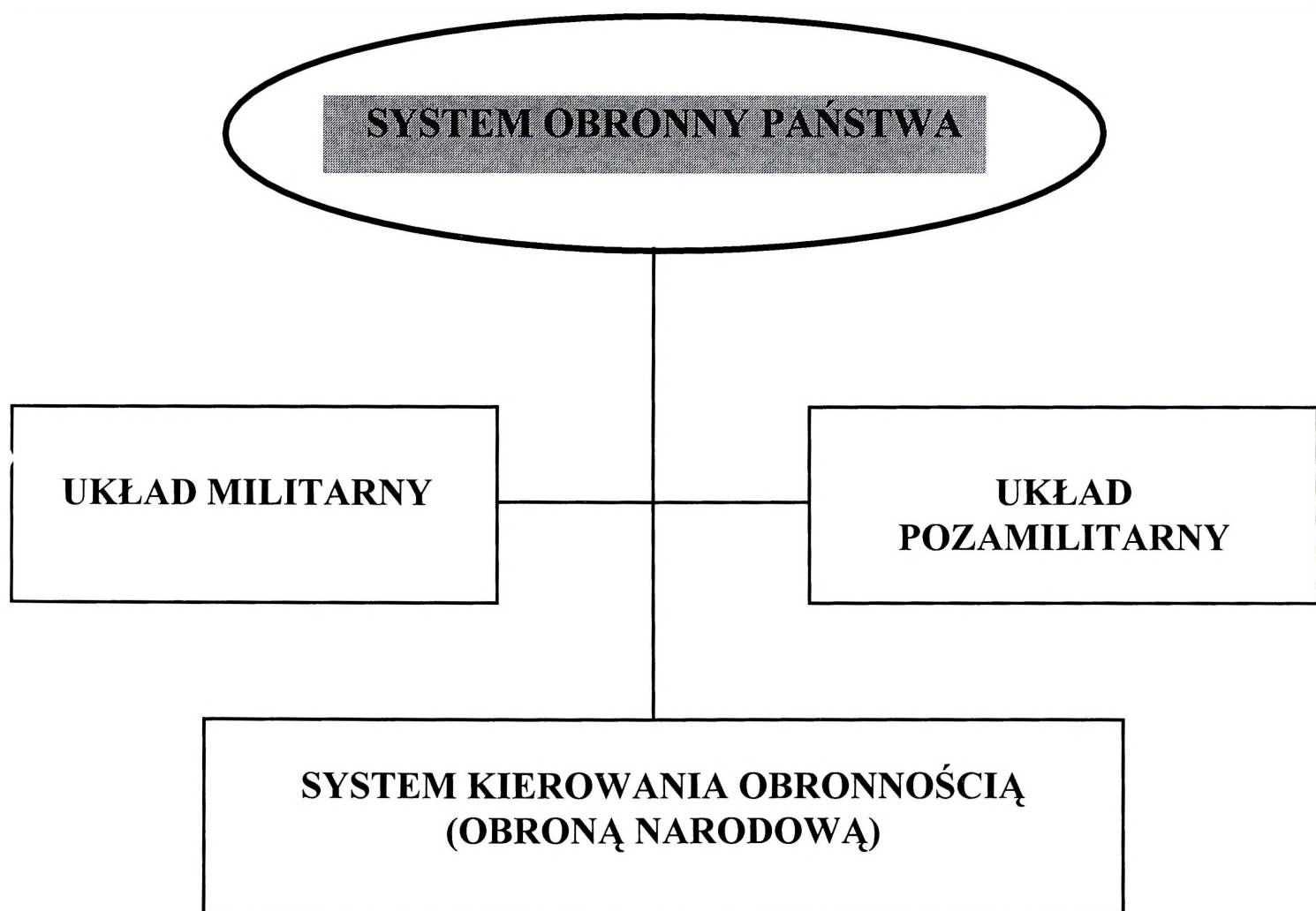
II. SYSTEM OBRONNY RP

1. STRUKTURA SYSTEMU OBRONNEGO

Systemem obronnym 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).

W skład struktury podmiotowej systemu obronnego RP wchodzi trzy podstawowe elementy:

- układ militarny (siły zbrojne);
- układ pozamilitarny;
- system kierowania obronnością.



Schemat nr 1

Sily zbrojne RP - zgodnie z Konstytucją Rzeczypospolitej Polskiej - służą obronie niepodległości państwa i niepodzielności jego terytorium i jako takie muszą zachować ciągłą gotowość do reagowania na zagrożenia oraz do przeprowadzenia - samodzielnie lub wspólnie z sojusznikami - niezbędnych do obrony państwa działań militarnych.

Układ pozamilitarny - przeznaczony jest do tworzenia niezbędnych warunków przygotowania i działania sił zbrojnych. W jego skład wchodzi:

- **polityczno-społeczne i informacyjne ogniwa obronne**
- **ogniwa ochronne**
- **gospodarcze ogniwa obronne**

System Kierowania Obronnością (obroną narodową) - przeznaczony jest do formułowania celów i zadań oraz planowania, organizowania i koordynowania działań w ramach przygotowania i utrzymywania na odpowiednim poziomie potencjału obronnego państwa w czasie pokoju oraz sprawnego rozwijania i wykorzystywania tego potencjału w okresach kryzysu i wojny. System kierowania obronnością tworzą organy władzy oraz administracji rządowej i samorządowej, a także ośrodki kierowania gospodarką, z przypisanymi im ustawowo kompetencjami.

1.1. Układ militarny

Nowa treść zadań strategicznych i operacyjnych Wojska Polskiego oraz zmienione warunki ich realizacji stymulują istotne zmiany w siłach zbrojnych. Konsekwencją tego są intensywne prace nad nowym modelem wojska. Równocześnie ze zmniejszeniem jego liczebności następują stopniowe przeobrażenia strukturalne, przesunięcia dyslokacyjne, modernizacja techniczna.

Przeprowadzamy istotną reorganizację sił zbrojnych na szczeblach operacyjnych i taktycznych. W nowej rzeczywistości winniśmy posiadać armię składającą się z mniejszych, ale wysoce mobilnych zgrupowań, zdolnych do działania na różnorodnych kierunkach. O ile przejście na szczeblu operacyjnym na nową strukturę może nastąpić stosunkowo szybko, to zmiany na szczeblach taktycznych muszą trwać dłużej. Wiążą się one bowiem z koniecznością zmian w wyposażeniu technicznym.

Przewiduje się stopniowo doprowadzenie do bardziej równomiernego rozmieszczenia poszczególnych jednostek wojskowych na obszarze kraju.

Zakłada się, że wojska lądowe składać się będą z dwóch części:

- **wojsk operacyjnych** - składających się z jednostek wojskowych wyposażonych w najlepszy sprzęt bojowy (objęty limitem porozumień wiedeńskich), o wysokim stopniu uzawodowienia;
- **wojsk obrony terytorialnej** - wyposażonych przede wszystkim w lekką broń przeciwpancerną, przeciwlotniczą i strzelecką.

Nadzwyczaj trudnym zadaniem będzie modernizacja techniczna sił zbrojnych. Zgodnie z ustaleniami konferencji wiedeńskiej - CFE - Polska może posiadać:

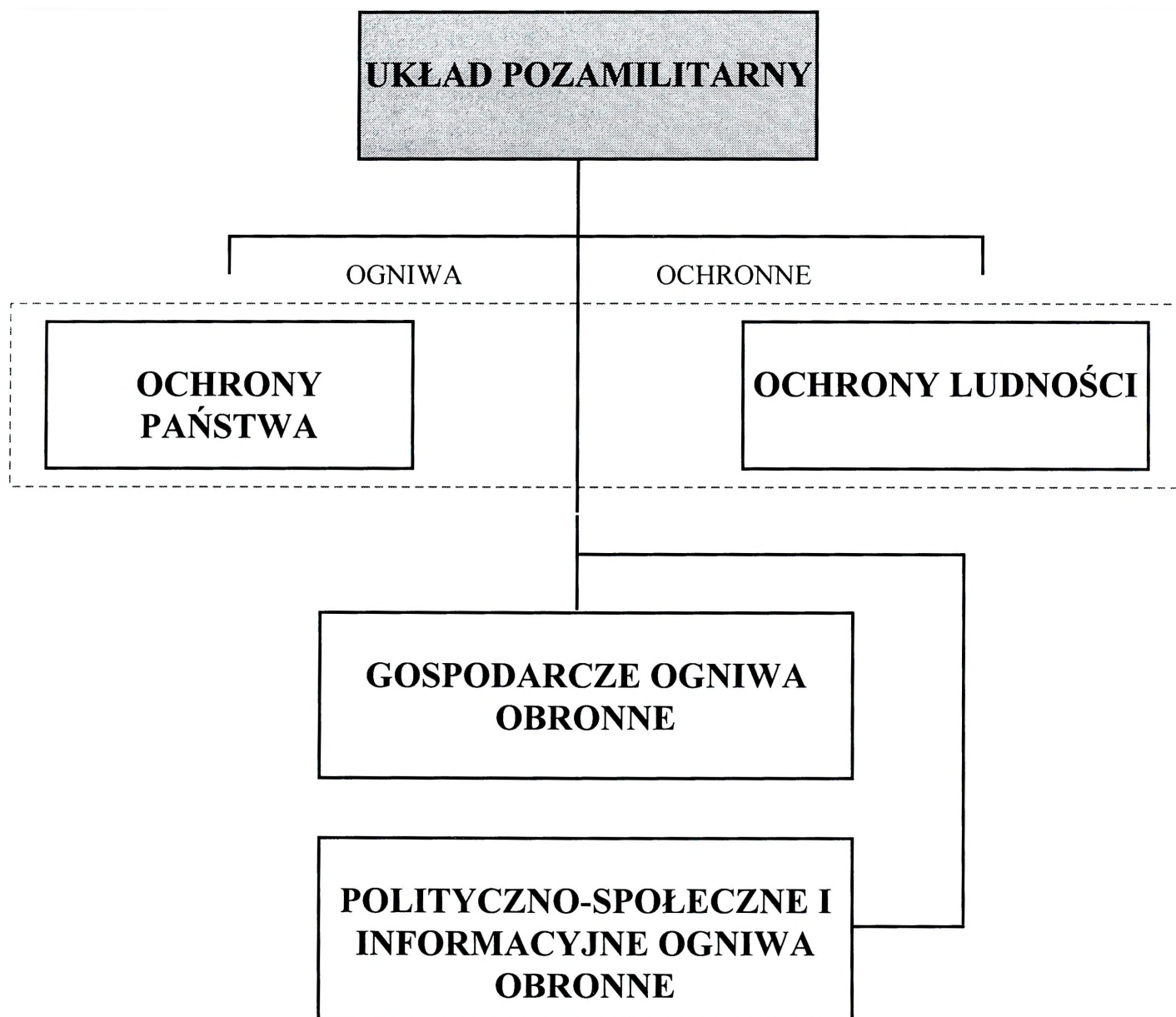
- 1730 czołgów;
- 2150 transporterów opancerzonych (1700 BWP);
- 1610 jednostek artyleryjskich o kalibrze ponad 100 mm;
- 130 śmigłowców uzbrojonych w broń rakietową;
- 460 samolot bojowych.

Oznacza to w sumie konieczność radykalnego zredukowania podstawowych środków walki z równoczesną reorientacją techniczną. Jako priorytet musimy traktować modernizację systemów dowodzenia, rozpoznania i WRE, 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. Zamierza się to osiągnąć przez wprowadzenie do sił zbrojnych śmigłowców i tworzenie oddziałów powietrzno szturmowych i w przyszłości powietrzno-zmechanizowanych. Będą to z założenia awangardowe jednostki, składające się na powietrzno-mobilne zgrupowanie operacyjne, o pełnym ukończeniu, najwyższym stopniu gotowości i zdolności bojowej, w dużym stopniu uzawodowienia. Stworzy to możliwość 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.

1.2. Układ pozamilitarny

Układ pozamilitarny jest bardzo ważnym elementem systemu obronnego. Przeznaczony jest bowiem do tworzenia niezbędnych warunków przygotowania i działania sił zbrojnych oraz funkcjonowania pozostałych struktur państwa.



Schemat nr 2

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.

Stan i możliwości układu pozamilitarnego w zdecydowanym stopniu uzależnione są od potencjału gospodarki oraz przygotowania kierowniczej kadry i przekonania jej o konieczności świadczeń na rzecz obronności.

ogniwa ochronne np.:

- Urząd Ochrony Państwa;
- Policja;
- Straż Graniczna;
- formacje OC;
- jednostki Straży Pożarnej;

gospodarcze ogniwa obronne np.:

- resorty: finansów;
- skarbu państwa;
- transportu i gospodarki morskiej;
- łączności;
- zdrowia i opieki społecznej;

polityczno-społeczne i informacyjne ogniwa obronne np.:

- siły i środki takich zwłaszcza resortów jak: spraw zagranicznych (dyplomacji);
- edukacji narodowej (szkolnictwa);
- media publiczne i prywatne, organizacje polityczne, społeczne i zawodowe.

Analizując system obronny państwa stwierdzamy, że ogniwa wojewódzkie są bardzo ważnym elementem układu pozamilitarnego. Stanowią one uzupełnienie i wsparcie układu militarnego. Wzajemne ich powiązanie i zależności nabierają szczegółowego znaczenia w okresie zagrożenia i wojny.

Województwo stanowi podstawową dla systemu obronnego jednostkę organizacyjną podziału administracyjnego kraju i z tego powodu spełnia kluczową rolę w funkcjonowaniu całego systemu obronnego. Na jego obszarze integrowane są pod kierownictwem wojewodów wojewódzkie ogniwa ochrony państwa i ochrony ludności oraz wydzielone z resortów podmioty gospodarcze.

1.3. System kierowania obronnością (obroną narodową)

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.

2. ZADANIA SYSTEMU OBRONNEGO

2.1. Przygotowania obronne w czasie pokoju

Dotychczas obowiązujący stan prawny (przed wejściem w życie nowej konstytucji) określa, że najważniejszymi organami odpowiedzialnymi za organizację, nadzór oraz kontrolę procesu przygotowań obronnych są: Rada Ministrów i Komitet Obrony Kraju (KOK). KOK ustalał dotychczas generalne założenia obrony RP i wytyczał kierunki działania, a także określał założenia organizacyjne sił zbrojnych, obrony cywilnej i zadania w ramach powszechnego obowiązku obrony oraz sprawował nadzór i kontrolę ich wykonania. Swoje funkcje wypełniał poprzez uchwały.

Zachodzące w państwie zmiany systemowe i gospodarcze postawiły pod znakiem zapytania aktualność tych przepisów. Prywatyzacja gospodarki i decentralizacja zarządzania państwem zmniejszyła kompetencje ministrów w stosunku do znacznej ilości jednostek organizacyjnych realizujących ważne zadania obronne, czego konsekwencją jest wzrost podmiotów, dla których wojewodowie stali się organizatorami działań w zakresie obronności i bezpieczeństwa państwa.

Trwający od początku lat 90-tych niekorzystny stan rzeczy spowodowany jest między innymi brakiem jednoznaczności i spójności kompetencyjnej. Dotyczy to zwłaszcza

kompetencji organów państwowych, takich jak: Prezydent RP, Rada Ministrów, Komitet Obrony Kraju oraz Ministerstwo Obrony Narodowej. W świetle 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. Ustawa i przepisy KOK-u, określające rolę ministrów i wojewodów nie odpowiadają tworzącym się strukturom, głównie w administracji i gospodarce. Przepisy te nie uwzględniają również zmian w terenowych organach administracji oraz trwającego procesu przekształceń własnościowych. Trudno dostrzec również systemowe rozwiązania w zakresie finansowania przygotowań obronnych.

Ważnym etapem zmian w dziedzinie obronności było opracowanie przez Ministerstwo Obrony Narodowej „Polityczno-strategicznego planu obrony Rzeczypospolitej Polskiej”, w którym określone zostały zagrożenia bezpieczeństwa państwa, zamiar strategiczny obrony i główne zadania podstawowych elementów systemu obronnego.

W fazie końcowych uzgodnień międzyresortowych znajduje się również projekt, w formie uchwały Rady Ministrów, planu obronnego na czas zagrożeń i wojny, ustanawiający procedury i mechanizmy tego planowania (uwzględniona została w nim koordynacyjna rola MON zgodnie kompetencjami ustalonymi przez Radę Ministrów).

W tym roku rozpoczęto prace nad wieloletnim rozwojem sił zbrojnych (uwzględniającym również budżetowanie), będącego częścią znajdującego się w początkowej fazie uruchomienia wieloletniego programowania rozwoju systemu obronnego państwa. Obecnie w toku uzgodnień międzyresortowych znajduje się projekt „Rządowego programu modernizacyjnego Sił Zbrojnych RP na lata 1998-2002 i kierunki dalszego ich rozwoju”. Kolejnym programem rozwoju objęte zostaną również pozostałe elementy systemu obronnego. Ponadto należy tu również uwzględniać rozwiązania obowiązujące w NATO jeszcze przed momentem integracji ze strukturami Paktu.

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.

Ustawa ta wnosi nowe elementy także do koncepcji organizacji wojennego systemu kierowania państwem. Rola Ministra Obrony Narodowej w tym systemie winna uwzględniać jego rolę w kierowaniu obronnością w czasie pokoju.

2.2. Kierowanie obronnością w czasie zagrożenia i wojny

W zakresie kierowania obronnością w czasie zagrożenia 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 konstytucja). 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 - Gabinet Wojenny (proponowana również nazwa - Komitet Obrony Państwa). powoływany byłby przez Prezydenta z chwilą wprowadzenia stanu wojennego.

Prezydent, jako kierujący obroną państwa powinien uzyskiwać informacje o przebiegu działań wojennych i potrzebach obronnych i na ich podstawie podejmować decyzje polityczno-strategiczne. Proponuje się, że do przygotowywania propozycji do tych decyzji, planowania zadań z nich wynikających, a także koordynowania ich realizacji utworzony zostanie odpowiednio zorganizowany i przygotowany Sztab Obrony Państwa (Obrony Narodowej). Ponieważ główna część zakresu tych zadań jest realizowana w czasie pokoju przez Ministerstwo Obrony Narodowej, dlatego też Sztab Obrony Narodowej powinien być zorganizowany na bazie jednostek organizacyjnych MON (w tym również Sztabu Generalnego).

Nowa konstytucja określa, że na czas wojny Prezydent, na wniosek Rady Ministrów powołuje Naczelnego Dowódcę Sił Zbrojnych. Realizowałby on tym samym przygotowane przez Ministerstwo Obrony Narodowej (Sztab Generalny) strategiczne plany działań zbrojnych, kierował ich realizacją, określał osobowe i materiałowe potrzeby sił zbrojnych.

2.3. Stanowiska kierowania

W celu stworzenia odpowiednich warunków dla podejmowania decyzji na czas zagrożenia i wojny organizuje się stanowiska kierowania i zapasowe miejsca pracy:

- **główne stanowiska kierowania** - dla Prezydenta RP, Prezesa Rady Ministrów, organów administracji rządowej i samorządu terytorialnego, przygotowane w odpowiednio przystosowanych obiektach, będących stałymi siedzibami tych organów. Mają one zapewnić warunki kierowania państwem (resortem, województwem itp.) w czasie zagrożenia i wojny.
- **zapasowe stanowiska kierowania** - dla Prezydenta RP, Prezesa Rady Ministrów oraz organów ustalonych przez Radę Ministrów, a także dla wojewodów. Mają one zapewnić warunki kierowania państwem w czasie wojny, jeżeli kierowanie z głównych stanowisk jest niemożliwe.
- **zapasowe miejsca pracy** - dla określonych organów naczelných i centralnych, usytuowane poza aglomeracją miejską Warszawy.

Konieczność dostosowania systemu obronnego państwa, w tym sił zbrojnych, do standardów obowiązujących w NATO, wymaga ukierunkowania działań zmierzających do przyjęcia rozwiązań funkcjonujących w zachodnich systemach obronnych. Prace te winny uwzględniać sytuację społeczno-ekonomiczną państwa przy jednoczesnym zapewnieniu pełnej kompatybilności naszego systemu obronnego z odpowiednimi systemami NATO. Do podstawowych zadań w tej mierze należy zaliczyć działania organizacyjno-prawne (przyjęcie ustawy o obowiązku wojskowym i innych powinnościach obronnych, ustawy o stanie wojennym) oraz edukacyjne na rzecz zapewnienia cywilnej i demokratycznej kontroli nad siłami zbrojnymi, systematyczny rozwój wojska i standaryzacji systemu obronnego Polski, konieczność rozbudowy i dostosowania infrastruktury umożliwiającej wypełnianie roli państwa w warunkach sojuszniczego wsparcia, wypracowanie przejrzystości w planowaniu obronnym i w pracach nad budżetem obronnym i wojskowym oraz realizację współpracy wojskowej z NATO, ukierunkowanej na współdziałanie w ramach wspólnej obrony.

Realizacja tego zadania wymaga czasu, środków finansowych i zaangażowania wszystkich, w których kompetencjach i obowiązkach leżą zadania związane z obronnością państwa.

III. ŁĄCZNOŚĆ W OPERACYJNYM PRZYGOTOWANIU OBSZARU KRAJU DO OBRONY

1. RYS HISTORYCZNY

Wzrost ilości informacji we wszystkich obszarach i płaszczyznach ludzkiej działalności spowodował, że stanowi ona obok materii i energii trzeci element otaczającej nas rzeczywistości. Istota kierowania państwem, dowodzenia siłami zbrojnymi i zarządzania gospodarką narodową, jak też organizacja bytu społecznego polega na sprawnym przesyłaniu informacji /wiadomości/ na odległość za pomocą różnych systemów łączności. W siłach zbrojnych wysoka jakość łączności jest podstawowym i koniecznym warunkiem sprawnego dowodzenia, a zatem efektywnego wykorzystania wojsk w działaniach bojowych.

„Dlatego też męką największą, jaką ja, Naczelny Wódz nie chcący darmo krwi przelewać, miałem - była kwestia łączności” - stwierdził przed 68 laty ówczesny Generalny Inspektor Sił Zbrojnych marszałek Józef Piłsudski.

Wojna 1939 r. przyniosła, przy całym swym tragizmie, również doświadczenia utraty dowodzenia na szczeblu strategicznym, operacyjnym i taktycznym, przede wszystkim z powodu braku łączności. W 1936 r. opracowano tylko plan organizacji łączności przewodowej Naczelnego Wodza na wypadek "Z". Plan ten jednakże pozbawiony podstawy - planu operacyjnego - nie miał praktycznej wartości w wypadku konfliktu zbrojnego z Niemcami. Rozpoczętej w marcu 1939 r. pracy nad planem łączności do wybuchu wojny nie ukończono. Plan łączności, jako wtórny dokument operacyjny przewidywał jedynie organizację i pracę łączności na okres pierwszego etapu kampanii, a więc bitwy o główną pozycję obronną.¹ Krótko mówiąc: plan łączności na potrzeby wojny w 1939 r. był zaledwie planem łączności wstępnego ugrupowania osłonowego. Opracowany w bardzo krótkim czasie wykazywał szereg luk i usterek, stanowiąc zaledwie szkielet pierwszych poczynąń wojennych². Plan łączności nie zabezpieczał systemu dowodzenia w wypadku konieczności wyznaczenia głównej pozycji obronnej i zorganizowania oporu w głębi kraju. Nie

¹ Jurga T. "Obrona Polski 1939" IW PAX Warszawa 1990r. str.172

² Popławski T. "Analiza łączności w wojsku lądowym Polskich Sił Zbrojnych przed drugą wojną światową i w kampanii wrześniowej". WIH str. 124

przewidywano osi przesunąć stanowisk dowodzenia i miejsc ich pracy, które należało odpowiednio wcześniej przygotować pod względem łączności. Nie dysponowano odwodem sił i środków łączności. Nadmierna decentralizacja środków radiowych, niedostateczna ilość sprzętu radiowego oraz źle interpretowany zakaz użycia radia z obawy przed dekonspiracją ugrupowania, a także dostanie się do rąk niemieckich szyfru już w pierwszych dniach wojny spowodowały, że łączność radiowa prawie nie istniała. Natomiast sieć telefoniczna funkcjonowała bardzo słabo z powodu niedostosowania jej do potrzeb wojennych /np. nie zapewnienie dróg obejściowych dla sieci stałej w większych miastach, zbyt małe zapasy kabla polowego do budowy polowych linii/. Te braki i niedociągnięcia były jedną z przyczyn bardzo źle działającej łączności zarówno radiowej jak i przewodowej.

Przyjęcie strategii obronnej państwa stwarza sprzyjające warunki przygotowania zawczasu na obszarze kraju środków i urządzeń telekomunikacyjnych do zapewnienia trwałej łączności.

Łączność na terytorium kraju zapewnia system łączności państwa. Jego potencjał powinien zaspokajać potrzeby i wymagania wszystkich organów kierowania państwem i dowodzenia siłami zbrojnymi. Składa się on z sieci telekomunikacyjnej użytku publicznego, sieci resortowych np.: /MON, MSW i A, MŁ / i zakładowych oraz poczty. Sieć telekomunikacyjną tworzą: obiekty i linie telekomunikacyjne /kablone, napowietrzne i radiowe/,

obiekty teletransmisyjne /SW/ i radiokomunikacyjne /łączności radiowej i radiofonicznej, radiofonii i telewizji/ oraz naziemne stacje łączności satelitarnej. Ministerstwo Obrony Narodowej dysponuje siecią resortową zwaną "Stacjonarnym systemem łączności SZ RP" lub "Międzygarnizonowym systemem łączności MON". Sieć telekomunikacyjna użytku publicznego stanowi podstawę stacjonarnego systemu łączności MON, który jest z nią sprzężony.

Operacyjne przygotowanie obszaru kraju do obrony pod względem łączności obejmuje wiele przedsięwzięć o charakterze organizacyjnym, technicznym i inwestycyjnym w sieci telekomunikacyjnej użytku publicznego, a w tym także wojskowej stacjonarnej sieci łączności - stosownie do potrzeb wynikających z planów operacyjnych użycia sił zbrojnych / np. przez rozbudowę oraz też modernizację jej potencjału a przede wszystkim infrastruktury telekomunikacyjnej kraju/.

Celem operacyjnego przygotowania obszaru kraju do obrony pod względem łączności jest przygotowanie systemu łączności państwa do zapewnienia operatywnego, ciągłego i skrytego dowodzenia wojskami w okresie zagrożenia wojennego i wojny, przede wszystkim zaś wcześniejsze przystosowanie jego elementów składowych, takich jak węzły i linie telekomunikacyjne, do przewidywanych potrzeb i wymagań systemu dowodzenia, przez zapewnienie:

- zdolności do wydzielenia łączy telekomunikacyjnych nowym elementom systemu dowodzenia w różnych rejonach działań wojsk;
- niezawodności i elastyczności oraz możliwości odtwarzania naruszonych połączeń telekomunikacyjnych;
- odporności na uszkodzenia i zniszczenia środków i urządzeń łączności.

W istniejącej sieci telekomunikacyjnej można wyróżnić linie łączności przebiegające ze wschodu na zachód i rokady biegnące z północy na południe. W punktach przecięcia tych linii znajdują się stacje wzmacniakowe bądź teletransmisyjne. Sieć telekomunikacyjna na obszarze kraju posiada postać wieloboków lub też ma zbliżoną najwyraźniej do nierównomiernej siatki. Za pomocą linii kablowych realizuje się zasadnicze potrzeby SZ RP. Na 477 stacji wzmacniakowych tylko 5 jest w obiektach umocnionych, 10 w zagłębionych i 68 w pół zagłębionych, w większości są one jednak nie zagłębione i nie umocnione, czyli nieodporne na oddziaływanie przeciwnika. Stacje wzmacniakowe są rozmieszczone w większości w budynkach naziemnych, zlokalizowanych w zwartej zabudowie miast, na wypadek wojny szczególnie zagrożonych. W wypadku konfliktu zbrojnego sytuacja taka może utrudnić manewr traktami nośnymi i łączami oraz odtwarzanie naruszonego systemu łączności.

W celu powiązania stacjonarnego systemu łączności MON z systemem telekomunikacyjnym kraju rozbudowywana jest wojskowa sieć kablowa a na potrzeby alarmowania i powiadamiania kadry - telefoniczna sieć miejscowa.

W trakcie rozbudowy i modernizacji /rekonstrukcji/ sieci telekomunikacyjnej użytku publicznego, w ramach operacyjnego przygotowania obszaru kraju, przystosowuje się ją do oddania i przyjęcia dodatkowych łączy i traktów - zgodnie z planami operacyjnymi, a przede wszystkim stosuje się uodpornienia sieci i środków teletransmisyjnych: lokalizacyjne, punktowe, liniowe, eksploatacyjne.

2. PRZEDSIĘWZIĘCIA PRZYGOTOWANIA SYSTEMU TELEKOMUNIKACYJNEGO NA RZECZ OBRONNOŚCI

W czasie operacyjnego przygotowywania do obrony kraju dysponowanie obszarem kraju i całą infrastrukturą telekomunikacyjną z nim związaną odgrywa zasadniczą rolę. Stwarza możliwość wcześniejszego kształtowania sieci telekomunikacyjnej użytku publicznego z uwzględnieniem potrzeb obronnych. Działania takie są czynione, zwłaszcza w zakresie rozbudowy systemów międzynarodowych i międzymiastowych.

Obecny stan telekomunikacji kraju, pomimo burzliwego rozwoju, jest niezadowalający zarówno pod względem ilościowym jak i jakościowym /np: niewłaściwa struktura organizacyjna - zagęszczenia i rozrzedzenia linii telekomunikacyjnych, mała skuteczność obrony przed rozpoznaniem i obezwładnianiem radioelektronicznym/. Do przesyłania informacji wykorzystywany jest jeszcze przestarzały sprzęt. Sieci łączności niektórych resortów i instytucji funkcjonują na podstawie różnych rozwiązań technicznych / np. obecnie eksploatowane urządzenia łączności nie są przystosowane do współpracy z nowowprowadzanymi - technika analogowa i cyfrowa /. Przez to eksploatowany system łączności jest mało spójny i podzielony na zbyt wiele podsystemów resortowych. Nie zapewnia to wymaganej koordynacji i kompatybilności systemowej. Stwarza znaczne utrudnienia w przekazywaniu informacji i niedogodności w organizowaniu łączności, jak również niebezpieczeństwo znacznej utraty informacji.

Zasadniczą rolę w systemie łączności wojsk operacyjnych w działaniach prowadzonych na terenie kraju spełniać będzie międzygarnizonowy system łączności sił zbrojnych. Przyjęto, że planowany system łączności w działaniach prowadzonych na obszarze kraju będzie opierać się na podstawowych węzłach sieci i garnizonowych węzłach łączności oraz polowych i stacjonarnych liniach łączności uzupełnionych rozwijanymi środkami polowymi. Daje to możliwości wykorzystywania GWŁ-ów w roli WŁ określonych stanowisk dowodzenia lub pomocniczych węzłów łączności. W tym celu wyposaża się niektóre GWŁ w dodatkowy sprzęt i urządzenia łączności.

Do jej organizowania będzie się więc wykorzystywać polowe i stacjonarne środki oraz linie łączności. Szefowie łączności związków taktycznych /oddziałów/ powinni znać i dysponować schematami infrastruktury sieci telekomunikacyjnej użytku publicznego występującej na obszarze działań z oznaczonymi miejscami odbioru /punktami dostępu/, a

także posiadać urządzenia dowiązania do punktów odbioru łączy. Obecnie na obszarze kraju przygotowuje się około kilkuset punktów odbioru łączy. Różnorodność urządzeń sprawia, że te pododdziały powinny dysponować różnego typu "urządzeniami dostępu" do sieci stacjonarnej. W składzie jednostek wojsk łączności należy przygotować pododdziały wyspecjalizowane w odbiorze kanałów i budowy linii dowiązania.

System łączności sił zbrojnych w ramach operacyjnego przygotowania powinien być doskonalony i unowocześniany w zakresie :

- zwiększenia żywotności i niezawodności;
- zwiększenia szybkości i ilości przekazywanych informacji;
- zapewnienia łączności nowo powstałym elementom systemu dowodzenia ;
- umożliwienia łatwego, szybkiego /kompleksowego/ dowiązania i połączenia polowego systemu łączności z systemem telekomunikacyjnym kraju;
- ochrony przekazywanych informacji- bezpieczeństwa łączności.

Jak wiadomo, stacjonarna sieć łączności jest szeroko wykorzystywana do zapewnienia łączności SZ w czasie pokoju i będzie również - na okres zagrożenia wojennego i wojny. To jednak nie może być traktowana jako środek rozwiązujący wszystkie problemy dowodzenia wojskami na obszarze kraju, a jedynie może stanowić jedną ze składowych systemu łączności.

Na potrzeby sił zbrojnych wykorzystywany będzie opracowywany od kilku lat zintegrowany system łączności /technika cyfrowa/ oparty na elementach stacjonarnej i polowej sieci łączności. Należy nadmienić, że jest on przygotowywany obecnie do produkcji i posiada korzystne taktyczno - techniczne parametry oraz jest porównywalny z systemami łączności armii państw zachodnich.

Natomiast z analizy stanu systemu łączności państwa wynika potrzeba i zachodzi konieczność budowy jednolitej sieci telekomunikacyjnej kraju takiej, która zapewni naczelnym organom władzy i administracji państwowej, siłom zbrojnym oraz innym użytkownikom terminową, wierną i skrytą łączność.

W procesie kierowania państwem i dowodzenia siłami zbrojnymi zasadniczego znaczenia nabiera walka o czas. Szybkość przekazywania informacji, stopień jej wiarygodności i bezpieczeństwo są czynnikami, które będą decydować o efektywności działań obronnych. Złożoność systemu kierowania obroną państwa zmusza do rozwoju jego materialnej bazy - systemu łączności.

Mając na uwadze potrzeby obronności państwa celowe jest przyspieszenie prac nad budową nowego systemu łączności określanego jako krajowy systemem łączności o innej strukturze, wykorzystującego już tylko technikę cyfrową i włączenie do niego wszystkich użytkowników. Umożliwi to należyte wykorzystanie baz danych poszczególnych instytucji, scentralizowane kierowanie wszystkimi służbami podczas wykonywania zadań na całym obszarze kraju i zagwarantuje bezpieczeństwo łączności. Powinien on zapewnić wszystkim użytkownikom łączność nie utajnioną i utajnioną: telefoniczną oraz transmisję danych.

Obecnie pojmowane założenia prowadzenia obronnych działań bojowych wymagają zbudowania na obszarze kraju takiego systemu, który umożliwi operatywne oraz ciągłe kierowanie i dowodzenie w warunkach pokoju, jak i w wyższych stanach gotowości obronnej państwa. Powinien on w czasie pokoju spełniać rolę rządowego systemu kierowania państwem, a w czasie wojny sprostać ekstremalnie wysokim wymaganiom systemu obronnego państwa i dowodzenia wojskami.

Podstawową cechą określającą stopień przydatności danego systemu telekomunikacyjnego na potrzeby administracji kraju i systemu obronnego jest możliwość jego hermetyzacji czyli zapewnienia ważnym 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. Dla zapewnienia bezpiecznej wymiany informacji pomiędzy naczelnymi organami władzy i administracji państwowej w sytuacjach wyjątkowych (w czasie kryzysu i wojny) planowana jest, w ramach Krajowego Systemu Łączności, budowa cyfrowej wąskopasmowej sieci łączności, spełniającej rolę krajowej sieci awaryjnej (w krajach członkowskich NATO przewiduje się istnienie narodowych systemów awaryjnych, realizowanych głównie jako cyfrowe systemy tzw. wąskopasmowe z podstawowym cyfrowym kanałem abonenckim o przepływności 16 kbit/s).

Do najistotniejszych cech można zaliczyć:

- niskie koszty eksploatacji (koszt dzierżawy systemu teletransmisyjnego jest ok. 4-krotnie niższy od kosztów podobnego systemu dla sieci normalno-przepustowej z kanałem abonenckim o przepływności 16 kbit/s);
- duża elastyczność konfiguracji sieci (poprzez stosowanie procedur automatycznego uaktualniania dróg połączeniowych), umożliwiająca bez konieczności ingerencji systemów zarządzania dołączenie czy wyłączenie centrów komutacyjnych lub

reorganizacji struktury sieci (np. przez zmianę przeznaczenia węzłów poprzez zmianę numeracji central);

- kompatybilność sprzętowa i programowa z urządzeniami stosowanymi w specjalnych sieciach systemów militarnych, w tym również i SZ RP (system pk. STORCZYK)
- możliwość powszechnego stosowania w systemie tanich grupowych (na kanały międzycentralowe) i indywidualnych (abonenckich) urządzeń kryptograficznych;
- mobilność systemu (czas instalacji i alokacji nowej centrali w systemie nie przekracza 5 minut) i możliwość jego bezpośredniej współpracy z urządzeniami radiodostępu z zachowaniem ciągłości utajniania;
- stosowaniem pięciostopniowego priorytetu dostępu dla abonentów do zasobów systemowych sieciowych systemu;

Wąskopasmowy system łączności z modulacją delta i cyfrowym kanałem abonenckim o przepływności 16 kbit/s został wybrany jako sieć awaryjna z uwagi na posiadane przez niego unikalne cechy, wyróżniające go z innych systemów powszechnych.

Całość systemu łączności kierowania obroną państwa i dowodzenia siłami zbrojnymi zarówno pod względem organizacyjnym, technicznym jak i świadczonych usług, stanowić będzie zespół węzłów, traktów i linii łączności /stacjonarnych i polowych/ urządzeń komutacyjnych oraz końcowych zapewniających niezbędne usługi telekomunikacyjne i informatyczne wszystkim organom kierowania i dowodzenia funkcjonującym w systemie obronnym państwa.

Reasumując należy jeszcze raz podkreślić, że w operacyjnym przygotowaniu obszaru kraju do obrony pod względem łączności, które powinno obejmować wszystkie instytucje, urzędy i siły zbrojne nie tylko w okresie pokoju, ale przede wszystkim w czasie zagrożenia wojennego i wojny, należy:

- efektywnie wykorzystać na potrzeby obronności państwa ich
- organiczne systemy łączności;
- przydzielać częstotliwości urządzeniom nadawczym na okres zagrożenia państwa i wojny;
- realizować przez podmioty gospodarcze a szczególnie resort łączności zadania obronne /między innymi inwestycji/ proponowane przez siły zbrojne;
- rozbudowywać, i programować wykorzystanie obiektów i linii telekomunikacyjnych oraz ich ochronę i obronę na całym terytorium kraju;

- prognozować kierunki rozwoju i produkcji środków i systemów telekomunikacyjnych;
- ustalać sposoby usuwania niesprawności /awarii/ i zakłóceń systemu ;
- współpracować w zakresie innych wspólnych przedsięwzięć.

Umożliwi to poprawę wskaźników systemu łączności między innymi takich, jak: wyprzedzającej gotowości systemu do gotowości bojowej wojsk, żywotności, mobilności, poziomu utajniania i bezpieczeństwa łączności. Zastosowane nowe technologie - technika cyfrowa i automatyzacja procesów dowodzenia - pozwolą na należyte wykorzystanie jego parametrów taktyczno-technicznych i możliwości eksploatacyjnych.

IV. INFRASTRUKTURA TELEKOMUNIKACYJNA KRAJU. KIERUNKI ROZWOJU

1. STAN INFRASTRUKTURY TELEKOMUNIKACYJNEJ KRAJU

1.1. Operatorzy telekomunikacyjni

Jeśli przypomnimy sobie dziś jeszcze wcale nie tak odległą przeszłość, to przed rokiem 1989 dostępność do usług telekomunikacyjnych w Polsce, ich jakość, powszechność i dostosowanie do potrzeb użytkowników sieci telekomunikacyjnej pozostawiały wiele do życzenia.

Oprócz tego występowało wówczas znaczne skumulowanie opóźnień w rozwoju nowoczesnych technik i technologii telekomunikacyjnych, widoczne nawet w stosunku do niektórych krajów ówczesnego bloku socjalistycznego. Należy przy tym pamiętać, że istniała wówczas organizacja COCOM, która ograniczała sprzedaż sprzętu i rozwiniętej technologii do krajów o systemach niedemokratycznych. Oznaczało to, że każda transakcja z zachodnim producentem, dotycząca sprzętu zastrzeżonego (nadającego się do wykorzystania na potrzeby militarne), mogła być zrealizowana tylko po uzyskaniu specjalnej zgody. Może się to wydać paradoksalne, ale owo techniczno-eksploatacyjne opóźnienie polskiej telekomunikacji legło u podstaw rekonstrukcji naszego systemu telekomunikacyjnego - jednego obecnie z najbardziej nowoczesnych rozwiązań w skali światowej.

Polska staje obecnie przed nieco łatwiejszymi problemami do rozwiązania niż kiedyś. Nie ma już zastrzeżeń natury techniczno - ekonomicznej co do kapitalizacji infrastruktury telekomunikacyjnej (nie znaczy to jednak, że takie problemy nie występują). I najważniejsze - mamy obecnie szansę „przeskoczenia” pewnych etapów pośrednich w budowie nowoczesnej telekomunikacji.

Pierwszego 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.

Należy dodać, że pod względem infrastruktury telekomunikacyjnej Polska zajmowała jedno z ostatnich miejsc w Europie (przed Albanią i Rumunią). W dodatku zły stan techniczny

sieci i urządzeń, a także niski poziom infrastruktury pokazywał, jak wielki wysiłek finansowy i organizacyjny będzie potrzebny, aby stworzyć warunki do rozwoju kraju. Poniżej przedstawiono wskaźniki charakteryzujące rozwój polskiej telekomunikacji i porównanie polskiej telekomunikacji do 20 krajów o największych przychodach (źródło: Raport Teleinfo. Telekomunikacja w Polsce - stan, inwestycje, perspektywy).

20 krajów o największych przychodach z telekomunikacji, a Polska				
Kraj	Przychody z telekomunikacji (mln USD)	Przychody na mieszkańca (USD)	Przychody na przyłącze abonenckie (USD)	Przychody na jednego zatrudnionego (USD)
USA	195 333,0	749,8	1 246	294 620
Japonia	73 379,8	588,1	1 224	b.d.
Niemcy	46 151,4	568,8	1 177	202 772
Anglia	25 434,6	437,9	897	b.d.
Francja	23 662,3	409,9	749	155 061
Włochy	20 003,70	351,0	805	194 211
Australia	11 491,4	644,1	1 298	174 106
Hiszpania	11 344,0	289,4	751	163 059
Kanada	10 388,1	356,7	602	130 003
Szwajcaria	8 889,2	1 263	2 058	454 271
Korea Płd.	8 727,8	194,6	469	140 594
Brazylia	8 720,9	54,0	722	92 754
Holandia	8 114,0	524,8	999	265 615
Meksyk	6 509,1	70,9	740	132 796
Chiny	6 166,8	5,2	226	12 734
Argentyna	6 009,1	173,7	1 086	202 395
Szwecja	5 755,5	651,9	957	175 436
Tajwan	5 275,8	248,2	620	147 419
Belgia	4 339,0	428,5	937	b.d.
Honkong	3 804,0	652,2	1 208	116 025
.....				
Polska	2 464,9	63,2	377	33 533

Rok	Liczba abonentów			Liczba abonentów na 100 mieszk.		
	Miasto	Wieś	Ogółem	Miasto	Wieś	Ogółem
1992	3 411 049	527 095	3 938 144	14,29	3,62	10,25
1993	3 828 392	587 359	4 415 751	16,08	4	11,47
1994	4 333 123	672 971	5 006 094	18,15	4,58	12,98
1995	4 924 255	804 242	5 728 497	20,63	5,46	14,85
1996	5 545 890	992 691	6 538 581	23,23	6,74	16,94
1997 (plan)	6 213 748	1 218 646	7 432 394			19,24

Prywatni operatorzy telekomunikacyjni

Ustawa o łączności z 1990 r. (i późniejsze jej nowelizacje) dopuściła konkurencję w telekomunikacji. W myśl tej ustawy lokalni operatorzy mogli tworzyć własne sieci, a telekomunikacja miała obowiązek przyłączać ich do sieci ogólnokrajowej.

W Polsce prywatne sieci telefoniczne prowadzi tylko kilkanaście firm (wydano 70 koncesji), które w końcu ubiegłego roku miały nieco powyżej 70 tys. abonentów (wobec prawie 7 mln abonentów Telekomunikacji).

1.2. Systemy radiowe

Telefonia komórkowa

Sieci komórkowe mają już ponad 600 tys. abonentów. Istnieją dwa systemy: analogowy NMT i cyfrowy GSM. Planuje się budowę systemu DCS.

Nowością na polskim rynku jest system DCS, który pracuje na częstotliwości 1800 MHz. Centertel zamierza w końcu tego roku uruchomić sieć DCS w Warszawie., ale cała sieć ma być gotowa w końcu przyszłego roku. DCS opłaca się budować w większych miastach, gdzie jest duży ruch.. Centertel zbuduje sieć w dziesięciu miastach wraz z ich okolicami:

w Warszawie, Trójmieście (Gdańsk, Gdynia i Sopot), Krakowie, Wrocławiu, Poznaniu, Łodzi, Lublinie, Bydgoszczy, Szczecinie oraz Katowicach (i sąsiednich miastach: Sosnowcu, Bytomiu, Zabrze, Rudzie Śląskiej, Gliwicach, Dąbrowie Górniczej, Mysłowicach, Chorzowie, Będzinie, Świętochłowicach, Czeladzi i Siemianowicach Śląskich).

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).

Systemy przywoławcze (pagingowe)

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

komunikatów przywoławczych. Standaryzacja wielu niespójnych systemów doprowadziła w 1978 r. do określenia międzynarodowego standardu POCSAG.

W ramach Unii Europejskiej przygotowano (w 1992 r.) standard cyfrowego systemu przywoławczego ERMES.

Ze względu na zasięg rozróżnia się:

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

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

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

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

POCSAG (Post Office Code Standardization Advisory Group)

Protokół formatowania danych przywoławczych stosowany w systemach pagingowych. Przyjęty przez CCIR protokół otrzymał nazwę kodu przywoławczego nr 1. W pierwotnej wersji szybkość transmisji danych przywoławczych wynosiła. 512 bit/s, wersje późniejsze dopuszczają szybkość 1200 bit/s i 2400 bit/s.

Wszyscy działający w Polsce prywatni operatorzy miejskich sieci przywoławczych wykorzystują taką samą szybkość transmisji - 512 bit/s (Telepage, EasyCall, Elite, MetroBip)

ERMES (European Radio Message System)

Na potrzeby systemu przyznano 16 częstotliwości radiowych w paśmie 169,4 -169,8 MHz z odstępem kanałowym 25 kHz. W każdym kraju europejskim będą dostępne 4 z 16 przydzielonych kanałów, a pagery przystosowane do odbioru przywołań ze wszystkich kanałów. ERMES zapewnia stosowanie wszystkich form przywołania (dźwiękowe, numeryczne i tekstowe) oraz dodatkowo kodową transmisję do ok. 65 tys. bitów (lub 16 tys.

znaków numerycznych). W systemie ERMES komunikaty tekstowe są przesyłane w postaci 7 bitowych kodów ASCII, a wiadomości numeryczne kodami 4 bitowymi, zawsze z zabezpieczeniem przed błędami za pomocą kodu cyklicznego. Pierwszą publicznie dostępną instalację ERMES przeprowadzono we Francji (1994 r.), następne wprowadzono w Niemczech, Wielkiej Brytanii i krajach skandynawskich.

Systemy trunkingowe

Radiowy system komunikacyjny polegający na automatycznym przydzielaniu i podziale ograniczonej puli kanałów radiowych (trunks) między znacznie wyższą od tej puli liczbę użytkowników. Idea trunkingu opiera się na teorii prawdopodobieństwa, zgodnie z którą jest małe prawdopodobieństwo, aby wszyscy abonenci w tym samym czasie chcieli korzystać z całej puli dostępnych kanałów radiowych. Ponieważ kanały komunikacyjne (pasma częstotliwości radiowej) są przydzielane abonentowi na żądanie i zwalniane natychmiast po zakończeniu rozmowy, uzyskuje się wysoką efektywność wykorzystania widma częstotliwości, co pozwala na zredukowanie liczby nośnych niezbędnych do zapewnienia wymaganej jakości usług.

Technika trunkingu jest szeroko stosowana do wewnętrznej łączności w przedsiębiorstwach rozległych oraz w stacjonarnej i ruchomej transmisji danych.

W Polsce pracuje wiele prywatnych i publicznych sieci trunkingowych, spełniających funkcje teledycyjne. Większość z nich ma charakter wyspowy i nie ma wzajemnych połączeń. Największy zasięg zapewnia RADIO-NET (Gdynia-Gdańsk), oparta na systemie TRUNK-SWITCH realizowanym przez australijską firmę Stanilite. Nadzieją na standaryzację na poziomie europejskim jest TETRA, będący w zakresie systemów teledycyjnych odpowiednikiem standardu GSM.

TETRA (Trans European Trunked Radio)

Europejski standard zbiorowej łączności typu dyspozytorskiego, przystosowanej do cyfrowej transmisji mowy i danych typu pakietowego. Zastępuje dotychczasowe dyspozytorskie sieci zbiorowe o lokalnym zasięgu, działające do tej pory w zakresie częstotliwości 410-430 MHz. W systemie TETRA przewidziano dwukierunkową transmisję z odstępem kanałowym 25 kHz (także 12,5 kHz i 6,25 kHz) w paśmie częstotliwości 380-400 MHz. System TETRA jest pierwszym europejskim systemem trunkingowym, przewidywanym

do zastosowania w międzynarodowych służbach o charakterze publicznym (policja, straż, służby celne i porządkowe).

Ogólne parametry techniczne systemu TETRA	
Liczba kanałów przy odstępnie 25 kHz	4 głosowe (TDMA) 1 danych
Szybkość transmisji: • mowy; • danych	36 kbit/s 19,2 kbit/s
Czas zestawienia połączenia	> 300 ms
Przeniesienie (handover)	< 1 s
Metoda dostępu	Aloha szczelinowy
Rodzaj modulacji	$\pi/4$ QPSK
Kodek (połówkowy)	7,2 kbit/s (4,5 kbit/s)
Moc urządzeń	1,3 W lub 10 W
Maks. Szybkość przemieszczania terminala	< 200 km/h
Maksymalny rozmiar komórki	60 km

Inne systemy radiotelefoniczne.

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. Tę ostatnią częstotliwość trzeba będzie około 2000 r. zwolnić. PAR stosuje wyższe stawki do firm, które je użytkują.

Mało kto wie, że oprócz trunkingu i przestarzałych systemów dyspozytorskich działa w Polsce duplexowa 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.

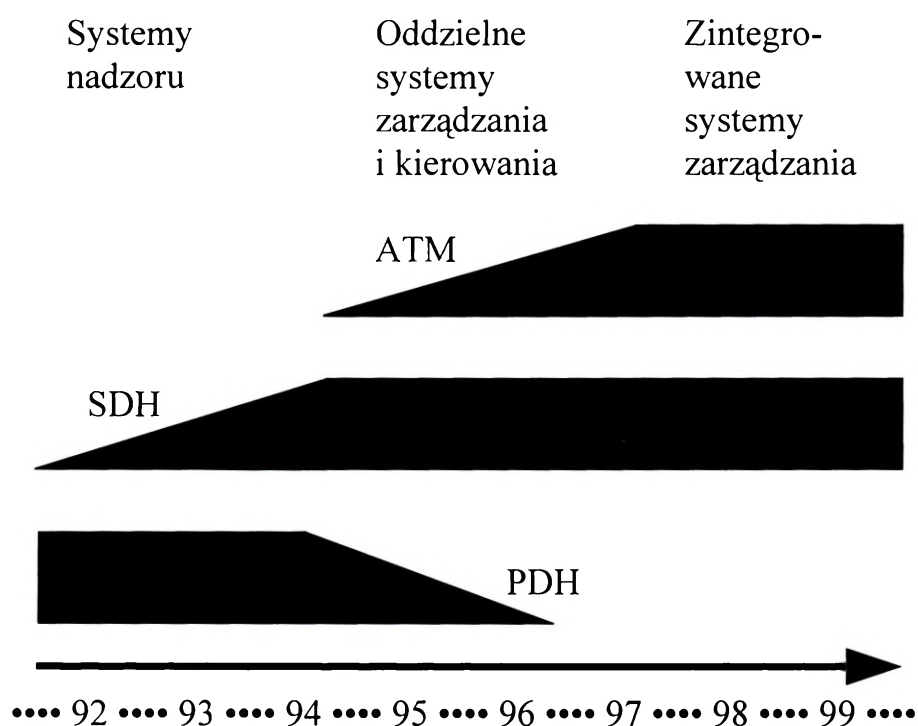
2. KIERUNKI ROZWOJU TELEKOMUNIKACJI W OPARCIU O NOWE TECHNIKI I TECHNOLOGIE

Na stan infrastruktury telekomunikacyjnej kraju, mają wpływ nowe techniki i technologie, których zastosowanie umożliwia dostęp do nowych usług.

2.1. Tendencje rozwojowe systemów teletransmisyjnych PDH, ISDN, SDH, ATM

Ponieważ w nowo zainstalowanych 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.

Stanowi to podstawę do rozwoju nowych usług w oparciu o sieć inteligentną, a cyfrowa postać sygnału jest bazą do tworzenia sieci synchronicznej SDH i wykorzystania technologii szerokopasmowej ATM (przedstawia to rys. poniżej)



Teletransmisyjne systemy plezjochroniczne PDH

Początkowo cyfrowe systemy teletransmisyjne służyły niemal wyłącznie celom transmisji telefonicznych sygnałów rozmównych i były oparte w pierwszym rzędzie na modulacji kodowo - impulsowej PCM³.

³PCM (Pulse Code Modulation) - w telekomunikacji podstawowa technika konwersji sygnału analogowego mowy do postaci cyfrowej. Często stosowana w innych dziedzinach do zamiany różnych sygnałów analogowych (temperatura, ciśnienie, dźwięk, itp.) na ciągi sygnałów cyfrowych, „łatwiejsze” do transmisji, regeneracji i wzmocnienia, a także bardziej odporne na zakłócenia niż sygnały analogowe.

W tym samym okresie co modulacja PCM powstała modulacja delta. Różni się ona od modulacji PCM sposobem kodowania sygnału próbkowanego i 4-krotnie niższą przepływnością (16 kbit/s). Ze względu na małą przepływność ma ona zastosowanie w systemach łączności specjalnej - systemy dostępu radiowego.

Dążenie do maksymalnego wykorzystania możliwości przepustowych stosowanych linii transmisyjnych stało u podstaw opracowania cyfrowych systemów wielokrotnych z wykorzystaniem sygnałów cyfrowych o dużej przepływności uzyskanych z łączenia wielu sygnałów o mniejszej przepływności przez zwielokrotnienie z podziałem czasu TDM⁴ (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. Technika tą była tzw. plezjochroniczna (tzn. prawie synchroniczna) technika zwielokrotniania sygnałów cyfrowych. Przy wykorzystaniu tej techniki zwielokrotniania powstała oparta na niej hierarchia cyfrowa systemów teletransmisyjnych PDH⁵ (Plesiochronous Digital Hierarchy).

Do ograniczeń systemów plezjochronicznych należy zaliczyć:

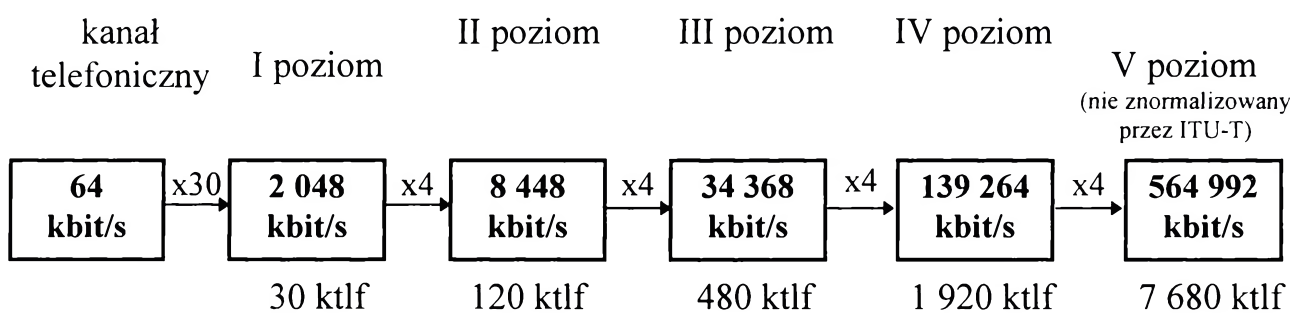
- zróżnicowanie międzynarodowych standardów zwielokrotnienia (istnieją 3 standardy zwielokrotnienia: europejski, japoński i amerykański);
- konieczność multipleksacji/demultipleksacji w każdym praktycznie węźle sieci;
- niedostosowanie do transmisji sygnałów o przepływnościach różnych od standardowych dla poszczególnych poziomów zwielokrotnienia;
- mała elastyczność (rekonfigurowalność) sieci transmisyjnej;
- brak możliwości zautomatyzowanego zarządzania siecią;

⁴ Pierwsze wielokrotne systemy PCM zostały opracowane w latach sześćdziesiątych. 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-kanalowy 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 (ok. 2 Mbit/s).

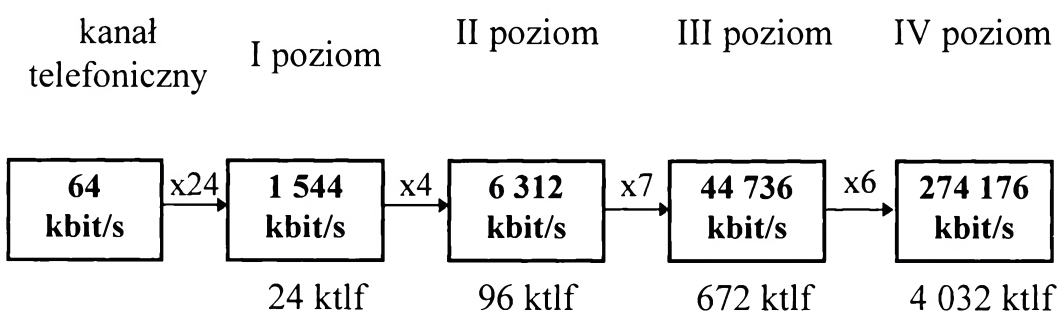
⁵ W systemach plezjochronicznych nie ma pełnego synchronizmu sygnałów. W poszczególnych węzłach sieci instalowane są niezależne zegary o stosunkowo dużej niestalości częstotliwości. Korekcję przesunięć fazowych i opóźnień sygnałów pochodzących z różnych źródeł bądź przechodzących różnymi drogami uzyskuje się poprzez wykorzystanie buforowania i uzupełnienie przepływu 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.

- brak standaryzacji styku optycznego, co utrudnia stosowanie torów światłowodowych pochodzących od różnych producentów
- duża liczba sprzętu i jego zróżnicowanie;
- wysokie koszty systemu.

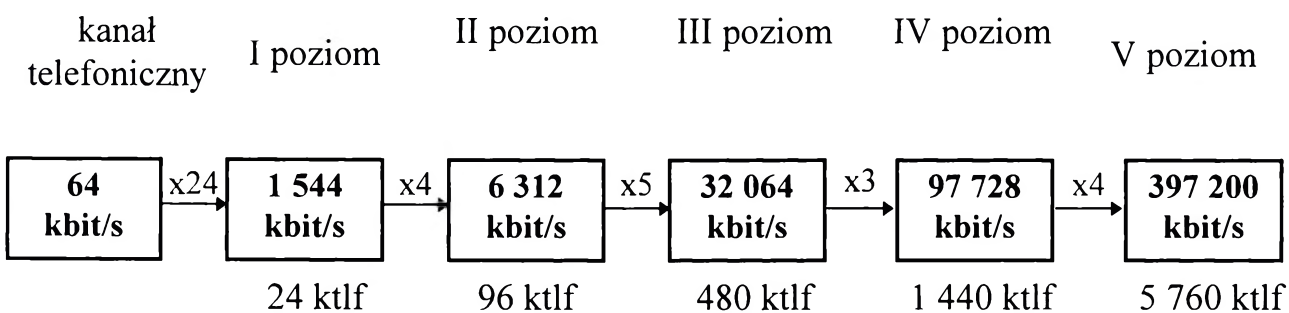
Eksplloatowane obecnie cyfrowe sieci telekomunikacyjne w znacznej części oparte są na plezjochronicznej hierarchii cyfrowej PDH, która powstała głównie na potrzeby telefonii i nie umożliwia realizacji połączeń wymagających dużych oraz zmiennych przepływności. Ponadto w zakresie plezjochronicznych systemów 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. Dla przykładu podano hierarchie plezjochronicznych systemów teletransmisyjnych w Europie, Stanach Zjednoczonych i Japonii.



Hierarchia plezjochronicznych systemów teletransmisyjnych w Europie.



Hierarchia plezjochronicznych systemów teletransmisyjnych w Stanach Zjednoczonych.



Hierarchia plezjochronicznych systemów teletransmisyjnych w Japonii.

ISDN

Jakkolwiek telefonia jest jeszcze dominującą usługą dzisiejszych sieci telekomunikacyjnych, to zapotrzebowanie na zaawansowane nietelefoniczne usługi gwałtownie rośnie. Kolejnym etapem rozwoju telefonii jest ISDN⁶. 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 naraz, 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. Współpraca podzespołów dostarczanych przez różnych producentów stała się wreszcie możliwa i prosta w realizacji. Znikła więc konieczność używania dodatkowych interfejsów, co przyspieszyło budowę sieci i obniżyło koszty jej instalacji.

Dzisiejsze wąskopasmowe ISDN są pierwszym etapem na drodze do osiągnięcia w pełni zintegrowanej sieci. Jednakże, wiele powstających obecnie usług takich, jak przesyłanie obrazów wysokiej jakości wymagają przesyłania szerszego pasma, niż to, które może zaoferować ISDN. Prowadzone są zatem prace nad wykorzystaniem ISDN zdolną do realizacji takich usług poprzez zdefiniowanie interfejsów abonenckich o przepustowościach rzędu setek megabitów na sekundę.

⁶ ISDN (ang. Integrated Services Digital Network) - zintegrowana usługowo sieć cyfrowa. 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.

Teletransmisyjne systemy synchroniczne SDH

Synchroniczne systemy teletransmisyjne SDH⁷ (ang. Synchronous Digital Hierarchy), jako podstawowe medium transmisyjne wykorzystują światłowody i stanowią odpowiedź na wady PDH. Najprościej rzecz ujmując, sieć synchroniczna, wykorzystując ten sam kabel światłowodowy, umożliwia znaczne zwiększenie przepływności oraz wprowadzenie zaawansowanych metod zarządzania siecią przy jednoczesnym zmniejszeniu liczby urządzeń. 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. Aby była możliwa współpraca dotychczasowych systemów plezjochronicznych z kanałem 155 Mbit/s, przewidziano adapter nazwany synchronicznym modulem transportowym pierwszego rzędu STM-1 (Synchronous Transport Module). 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. Przepływność 10 Gbit/s oznacza możliwość jednoczesnej transmisji ok. 120 tys. kanałów telefonicznych. Dla porównania, przepływność najwyższego poziomu hierarchii plezjochronicznej 565 Mbit/s oznacza możliwość jednoczesnej transmisji „tylko” 7 680 takich kanałów.

Można zaryzykować twierdzenie, że polska telekomunikacja w obliczu tej nowej techniki jest w bardzo dobrej sytuacji. Przystępując bowiem na początku lat dziewięćdziesiątych do budowy sieci telekomunikacyjnych z wykorzystaniem techniki cyfrowej, można było myśleć o budowie tych sieci w sposób jednolity, w oparciu o systemy SDH. Takie też strategiczne decyzje podjęto w TP S.A., a także i u innych operatorów.

Synchroniczna hierarchia cyfrowa SDH zapewnia operatorom sieci telekomunikacyjnych spójny mechanizm dzielenia, nadzorowania i kontrolowania zdolności teletransmisyjnych całej sieci. Zwiększona efektywność umożliwia redukcję kosztów eksploatacyjnych, a elastyczność sieci - wprowadzanie nowych, przynoszących korzyści finansowe usług. SDH zwiększa zatem zyski operatorów oraz konkurencyjność ich oferty.

⁷ 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. Pozwala to na realizację synchronizmu przesyłanych

Sieć synchroniczna może służyć jako środek transportowy dla szerokiego zakresu technik i usług telekomunikacyjnych. Synchroniczna hierarchia cyfrowa umożliwia stworzenie sieci zdolnej do szybkiej rekonfiguracji i zestawienia alternatywnych dróg połączeń.

ATM

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.

Z tego powodu CCITT wybrał asynchroniczny tryb przesyłania⁸ (ATM - Asynchronous Transfer Mode) jako docelową technikę transmisji B-ISDN⁹. **Należy podkreślić, że ATM jest metodą przenoszenia informacji¹⁰ i jako taka nie zależy od zastosowanej techniki transmisji.**

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: Ethernet¹¹, Token Ring¹² czy FDDI¹³.

sygnałów i wykonywanych na nich operacjach, co pozwala uniknąć wad systemów plejzochronicznych. Wadą takiego rozwiązania jest wysoka cena zegarów PRC (zegary atomowe).

⁸ 1) ATM jest to szerokopasmowy system transmisji wykorzystujący technikę pakietową. Głównym jego elementem są centra komutacji pakietów połączone liniami transmisyjnymi.

2) Od zwielokrotnienia SDH i PDH różni się tym, że nie zachodzi konieczność synchronizacji zegarów centrów komutacyjnych.

⁹ B-ISDN (Broadband Integrated Services Digital Network) - sieć szerokopasmowa stanowiąca rozszerzenie wąskopasmowej ISDN.

¹⁰ ATM jest techniką komutacji krótkich pakietów o skończonej długości zwanych komórkami. Zasada jest podobna jak w innych metodach komutacji pakietów. Każda komórka ATM składa się z 53 bajtów, z których 48 przenosi informację użytkową a 5 tworzy nagłówek. Nagłówek komórki identyfikuje „wirtualny tor” określający drogę przesyłania komórki w sieci.

¹¹ Komputerowa sieć lokalna pracująca z szybkością 10 Mbit/s. Nowsze rozwiązania technologiczne zapewniają pracę z szybkością 100 Mbit/s (Fast Ethernet). Podstawową wadą tego typu sieci jest mała możliwość rozbudowy w celu przyłączenia wielu użytkowników. Od maja 1996 r. trwają prace nad opracowaniem nowego standardu o przepływności 1 Gbit/s (tzw. Gigabit Ethernet).

¹² Sieć komputerowa wykonana w topologii pierścienia. Standard zaproponowany przez IBM jest przewidziany dla dwóch szybkości transmisji 4 Mbit/s i 16 Mbit/s. Maksymalna liczba stacji w pierścieniu wynosi 260.

¹³ Sieć cyfrowa o topologii podwójnego pierścienia, stosowana w sieciach LAN i MAN. Podstawowym medium transmisyjnym jest światłowód. Dane są przesyłane z szybkością 100 Mbit/s.

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 izochronicznych (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.

2.2. Sieci telekomunikacyjne

Krajowa Sieć Awaryjna

Komisja ds. Planowania Łączności Cywilnej NATO (CCPC) 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 krajowe¹⁴, wąskopasmowe z kanałem abonenckim o przepływności 16 kbit/s z modulacją delta. Normy EUROCOM określają parametry styków i sygnalizacji tych sieci.

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

¹⁴ W Szwecji - ConTakt, w Danii - Atoko D, w Wielkiej Brytanii - Ptarmigan, w USA - Tri Tack, DSN.

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

Sieć światłowodowa

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.

Sieci inteligentne

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 jawił się jako podstawowy 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.

Warto zauważyć w tym miejscu, że świadczenie usług telekomunikacyjnych przebiega w zasadzie dwutorowo. Z jednej strony jest uwarunkowane postępowem technologicznym (usługi dodatkowe w centralach telefonicznych, ISDN), a z drugiej strony zapotrzebowaniem rynku na usługi niestandardowe. 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.

W efekcie narzuconych zebranych na świecie doświadczeń i analizy zapotrzebowań na nowe niestandardowe usługi telekomunikacyjne stworzono uniwersalną koncepcję, obejmującą rozwiązania techniczne i sposoby ich świadczenia i nadano jej nazwę sieci inteligentnej - IN (Intelligent Network).

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.).

Zbiór usług możliwych do świadczenia z użyciem sieci inteligentnej jest bardzo bogaty. W standardach międzynarodowych zdefiniowano ok. 30 usług. Nie wszystkie usługi cieszą się jednakową popularnością na rynku komunikacyjnym. Najbardziej chyba

powszechnymi i znanymi usługami są: usługa połączenia bezpłatnego (Freephone) tzw. Infolinia 800 czy usługi audioteksowe o prefiksie 700.

Ponieważ coraz częściej pojawiają się na rynku rozwiązania dotyczące współdziałania systemów cywilnych, NATO śledzi je pod kątem zastosowań w swoich systemach. Dotychczas były to zamknięte systemy, które opracowywano z wykorzystaniem nietypowych i niestandardowych rozwiązań. Przykładem jest wykorzystywanie specjalistycznych układów o podwyższonej niezawodności, produkowanych w krótkich seriach, co znacznie podwyższa koszty całego przedsięwzięcia. Aktualnie popularna jest tendencja do wykorzystywania i adaptacji istniejących rozwiązań komercyjnych tzw. COTS (Commercial Off-The-Shelf) w zastosowaniach wojskowych. Prace tego typu prowadzone są w wielu krajach. Fakt ten nie powinien nikogo dziwić, ponieważ związane jest to z redukcją wydatków budżetowych na cele wojskowe. Pod uwagę będą brane technologie, które są/będą zintegrowane lub już współdziałają z istniejącymi systemami.

My zajmiemy się usługą wirtualnej sieci prywatnej (Virtual Private Network) ze względu na przydatność takiej usługi dla potrzeb służb specjalnych na wypadek wojny i zagrożeń.

Wirtualna sieć prywatna VPN (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 ta jest adresowana dla dużych korporacji, posiadających wiele przedstawicielstw i potrzebujących efektywnych źródeł komunikacji wewnątrz firmy.

V. POTRZEBY TELEKOMUNIKACJI W CELU DOSTOSOWANIA DO UNII EUROPEJSKIEJ I NATO

Dynamiczny rozwój technologii i techniki w dziedzinie systemów telekomunikacyjnych i informatycznych oraz ich wzajemne przenikanie mają wpływ na wszystkie aspekty życia współczesnego społeczeństwa. Krajowe i międzynarodowe instytucje polityczne, gospodarcze, wojskowe, naukowe, a nawet osoby fizyczne coraz bardziej uzależniają się od stałej dostępności do usług opartych na tych technologiach. Powoduje to wzrost zapotrzebowania na skuteczne, niezawodne i tanie systemy łączności oraz systemy informatyczne.

Równolegle z rozwojem technologii mają miejsce zmiany organizacyjne w strukturach telekomunikacji krajowych. Na dzień dzisiejszy praktycznie we wszystkich krajach rozwiniętych, w tym i w Polsce, prowadzi się reorganizację systemową, mającą na celu doprowadzenie do rozdziału funkcji regulacyjnych od budowy sieci i świadczenia usług.

Problemy regulacyjne nadal będą należeć do kompetencji jednostki rządowej natomiast budowa infrastruktury telekomunikacyjnej oraz świadczenie usług zostanie podzielone pomiędzy wiele jednostek organizacyjnych. Każdy z operatorów może stanowić własność rządu danego kraju lub być w rękach prywatnych, zależnie od stopnia liberalizacji i prywatyzacji.

Powyższe zmiany technologiczne i organizacyjne wnoszą niewątpliwy wkład w rozwój jakości oferowanych usług, ale powodują też konieczność nowego spojrzenia na organizacyjną stronę w dziedzinie planowania przygotowań obronnych w systemach telekomunikacyjnych. Wzrasta rola działań koordynacyjnych zarówno na szczeblu krajowym, jak i międzynarodowym.

Przygotowanie obszaru kraju do obrony pod względem łączności powinno obejmować przedsięwzięcia o charakterze: organizacyjnym, inwestycyjnym i technicznym w sieci telekomunikacyjnej użytku publicznego, a w tym także wojskowej stacjonarnej sieci łączności. Łączność powinna być rozbudowywana stosownie do potrzeb wynikających z planów obrony państwa i operacyjnego użycia sił zbrojnych. Wykorzystywane w okresie operacyjnego rozwinięcia wojsk i w trakcie obrony systemy łączności są projektowane już w czasie pokoju a następnie modyfikowane zgodnie ze stosownymi planami. Perspektywa wejścia Polski do NATO wymusza konieczność ścisłego współdziałania z krajami Europy

Zachodniej mającego na celu stworzenie jasnych i kompetentnych struktur w zakresie organizacji, współpracy w dziedzinie telekomunikacji zarówno w kraju, jak i na szczeblu NATO.

1. WSKAŹNIKI OCENY ŁĄCZNOŚCI I SYSTEMÓW ŁĄCZNOŚCI

System łączności na potrzeby kierowania obronnością państwa zarówno pod względem organizacyjnym, technicznym jak i świadczonych usług, stanowić będzie zespół węzłów, traktów, linii łączności, urządzeń komutacyjnych zapewniających niezbędne usługi telekomunikacyjne i informatyczne wszystkim organom kierowania i dowodzenia funkcjonującym w systemem. Aby zastanowić się na zmianami jakie należy dokonać w dziedzinie telekomunikacji na potrzeby wejścia do NATO należy zastanowić się nad wskaźnikami oceny systemów łączności stosowanymi w NATO.

Proces wymiany informacji w systemach kierowania i dowodzenia najpełniej charakteryzuje jakość łączności wyrażająca się wymaganiami w zakresie terminowości, wierności i skrytości łączności.

Terminowość łączności jest to zdolność do przekazywania i dostarczania informacji oraz prowadzenia bezpośrednich rozmów w określonym czasie, uwarunkowanym sytuacją operacyjno - strategiczną.

Wierność łączności określa stopień zgodności informacji odebranej z informacją nadaną, przy istniejących w liniach łączności zakłóceniach i zniekształceniach.

Skrytość łączności jest to zdolność przeciwstawienia się rozpoznaniu przeciwnika, w zakresie ujawnienia treści przekazywanych informacji oraz wykrycia miejsca i przynależności obiektu nadawania.

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

Gotowość bojowa systemu łączności jest to zdolność do terminowego przejścia z danego stanu w inny, niezbędny do zapewnienia kierowania i dowodzenia wojskami. Powinna ona wyprzedzać gotowość bojową systemu kierowania i dowodzenia wojskami.

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.

Mobilność systemu łączności to zdolność do terminowego rozwijania, rozbudowy i przebudowy (adaptacji) struktury sieci, odpowiednio do kształtującej się sytuacji operacyjno - strategicznej oraz potrzeb systemu kierowania i dowodzenia.

Trwałość systemu łączności określana jest zdolnością do pracy przy oddziaływaniu na niego wszystkich czynników rażenia przeciwnika i wyraża się żywotnością, odpornością na zakłócenia oraz niezawodnością środków, elementów całej sieci.

Żywotność sieci i jej elementów określa zdolność do wykonania поставionych zadań w warunkach oddziaływania ogniowego przeciwnika i innych czynników rażenia współczesnej broni.

Odporność na zakłócenia sieci i jej elementów charakteryzuje zdolność do wykonania поставionych zadań w warunkach radioelektronicznego oddziaływania przeciwnika, a szczególnie wszystkiego rodzaju środków zakłócających.

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

Bezpieczeństwo systemu łączności 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.

Wskaźniki te przyjmowane w sposób obligatoryjny. Weryfikowane za pomocą symulacji modeli komputerowych oraz przez praktyczną realizację.

Podczas weryfikacji komputerowej uwzględnia się następujące czynniki:

- 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.

Dla zastosowań matematycznych oceny łączności i systemów łączności uwzględnia się następujące wskaźniki przedstawione w tabeli 1 i tabeli 2.

Tabela 1

Wskaźniki oceny łączności

Lp.	Oceniana właściwość	Wskaźniki
1	Terminowość	-prawdopodobieństwo przekazania informacji / zestawienia łącza / w czasie nie większym od dopuszczalnego dla różnego rodzaju łączności / rodzaju świadczonych usług telekomunikacyjnych i pocztowych / i kategorii pilności informacji przy założonej / prognozowanej / intensywności obciążenia.
2	Wierność	-prawdopodobieństwo zniekształcenia znaku kombinacji kodowej /kodogramu/ podczas przekazywania komend, transmisji danych i informacji telegraficznej -syłabowa czytelność / zrozumiałość/ podczas prowadzenia rozmów telefonicznych; -prawdopodobieństwo identyfikacji szczegółowego odcinka obrazu w trakcie przekazywania informacji za pomocą łączności telefaksowej; -prawdopodobieństwo niewłaściwego adresowania i straty informacji
3	Skrytość	-współczynnik utajniania kanałów /linii /łączności; -prawdopodobieństwo wykrycia obiektu / stacji, węzła / łączności; -matematyczne oczekiwanie ilości rozpoznanych / ujawnionych / obiektów łączności

Tabela 2

Wskaźniki oceny systemów łączności

Lp.	Oceniana właściwość	Wskaźniki
1	Gotowość bojowa	-prawdopodobieństwo terminowego realizowania kompleksu przedsięwzięć zapewniających osiągnięcie przez sieć łączność odpowiedniego stopnia gotowości w określonym czasie; -czas przejścia sieci łączności w wymagany stopień gotowości obronnej
2	Przepustowość	-maksymalna szybkość przekazywania sygnałów; -ilość standardowych kanałów w kierunku / odcinku łączności / łączności; -matematyczne oczekiwanie liczby kanałów w kierunku / odcinku sieci / łączności;
3	Trwałość	-współczynnik sprawnego działania i średni czas sprawnego funkcjonowania kierunku łączności; -prawdopodobieństwo tego że czas przerwy w łączności nie przekroczy granicy dopuszczalnej; -prawdopodobieństwo żywotności sieci, kierunku łączności; -matematyczne oczekiwanie ilości gotowych do pracy kanałów w kierunku łączności; -prawdopodobieństwo zespolenia / powiązania pary węzłów w sieci łączności
4	Mobilność Adaptacyjność	-prawdopodobieństwo terminowego zrealizowania określonych przedsięwzięć w celu zmiany struktury sieci łączności; -dopuszczalny czas realizacji postawionych zadań
5	Bezpieczeństwo	-matematyczne oczekiwanie liczby elementów sieci łączności wykrytych technicznymi środkami rozpoznania przez przeciwnika w określonym czasie; -prawdopodobieństwo ujawnienia elementów sieci łączności; -czas wykrycia określonej liczby elementów sieci łączności z odpowiednim prawdopodobieństwem; -współczynnik bezpieczeństwa sieci łączności

Efektem właściwego doboru ww. wskaźników jest możliwość wykorzystania przez abonentów, całego dostępnego im potencjału komutacyjnego i transmisyjnego sieci. Jednocześnie, przy wystąpieniu rozległych uszkodzeń struktur, jest zagwarantowana możliwość realizacji połączeń dla najważniejszych abonentów systemu.

W krajach NATO do praktycznej oceny wskaźników eksploatacyjnych systemów łączności stosowane są zautomatyzowane procedury oparte na systemach komputerowych. Procedury te są jednocześnie ich systemem zarządzania. Wszystkie te procedury można podzielić na cztery podstawowe grupy związane z procesami:

- planowania systemu i kontroli realizacji;
- nadzoru - zarządzania istniejącymi zasobami;
- kontroli jakości świadczenia usług;
- bezpieczeństwa sieci.

Uzyskiwanie żądanych wskaźników efektywności systemu jest więc procesem interakcyjnym realizowanym w sposób ciągły 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. Należy podkreślić, że w systemie łączności na potrzeby obronności państwa powinno się:

- efektywnie wykorzystywać organiczne podsystemy łączności;
- przydzielać częstotliwości urządzeniom nadawczym na okres zagrożenia państwa i wojny;
- realizować przez podmioty gospodarcze a szczególnie resort łączności zadania obronne na rzecz sił zbrojnych;
- rozbudowywać i programować wykorzystanie obiektów i linii telekomunikacyjnych oraz ich ochronę i obronę na całym terytorium kraju;
- prognozować kierunki rozwoju i produkcji środków i systemów telekomunikacyjnych;
- ustalać sposoby usuwania niesprawności (awarii) i zakłóceń systemu;

Umożliwi to poprawę wskaźników systemu łączności takich jak gotowość bojowa wojsk, żywotność, mobilność. Szybkość przekazywania informacji oraz stopień ich wiarygodności są podstawowymi czynnikami, które decydować będą o efektywności działań obronnych.

Skuteczność systemu obronnego Państwa jest determinowana sprawnością jego procesu informacyjnego.

Organizowany na obszarze kraju system łączności powinien świadczyć usługi łączności najwyższym organom władzy i administracji państwa jednostkom wojsk

operacyjnych, obrony terytorialnej, obrony regionalnej. Posiadać odpowiednią elastyczność. System powinien mieć możliwość wydzielenia podsystemu polowego, zapewniającego dowodzenie siłami zbrojnymi przeznaczonymi do działania na wskazanym kierunku. Weryfikacja teoretycznych podstaw i praktyczna realizacja budowy systemu łączności stosownie do nowych wymagań oraz przewidywanych potrzeb staje się jednym z najważniejszych problemów obronności państwa, który wymaga pilnego rozwiązania.

2. WSPÓLDZIAŁANIE SYSTEMÓW ŁĄCZNOŚCI

Zastosowanie na współczesnym polu walki nowoczesnej broni powoduje że sytuacja pola walki zmienia się błyskawicznie. Powoduje to że reakcja dowódcy musi być natychmiastowa. Dlatego stworzono automatyczną koncepcję zbierania, przetwarzania, przesyłania, i wykorzystywania informacji na potrzeby dowodzenia wojskami. System określony akronimem C4I (Command, Control, Communication, Computers, and Intelligence) czyli zautomatyzowany system dowodzenia, kierowania, łączności i rozpoznania. C4I charakteryzują się zdolnością do wypracowania w czasie rzeczywistym, decyzji dotyczących prowadzenia działań. Obecnie na zachodzie używa się akronimu C4I2/EW. System ten jest wyrazem dążenia do osiągnięcia integracji systemu dowodzenia z rozpoznaniem łącznością informatyką oraz walka radioelektroniczną. Podstawę do wyprowadzenia decyzji stanowią informacje zgromadzone z wykorzystaniem systemów CIS (Communication and Information System)

Ostatnie zmiany w układzie sił politycznych w Europie spowodowały konieczność współdziałania sił zbrojnych państw koalicyjnych w ramach jednej struktury dowodzenia. Dla przykładu jednostki IFOR/SFOR, zabezpieczające operacje pokojowe w byłej Jugosławii, działają pod międzynarodowym dowództwem. Podobnie Brygada Nordycka, w skład której wchodzi nasi żołnierze, również działa w strukturze międzynarodowej. W takim wypadku niezbędny jest odpowiedni stopień współdziałania nie tylko ludzi, ale i sprzętu lub w większym wymiarze systemów telekomunikacyjnych i informatycznych wykorzystywanych w dowodzeniu i kierowaniu.

Podczas wspólnych operacji prowadzonych przez siły zbrojne różnych państw, np. podczas misji ONZ, oprócz znajomości języków obcych, żołnierze muszą mieć możliwość wykorzystania elementów narodowych CIS do współdziałania ze sobą. Oznacza to, że radiostacje polskie i amerykańskie muszą mieć wspólne pasmo częstotliwości roboczych i

spełniać kryteria kompatybilności elektromagnetycznej. Zadaniem interoperacyjności jest między innymi dopasowanie standardu wymiany danych pomiędzy tymi sieciami.

Projektanci współczesnych wojskowych systemów telekomunikacyjnych i informatycznych pracują nad zapewnieniem współdziałania tych systemów tzw. interoperacyjnością. Zgodnie z definicją zaczerpniętą ze „Słownika terminów i definicji NATO”:

Interoperacyjność to zdolność systemów, jednostek lub sił do świadczenia usług i korzystania z usług innych systemów, jednostek lub sił oraz użycia tych usług (odpowiednio zmienionych) do wspólnego i efektywnego działania.

Powyższa definicja zawiera wszystko, z punktu widzenia wojska, również współdziałanie amunicji czy też paliwa do czołgów. Nas interesują systemy telekomunikacyjne i informatyczne, wobec czego formułkę powyższą musimy nieco zmodyfikować.

Interoperacyjność to zdolność systemów CIS do wymiany danych, w środowisku zależnym czasowo, dla zabezpieczenia procesów decyzyjnych użytkownika z zachowaniem znaczenia i relacji wymienianych danych.

System CIS najogólniej można rozpatrywać jako trzystopniową strukturę hierarchiczną, składającą się z następujących warstw:

- sieci strategicznej w skład której wchodzi przeważnie stacjonarne węzły telekomunikacyjne, wyposażone w sprzęt wojskowy i cywilny, połączone łąkami własnymi i dzierżawionymi;
- sieci taktycznej tworzonej głównie z węzłów mobilnych połączonych ze sobą liniami radiowymi, a także dowiązanych do przygotowanego wcześniej pomocniczego systemu kratowego;
- sieci radiowej pola walki zapewniającej łączność ruchomą na najniższych szczeblach dowodzenia.

Idealnym rozwiązaniem by było, gdyby wszystkie kraje członkowskie NATO wyposażono w taki sam system CIS. Jest to oczywiście nierealne, choćby ze względu na inwestycje już poczynione w narodowe systemy dowodzenia i kierowania wojskami. Wobec tego rozpoczęto prace nad takim rozwiązaniem, które uwzględniając architekturę, zasady działania i formaty przekazywanych wiadomości w istniejących i nowo projektowanych systemach, zapewni żądany poziom współdziałania.

W NATO utworzono specjalną agencję o nazwie ADSIA do rozwiązania tego problemu. Przyjęła ona spójne założenia i opracowała jednolity program wprowadzania interoperacyjności do systemów CIS. Powstał tzw. model współdziałania NATO (NATO Interoperability Model), który określa potrzeby i wymagania stawiane systemom CIS pod kątem ich interoperacyjności. Składa się on z trzech części:

1. Operacyjnej

Uszczegóławia zależności, definicje oraz zastosowania różnych typów informacji (danych), które wymieniane są pomiędzy jednostkami narodowymi.

2. Proceduralnej

Definiuje format oraz sposób prezentacji wymienianych danych w celu zapewnienia ich jasności i jednoznaczności.

3. Technicznej

Definiuje funkcjonalne i fizyczne charakterystyki sprzętu oraz sieci, z użyciem których powyższe dane są wymieniane.

W NATO nie istnieją jeszcze systemy telekomunikacyjne czy informatyczne w pełni oparte na wspólnej architekturze. Są one w trakcie opracowywania. Wiąże się to z dużymi kosztami, które obniża się poprzez zastosowanie ogólnie przyjętych standardów. W niektórych obszarach istnieje ich po prostu zbyt wiele (podobnie zresztą jak organizacji standaryzujących). Aby sytuację nieco poprawić NATO bezpośrednio współpracuje z następującymi organizacjami standaryzującymi:

- International Standard Organization (ISO) i International Electrotechnical Commission (IEC);
- International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-TS);
- X/Open;
- Tri-Service Group on Communication and Electronics (TSGCE);

Ponieważ coraz częściej pojawiają się na rynku rozwiązania dotyczące współdziałania systemów cywilnych, NATO śledzi je pod kątem zastosowań w swoich systemach. Dotychczas CIS były zamkniętymi systemami, które opracowywano z wykorzystaniem nietypowych i niestandardowych rozwiązań. Przykładem jest wykorzystywanie specjalistycznych układów o podwyższonej niezawodności, produkowanych w krótkich seriach, co znacznie podwyższa koszty całego przedsięwzięcia. Aktualnie popularna jest tendencja do wykorzystywania i adaptacji istniejących rozwiązań komercyjnych tzw. COTS (Commercial Off-The-Shelf) w zastosowaniach wojskowych. Prace tego typu prowadzone są

w wielu krajach, ponieważ związane jest to z redukcją wydatków budżetowych na cele wojskowe.

3. ZMIANY W SYSTEMIE TELEKOMUNIKACYJNYM PROPONOWANE PRZEZ KOMPENDIUM ŁĄCZNOŚCI CYWILNEJ

W strukturze kierownictwa NATO istnieje komórka Komitet Cywilnego Planowania Telekomunikacji (CCPC). CCPC składa się z przedstawicieli władz poszczególnych krajów członkowskich NATO odpowiedzialnych za sprawy związane z łącznością cywilną. CCPC pomaga cywilnym komórkom odpowiedzialnym za planowanie łączności i systemów informacyjnych.

Zadaniem CCPC jest wspomaganie krajowych władz i organizacji w procesie legislacyjnym, szeroko pojętej organizacji świadczenia usług, budowy i eksploatacji cywilnych sieci telekomunikacyjnych i usług pocztowych. Swoje zadania realizuje on w formie wytycznych i zaleceń.

Zalecenia CCPC w zakresie przygotowań obronnych telekomunikacji krajowej zostały zamieszczone w „Kompedium Łączności Cywilnej” wydanym 2 października 1995 r. przez Naczelny Komitet ds. Cywilnego Planowania na Wypadek Zagrożeń (SCEPC).

Celem kompendium jest:

-aby wszyscy użytkownicy systemów łączności, którzy mają do spełnienia rolę w sytuacjach wyjątkowych, kryzysu, wojny byli nadal w stanie spełniać swoje zadania i wspierać Pakt

Zasady ogólne

1. Krajowe i międzynarodowe sieci i urządzenia telekomunikacyjne stanowią część ogólnego potencjału obronnego Paktu.
2. Każdy kraj zobowiązany jest do uruchomienia skutecznych mechanizmów mających na celu zagwarantowanie nieprzerwanej łączności krajowej i międzynarodowej w sytuacjach wyjątkowych, kryzysowych i wojennych. Powinny one zapewniać możliwość regularnych konsultacji, koordynacji oraz wymiany informacji w ramach poszczególnych krajów członkowskich NATO oraz pomiędzy nimi.
3. Operatorzy powinni otrzymywać z maksymalnym wyprzedzeniem informacje dotyczące wymagań obronnych. Łączy się to z koniecznością stałych konsultacji między operatorami i właściwymi władzami krajowymi.

4. Planowanie na okres sytuacji kryzysowych i wojennych może być połączone z planowaniem w sytuacjach wyjątkowych oraz w wypadku klęsk żywiołowych lub wywołanych działaniem człowieka.
5. Niezbędne są konsultacje dwu i wielostronne pomiędzy właściwymi władzami krajowymi i operatorami w celu wdrażania i nieprzerwanej eksploatacji usług międzynarodowych zgodnie z wymogami NATO, a także umożliwienia krajom członkowskim dokonywania wymiany informacji i doświadczeń w zakresie podwyższania potencjalnej dostępności do sieci i usług telekomunikacyjnych.
6. Z uwagi na znaczne zróżnicowanie uwarunkowań w poszczególnych krajach Komitet Cywilnego Planowania Telekomunikacji (CCPC) zobowiązany jest do określenia form i mechanizmów konsultacji, koordynacji i wymiany informacji.
7. CCPC powinien śledzić wyniki prac innych organizacji międzynarodowych (ITU, CEPT, OECD itp.) mających wpływ na politykę telekomunikacyjną NATO.

3.1. Koordynacja działań w sytuacjach kryzysowo - wojennych

W sytuacjach kryzysowo - wojennych sieci i usługi telekomunikacyjne muszą sprostać nagłym zmianom natężenia ruchu oraz pilnej potrzebie wspomagania działań obronnych. Zakres zniszczeń w sieci może być różny w zależności od kraju oraz jego regionu. W powstałych warunkach działania operatorów w zakresie budowania, konserwacji i odtwarzania łączności krajowej i międzynarodowej nie będą możliwe bez odpowiedniej koordynacji. W wyniku decyzji władz krajowych operatorzy powinni przejść z działalności pokojowej na wojenną, zgodnie z wcześniej przygotowanymi planami, zawierającymi następujące przedsięwzięcia:

1. Uruchomienie środków bezpiecznej łączności zapewniającej działania koordynacyjne na płaszczyźnie krajowej i międzynarodowej w celu zapobieżenia przeciekom niejawnych informacji, dotyczących między innymi lokalizacji i zakresu uszkodzeń sieci.
2. Zorganizowanie i wdrożenie wymiany raportów o stanie łączności pomiędzy krajowymi ośrodkami kierowania łącznością.
3. Nawiązanie współpracy z władzami krajowymi odpowiedzialnymi za podejmowanie decyzji w sytuacji, kiedy urządzenia komercyjne przestaną wystarczać do spełnienia wymagań obronnych (wzmocnienie z rezerw lub określenie priorytetów).

4. W wypadku katastrofalnego uszkodzenia sieci użytku publicznego, - wdrożenie awaryjnych środków koordynacji na szczeblu krajowym lub regionalnym.

3.2. Działania i środki do uwzględnienia w procesie planowania obronnego

W czasie pokojowej działalności operatorzy muszą reagować na szereg sytuacji mających wpływ na ich zdolność obsługi ruchu i świadczenia usług. Tryb działania operatorów telekomunikacyjnych w czasie pokoju winien być kontynuowany w możliwie pełnym zakresie w czasie eskalacji sytuacji kryzysowej i wojny. Operatorzy muszą opracować plany uwzględniające szereg czynników podanych niżej.

3.3.1. Personel i zarządzanie

a) Planowanie obronne powinno uwzględniać możliwość powstania braków kadrowych w wypadku powszechnej mobilizacji w kraju oraz potrzebę zapewnienia (np. za pomocą alokacji kadr) wykwalifikowanego personelu telekomunikacyjnego. Personel musi zostać przeszkolony i otrzymać odpowiednie instrukcje do działania.

b) Należy planować i przygotować:

- ośrodki zarządzania w sytuacji kryzysowej i kwaterę centrum zarządzania na czas wojny;
- wzmocnienie operatorów na obszarach, gdzie spodziewane jest wzmożenie działań;
- redukcję działalności mającej mniejsze znaczenie;
- wzmocnienie bezpieczeństwa wewnętrznego i zwiększenie personelu na służbie w celu ochrony przed sabotażem, działalnością wywrotową itp.;
- urządzenia rezerwowe, zapasy i możliwości produkcyjne na okres kryzysu i wojny;
- akcję informowania i instruowania społeczeństwa o dobrowolnych lub obowiązkowych ograniczeniach w wykorzystywaniu usług telekomunikacyjnych.

3.3.2. Planowanie sieci telekomunikacyjnych

Planowanie budowy i eksploatacji sieci publicznych w czasie pokoju ma na celu nie tylko zapewnienie potrzeb komercyjno - usługowych, ale także wymagań okresu kryzysu i wojny, na przykład w zakresie jej żywotności i elastyczności. Biorąc pod uwagę wymagania

obronne, możliwość technicznej realizacji oraz ograniczenia finansowe, należy w planowaniu uwzględnić następujące środki:

- postawić wymagania w zakresie wielospójności węzłów i obiektów telekomunikacyjnych. Wielospójność uzyskiwać poprzez planowanie przebiegów tras w różnych rejonach geograficznych;
- zróżnicować przebiegi tras kablowych i mikrofalowych pomiędzy regionami państwa i państwami, dając pierwszeństwo w wykorzystywaniu raczej relacji kablowych dla najważniejszych kanałów łączności;
- dokonywać obejść strategicznych obiektów narażonych na zniszczenie w pierwszej kolejności, planować rozmieszczenie urządzeń rezerwowych dla węzłów i stacji wzmacniakowych;
- przygotować możliwości dynamicznej zmiany przepustowości określonych relacji łączności poprzez planowanie odpowiedniej nadmiarowości przepływności oraz określenie priorytetu w ruchu i czasu dostępu do sieci;
- kierowanie ruchu przez jak największą dostępną liczbę, co umożliwi obsługę najważniejszego ruchu w wypadku dużych zniszczeń;
- zorganizowanie ciągłego nadzoru nad poszczególnymi częściami sieci, odpowiedniego systemu sprawozdawczości i bezpiecznej sieci łączności dyspozytorskiej, co będzie miało podstawowe znaczenie dla nieprzerwanej eksploatacji sieci w warunkach kryzysowo - wojennych.

3.3.3. Instalacje i urządzenia telekomunikacyjne

Biorąc pod uwagę konieczność zrównoważenia wymagań obronnych, wykonalności technicznej i ograniczeń finansowych w zakresie uzyskania niezbędnego poziomu żywotności sieci, należy uwzględniać następujące środki:

- krajowe i międzynarodowe centra komutacyjne i zarządzające powinny wzajemnie wspomagać swoje działania oraz przejmować pracę zniszczonych lub poważnie uszkodzonych;
- zapewnić odpowiedni poziom ochrony fizycznej wszystkich części sieci odpowiadających za jej żywotność, a szczególnie centrów komutacyjnych, teletransmisyjnych i zarządzających, ważnych relacji kablowych oraz wszystkich obiektów, linii i stacji radiowych;

- mimo spadku zagrożenia ze strony impulsu elektromagnetycznego w uzasadnionych wypadkach problem ten powinien być rozważany;
- w miarę możliwości uwzględniać alternatywne wprowadzenie kabli do stacji teletransmisyjnych;
- obiekty telekomunikacyjne, magazyny rezerw i inne ważne instalacje telekomunikacyjne lokalizować z uwzględnieniem wykorzystania ukształtowania terenu dla dodatkowej ochrony;
- zapewnić rezerwy mocy i związane z tym zapasy paliw;
- zorganizować system odtwarzania łączności na bazie mobilnych i stacjonarnych rezerw sprzętowych oraz wyszkolonych jednostek remontowo - budowlanych;
- w uzasadnionych wypadkach planować zmniejszenie ilości emisji radiowych;
- przy ocenie i zakupie urządzeń telekomunikacyjnych, tam gdzie inne czynniki są podobne, należy stosować preferencje dla urządzeń bardziej odpornych na warunki wojenne.

3.3. Eksploatacja sieci

W sytuacji wyjątkowej, w czasie kryzysu i wojny publiczne sieci telekomunikacyjne powinny podołać zmianom w modelach ruchu oraz pilnym potrzebom wspomagania działań aliantów. W czasie wojny, nawet po ciężkich zniszczeniach, warunki w obrębie danego kraju mogą być bardzo zróżnicowane. Może zaistnieć sytuacja kiedy na wielu obszarach system świadczenia usług będzie w stanie kompletnego zniszczenia, w innych możliwe będzie normalne jego funkcjonowanie. W takich okolicznościach działania władz cywilnych polegać powinny na zapewnieniu nieprzerwanego świadczenia najważniejszych usług dla kraju i zagranicy.

3.3.1. Zarządzanie siecią

Zarządzanie Siecią definiuje się jako zbiór działań potrzebnych do monitorowania i utrzymania części składowych sieci mających na celu zapewnienie maksymalnego wykorzystania usług świadczonych w sieci, w każdej sytuacji.

Do przeciążenia i zatorów sieci może dojść z wielu powodów, na przykład:

- awarii elementów sieci;
- uwarunkowań zewnętrznych powodowanych dużą liczbą połączeń;
- zatory w połączonych sieciach;

Jeżeli nie zostaną szybko podjęte działania mające na celu kontrolowanie skutków takich wydarzeń, to przeciążenia lub zatory mogą rozprzestrzeniać się i powodować degradację pozostałych części sieci krajowych i międzynarodowych. Działania w ramach Zarządzania Siecią są prowadzone w celu ograniczenia takich wydarzeń.

Bieżące doświadczenia wskazują, że w czasie kryzysu zapotrzebowanie klientów na publiczne usługi komutowane wzrasta. Jeżeli nie zostaną wprowadzone funkcje sterowania w obrębie zarządzania siecią, to liczba zrealizowanych połączeń będzie niższa niż normalnie.

Funkcje sterowania, które można będzie wykorzystać do zapewnienia realizacji połączenia lub realizacji najważniejszych połączeń, obejmują:

- wyłączenie najważniejszych połączeń z funkcji sterowania zarządzania siecią, tak by rozmowy te można było zrealizować w okresach krytycznych;
- specjalne zastosowanie funkcji sterowania zarządzania siecią umożliwiających identyfikację połączeń uprzywilejowanych, takie jak zapewnienie pierwszeństwa dostępu do wolnej pojemności;
- sterowanie liczbą połączeń zarówno wchodzących, jak i wychodzących;
- zapobieganie wybieraniu określonych kierunkowych numerów państw i miast oraz kierunkowych numerów central przez nie uprawnionych użytkowników;
- rekonfiguracja sieci w celu zmiany trasy połączeń przez inne centra komutacyjne w tym samym kraju lub kraju tranzytowym;
- udostępnianie dodatkowych usług lub kanałów dla ważnych użytkowników w sytuacjach awaryjnych.

W czasie pokoju funkcje i techniki sterowania w ramach zarządzania siecią przynoszą operatorom sieci korzyści komercyjne, natomiast w czasie kryzysu lub wojny będą miały zasadnicze znaczenie dla nieprzerwanego świadczenia usług telekomunikacyjnych. Z uwagi na tak poważną ich rolę trzeba zapewnić ciągłość zatrudnienia w Centrach Zarządzania Siecią oraz lokować je w chronionych kwaterach daleko od potencjalnych celów ataku. Łącza komunikacyjne ośrodka (Centrum) z węzłami sieci winny charakteryzować się dużą odpornością. Jeśli to możliwe, centra zarządzania powinny dublować się lub należy zapewnić możliwość wykonania ich funkcji na szczeblu regionalnym lub lokalnym albo w Międzynarodowych Centrach Komutacyjnych.

3.3.2. Uprzywilejowany dostęp do usług telekomunikacyjnych

W sytuacjach, w których nieskuteczny staje się system zarządzania siecią, należy uruchomić funkcje sterowania (ręcznego lub automatyczne), które będą usuwać próby połączeń w zatłoczonych centralach komutacyjnych. Utrudnienie tego typu może dotyczyć określonej grupy użytkowników i powodować zawężenie dostępu do sieci wyłącznie najważniejszym użytkownikom. Przygotowanie takiego systemu sterowania ruchem musi należeć do operatorów. Uruchomienie może być przeprowadzone pod kierownictwem władz krajowych. Władze centralne kraju (współpraca władz cywilnych i wojskowych) powinny zostać zobowiązane do ustalenia, jakiej kategorii użytkownicy są najważniejsi dla sprawnego funkcjonowania społeczeństwa i systemu obronnego kraju. Na podstawie wytycznych władz centralnych, organa władzy na szczeblu regionalnym powinny określić podobną kategorię użytkowników w terenie.

3.3.3. Odtwarzanie międzynarodowych systemów transmisji

W czasie kryzysu i wojny realizacja stałych procedur odtwarzania łączności międzynarodowej uzgodnionych pomiędzy operatorami może być utrudniona. Wówczas konieczne będzie zorganizowanie działań natychmiastowych, przy użyciu najlepszych urządzeń, jakie jeszcze pozostały do dyspozycji. Niezbędne okazać się mogą w takim wypadku konsultacje między operatorami telekomunikacji cywilnej oraz między nimi a krajowymi władzami cywilnymi i wojskowymi.

Poszczególne kraje winny ustalić cywilne międzynarodowe kanały wydzielone, które uważa się za mające istotne znaczenie dla ogólnych możliwości obronnych Paktu i z uwagi na to w czasie kryzysu i wojny zapewnić ich funkcjonowanie.

3.3.4. Krajowe sieci awaryjne

Każdy kraj może budować sieci wydzielone od usług telekomunikacyjnych użytku publicznego na potrzeby władz krajowych w sytuacji wyjątkowej, w czasie kryzysu i wojny. Tego rodzaju sieci są zazwyczaj ograniczone pod względem pojemności ruchu. Uważa się za

korzystne połączenie krajowych sieci awaryjnych w czasie pokoju lub w początkowym okresie sytuacji kryzysowej.

System teletransmisyjny do realizacji połączeń w sieci powinien być maksymalnie odporny na oddziaływania zewnętrzne, zapewniać alternatywny wybór tras, różnorodną dystrybucję kanałów. Każdy kraj będzie chciał sprawować pewnego rodzaju kontrolę nad połączeniami przychodzącymi z zewnątrz do jego sieci awaryjnej, poprzez połączenia półautomatyczne. Zatrudnieni operatorzy powinni znać - oprócz języka ojczystego - angielski lub francuski.

Szkolenia i ćwiczenia

Niezbędnym i jednym z najważniejszych zadań w ramach przygotowań obronnych w telekomunikacji jest systematyczne szkolenie i uczestnictwo władz krajowych, odpowiedzialnych za telekomunikację, operatorów, jednostek remontowo - budowlanych, dostawców usług i producentów sprzętu w ćwiczeniach krajowych i międzynarodowych NATO.

Cele szkoleń i ćwiczeń:

1. Utrzymanie wysokiego poziomu realizacji zadań wspierających NATO w sytuacjach stanu pogotowia, kryzysu i wojny.
2. Ćwiczenie procedur i działań nie będących w codziennym użytku.
3. Ćwiczenie opanowywania sytuacji, w których - w celu najlepszego wykorzystania sprzętu telekomunikacyjnego - wymagana jest koordynacja działań pomiędzy władzami cywilnymi, wojskowymi i sztabem NATO.
4. Umożliwienie operatorom przećwiczenia procedur zarządzania siecią w sytuacjach kryzysu i wojny.
5. Doskonalenie współdziałania operatorów w kierunku poprawy ich zdolności do wspierania działań NATO.

4. NORMY PROPONOWANE PRZEZ NATO

Postęp technologiczny pozwolił na stosowanie systemów telekomunikacyjnych i informatycznych, które mogą przetwarzać i przenosić bardzo duże ilości informacji. Mają one coraz większą zdolność do komunikowania się na duże odległości, z dużą liczbą użytkowników, różnymi sposobami i przy coraz większej

niezawodności. W procesie komunikowania zaangażowanych jest wiele krajów i organizacji międzynarodowych, co powoduje konieczność zapewnienia możliwości współpracy sieci i urządzeń. Dlatego też standaryzacja jest kluczowym zagadnieniem w rozwoju telekomunikacji. NATO, aby wypełnić swoje zadania, obejmujące swoim zasięgiem rozległe obszary geograficzne, działanie systemu łączności jest w dużej mierze zależne od żywotności, niezawodności, zgodności ze wszystkimi standardami urządzeń i sieci telekomunikacyjnych. Biorąc pod uwagę rozwój sieci cywilnych, NATO zaakceptowało potrzebę posługiwania się cywilnymi standardami światowymi. W rzeczywistości niezbędnym zakresie tworzone są własne standardy NATO, po wcześniejszym przeprowadzeniu konsultacji i koordynacji z władzami krajowymi, operatorami sieci i dostawcami urządzeń. Za problemy standaryzacji w NATO odpowiedzialna jest Wojskowa Agencja Normalizacyjna (MAS). W dziedzinie telekomunikacji Porozumieniami Standaryzacyjnymi zajmuje się grupa EUROCOM. STANAG-i to normy NATO wytworzone przez Wojskową Agencję Normalizacyjną określające wszelkie aspekty działalności wojskowej. STANAG-i są niezbędne w każdym momencie dostosowania do używanych, nowych systemów CIS Polski i systemów państw NATO. Wszystkich STANAG-ów jest ponad 1000 z czego w posiadaniu Wojskowego Biura Służb Normalizacyjnych jest 600 na dzień dzisiejszy przetłumaczonych na język polski jest 380. WBSN otrzymało zadanie pogrupowania ich w kategorie tematyczne, a dokładniej mówiąc posegregowanie potrzebnych norm ze względu na rodzaj sił zbrojnych. Po dokonaniu tego podziału zostaną wydzielone normy odpowiadające za łączność.

VI. ZAGROŻENIA SYSTEMU TELEKOMUNIKACYJNEGO W CZASIE POKOJU, KRYZYSU I WOJNY ORAZ METODY OCHRONY

WSTĘP

Działalność w zakresie przygotowania sieci telekomunikacyjnej użytku publicznego do wykonania zadań w okresie wojny wynika z ustawy o powszechnym obowiązku obrony RP, uchwały Komitetu Obrony Kraju o militaryzacji i szeregu innych aktów normatywnych.

Przygotowanie obronne sieci telekomunikacyjnej polega głównie na zapewnieniu pożądanego stopnia jej żywotności w warunkach oddziaływania środków rażenia oraz zwiększonego prawdopodobieństwa wystąpienia klęsk ekologicznych. Żywotność tę osiąga się poprzez zabiegi uodporniające oraz sprawne odtwarzanie zniszczonego potencjału.

Rozkład przestrzenny zagrożeń jest bardzo nierównomierny, stąd wzięcie go pod uwagę w przestrzennym rozmieszczeniu węzłów i linii sieci łączności spowoduje wzrost uodpornienia.

Współczesna technika cyfrowa w telekomunikacji pozwala już, w odróżnieniu od dotychczasowej - analogowej, na rozproszenie struktury i taką lokalizację zasadniczego sprzętu, aby uodpornić system na destrukcyjne oddziaływania zewnętrzne.

Znając możliwości oddziaływania destrukcyjnego na system telekomunikacyjny, jednocześnie stosując rachunek ekonomiczny, można stworzyć kompleksowy program uodpornienia przydatny w czasie pokoju i spełniający wymogi na okres kryzysu i wojny.

1. ZAGROŻENIA ZEWNĘTRZNE SYSTEMU TELEKOMUNIKACYJNEGO

1.1. Zagrożenia w czasie pokoju

Przyjmuje się oddziaływanie na siatkowy, cyfrowy system telekomunikacyjny budowany w oparciu o transmisję kablową i częściowo linie radiowe, z uwzględnieniem radiodostępu np. telefonii komórkowej. Jest to system stacjonarny użytku publicznego powiązany z systemami resortowymi, min. sił zbrojnych. W czasie kryzysu i wojny dowiąże się do niego połowy system wojskowy zwłaszcza szczebla strategicznego i operacyjnego.

Każdy z elementów systemu może być niszczone poprzez oddziaływanie zewnętrzne. W czasie pokoju system telekomunikacyjny może być niszczone (poza naturalnymi uszkodzeniami wynikającymi z niedoskonałości sprzętu) w wyniku:

a) oddziaływań losowych środowiskowych:

- powodzi
- katastroficznych zatopień,
- ulewnych deszczy,
- pożarów,
- trzęsień ziemi - w Polsce występują rzadko i o słabej sile,
- tąpnięcia,
- rozprzestrzenienia się przemysłowych środków trujących,
- eksplozji gazów lub pyłów,
- wyładowań atmosferycznych,
- uszkodzeń linii wysokiego napięcia, innych awarii zasilania,
- uszkodzeń urządzeń przeciwzakłóceń w urządzeniach elektrycznych, zwłaszcza dużej mocy,
- fali uderzeniowej, impulsu elektromagnetycznego i promieniowania radioaktywnego od katastrofy urządzeń jądrowych.

b) oddziaływań losowych w wyniku niecelowych działań ludzkich:

- błędów użytkowników i personelu powodujących awarie, uszkodzenia, skasowania zbiorów, przekonfigurowanie systemu itp,
- nieumyślne spowodowanie dekonspiracji podsystemu zabezpieczenia poufności informacji.

c) oddziaływań celowych:

- oddziaływania radioelektronicznego (głównie rozpoznania radioelektronicznego prowadzonego w czasie pokoju, a nasilonego w czasie kryzysu i wojny),
- dywersji prowadzonej przez grupy zainteresowane zniszczeniem lokalnych elementów sieci,
- próby przerwania funkcjonowania systemu
- próby programowego przekonfigurowania elementów sieci,
- próby ataku na system zabezpieczenia poufności informacji,
- próby korzystania z systemu bez ponoszenia opłat.

Przykładowe zagrożenia przedstawiają tabele 1 i 2.

Tab. 1. Przykładowe metody włamywania się do sieci telefonicznej

Rodzaj sprzętu	Metoda włamywania
Centrala PABX	Niewłaściwe skonfigurowanie centralki. Włamanie przez port zdalnej kontroli po wprowadzeniu odpowiedniego tonu lub hasła.
Telefony komórkowe	Podrobienie układu scalonego zawierającego numer aparatu. Odegranie sekwencji nawiązującej połączenie innego aparatu.
Karty telefoniczne	Podrobienie karty magnetycznej lub mikroprocesorowej
Automat telefoniczny	Oddziaływanie polem magnetycznym. Uszkodzenie mechaniczne wyłączające układ naliczania.

Tab. 2. Zagrożenia w systemach komputerowych

Obiekt zagrożenia	Działanie niecelowe	Działanie celowe (świadome)
Centrum komputerowe	Pożar, powódź, inne kataklizmy. Awaria instalacji: gaśniczej, zasilania, klimatyzacji itp.	Podpalenie. Sabotaż. Strajk okupacyjny.
Infrastruktura telekomunikacyjna	Błędy przesyłania, adresowania danych	Podśluch linii.
Wykonywanie programów	Korzystanie z nieaktualnej wersji pliku lub programu.	Kopiowanie oprogramowania. Wprowadzanie wirusa do programów
Korzystanie z systemu	Błąd przy wprowadzaniu danych. Zniszczenie pliku przez nieuwagę.	Świadomy błąd wprowadzania danych. Kopiowanie, podmiana lub niszczenie plików. Wykonywanie robót niedozwolonych lub własnych.
Nośniki danych	Błąd przy manipulacji nośnika powodujący utratę danych. Zniszczenie danych elektrycznością statyczną lub polem magnetycznym.	Kradzież nośników. Podmiana nośnika. Kopie nośników w celu analizy danych.

1.2. Zagrożenia w czasie kryzysu i wojny

W czasie kryzysu i wojny zagrożenia już wymienione mogą się nasilić, a ponadto mogą wystąpić:

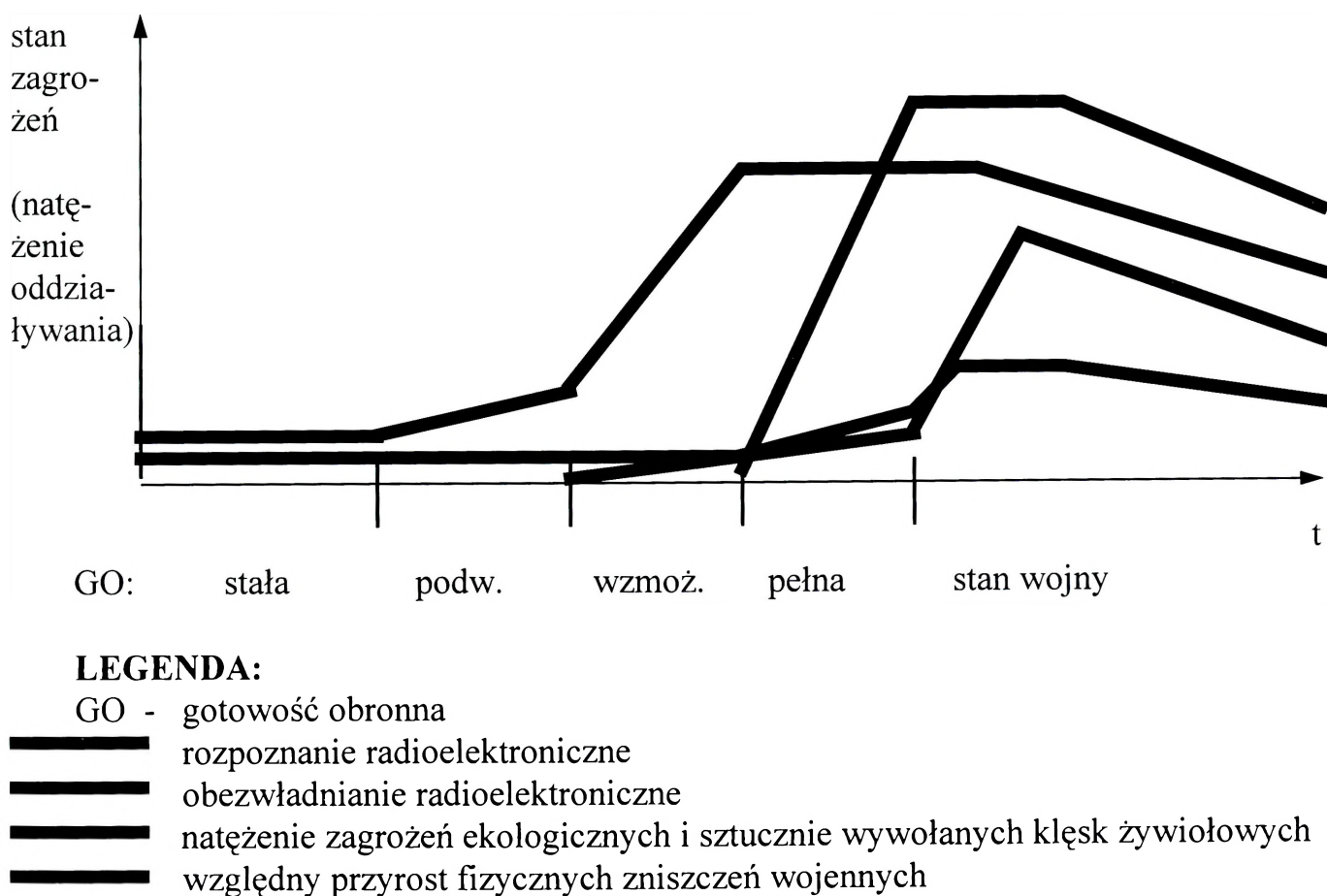
a) oddziaływania niszczące - bronią konwencjonalną (w tym precyzyjną)

b) oddziaływania niszczące - bronią masowego rażenia:

- bronią chemiczną i biologiczną;
- bronią jądrową - zniszczenia fizyczne, poprzez promieniowanie radioaktywne i impuls elektromagnetyczny,

c) oddziaływanie radioelektroniczne - walka radioelektroniczna.

W trakcie zmian stanów gotowości obronnej państwa (przed groźbą wojny) zacznie narastać stopień dezorganizujących system łączności oddziaływań zewnętrznych (niszczenia, rozpoznania i obezwładniania radioelektronicznego), który będzie maleć w czasie konfliktu wskutek wyczerpywania się potencjałów walczących stron (rys. 1). Rysunek ten przedstawia narastanie zniszczeń związanych z prowadzeniem walki zbrojnej.



Rys. 1. Przebieg zmian zagrożeń w czasie narastania konfliktu i wojny.

Schemat poglądowy.

1.1.1. Potencjał sił zbrojnych państw ościennych

Jednym ze wskaźników określających z pewnym prawdopodobieństwem stopień zagrożenia lokalnym konfliktem zbrojnym jest potencjał militarny i możliwości jego zwiększenia w określonym czasie przez państwa ościenne. W celu zachowania bezpieczeństwa zostały określone Traktatem Paryskim z 19 listopada 1991 r. limity uzbrojenia (które przedstawia poniższa tabela. Do tych wartości przyrównano stany rzeczywiste z połowy roku 1996.

Tab. 3. Potencjał militarny wybranych państw
(limit wg Traktatu Paryskiego/ stan z połowy roku 1996)

Lp	Państwo	Żołnierze	Czołgi	Transp. Opanc.	Artyleria pow. 100 mm	Samoloty bojowe	Śmigłowce uderz.
1	Polska	250000 210000	1730	2150	1610	460	130
2	Niemcy	345000 362000	4166 3490	3446 2622	2705 2068	900 578	306 224
3	Rosja	1430000	6400	11480	6415	3450	890
	Ogółem	818470	5490	9870	6090	2989	825
	Flota bałt.**	31000	26	166	34	102	12
	Obw. Kaliningr.	24560	853	924	411	?	52
4	Ukraina	450000 370000	4080 4039	5050 4896	4040 3727	1090 270	330 270
5	Białoruś	100000 76000	1800 2183	2600 2839	1615 1533	260 338	80 79
6	Czechy	90000 65000	957 953	1367 1363	767 767	230 187	50 36
7	Słowacja	50000 46000	478 478	638 638	383 383	115 114	25 19
8	Litwa*	9300		33		4	

* nie objęta traktatami

** 170 okrętów wojennych

Broń nuklearną posiada Rosja - 886, Ukraina - 158 i Białoruś - 18.

Jak widać z tabeli 3, państwa europejskie w zasadzie dostosowały się do przyjętych limitów, natomiast jakościowo sprzęt jest uzależniony od możliwości gospodarczych i technologicznych. Różnice istnieją zwłaszcza w możliwościach automatyzacji procesów informacyjnych i decyzyjnych związanych z rozpoznaniem dowodzeniem i sterowaniem środkami walki.

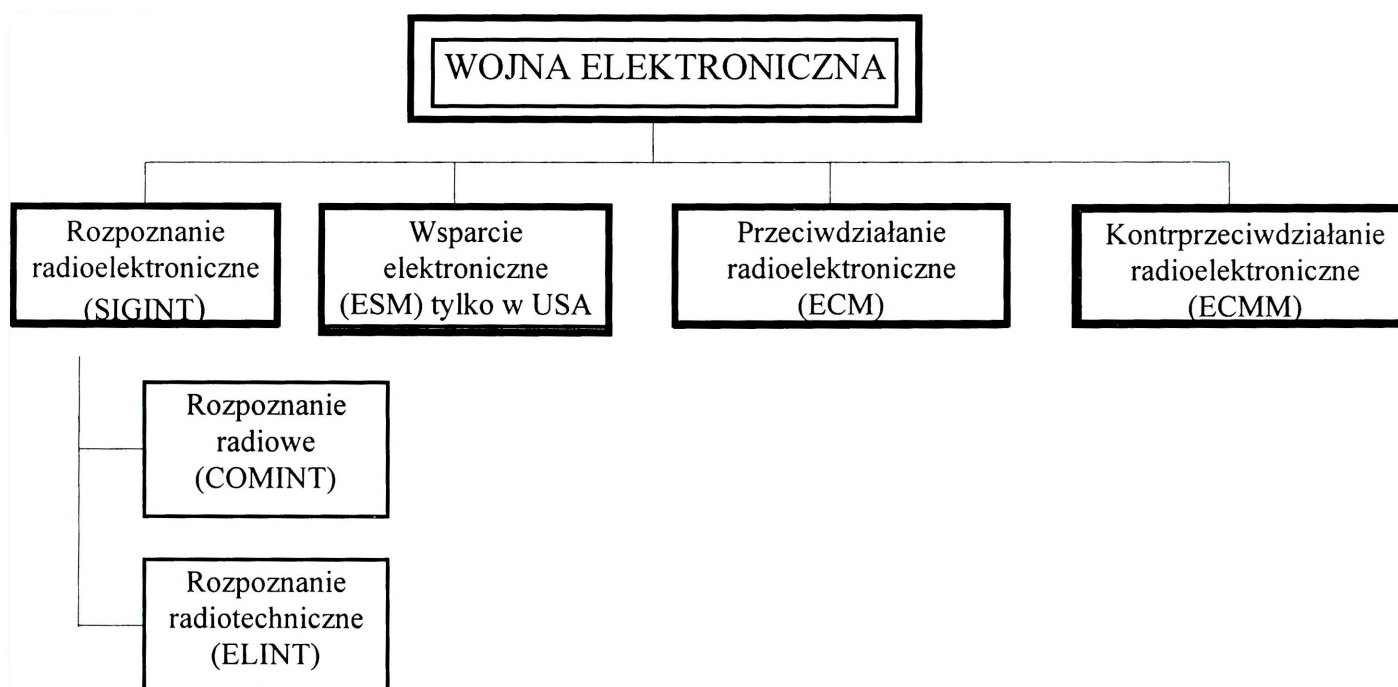
1.1.2. Możliwości oddziaływania radioelektronicznego

Możliwości te są ściśle związane z uwarunkowaniami finansowo-technicznymi.

Rozwinięte potencjały naukowo-techniczne posiadają USA, Niemcy, Rosja. Pozostałe państwa zabezpieczają potrzeby głównie drogą importową.

Walka radioelektroniczna to „zespół przedsięwzięć i działań wojsk wzajemnie powiązanych celem, miejscem i czasem, wykonywanych w sposób kompleksowy, zmierzających do wykrycia i rozpoznania, obezwładniania ogniem i zakłóceniami radioelektronicznymi, technicznych środków i systemów dowodzenia wojskami, kierowania środkami walki, rozpoznania i walki radioelektronicznej przeciwnika oraz zapewnienia stabilnej pracy i efektywnego wykorzystania analogicznych środków i systemów wojsk własnych”.

W armiach zachodnich rozpoznanie radioelektroniczne (jako najskuteczniejsza metoda rozpoznania ogólnowojskowego) jest elementem WRE i zalicza się do „wojny radioelektronicznej” (patrz rys. 2)



Rys. 2. Elementy wojny radioelektronicznej

Rozpoznanie radiowe ma na celu rozpoznanie relacji radiowych przeciwnika. Pozwala na ustalenie stanowisk dowodzenia, struktury ugrupowania i ruchu wojsk. Dane te stanowią podstawę procesów decyzyjnych.

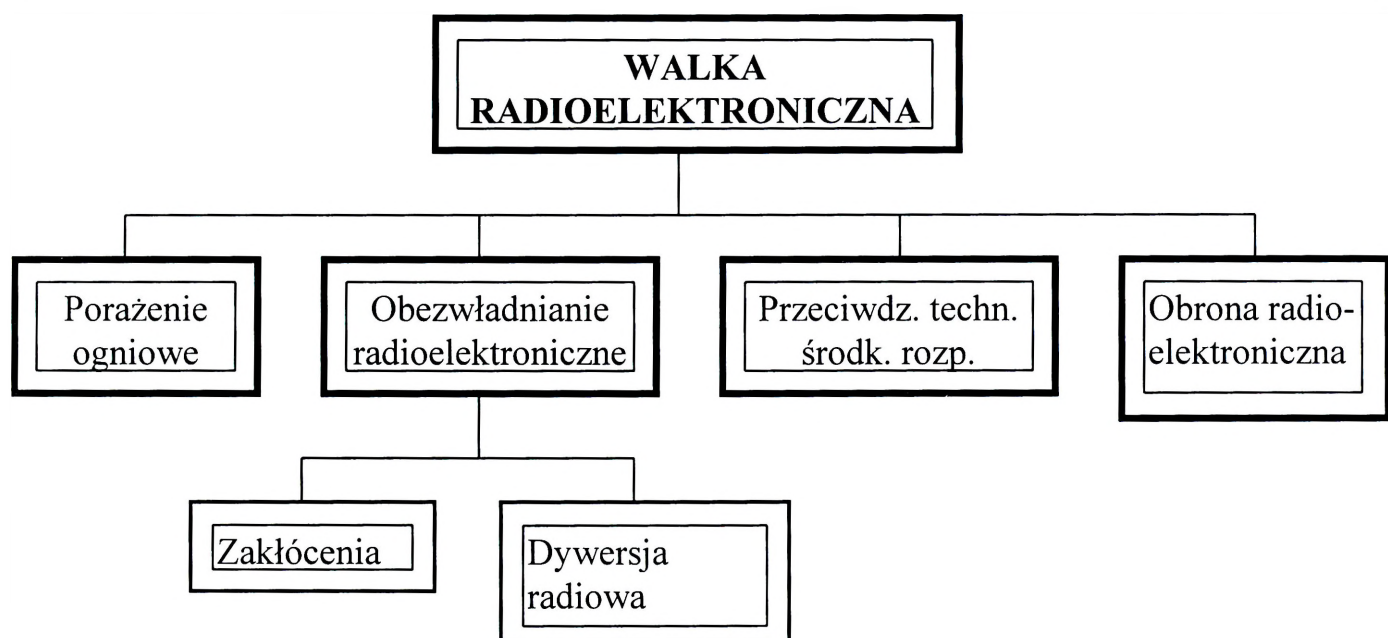
Rozpoznanie radiotechniczne ustala pozycje urządzeń radiolokacyjnych, środków kierowania ogniem i sterowania uzbrojeniem w paśmie radiolokacyjnym i podczerwieni.

Wsparcie elektroniczne dostarcza informacji o wszelkich środkach promieniowania przeciwnika. Służą do ustalania i oceny stopnia zagrożenia, ostrzegania. Bazuje na wcześniej posiadanych informacjach o przeciwniku. Sprzęt używany jak w rozpoznaniu radiowym i radiotechnicznym.

Przeciwdziałanie radioelektroniczne ma za zadanie zakłócanie relacji łączności, elektronicznych systemów namierzania i kierowania oraz aktywne mylenie rozpoznania radioelektronicznego przeciwnika. Łączy się je z oddziaływaniem ogniowym. Wymaga zaplanowania tak, aby nie oddziaływać na środki własne.

Kontrprzeciwdziałanie radioelektroniczne to utrudnianie skutecznego użycia środków rozpoznania i przeciwdziałania radioelektronicznego przeciwnika.

Walka radioelektroniczna (wg poglądów rosyjskich) polega na realizacji następujących zadań (rys. 3):



Rys. 3. Zadania walki radioelektronicznej

Porażenie ogniowe obejmuje użycie broni jądrowej, raketowej, artylerii, lotnictwa (w tym raket, bomb i pocisków samonaprowadzających się na źródła promieniowania elektromagnetycznego), również działania grup specjalnych, dywersyjnych, itd.

Obezwładnianie radioelektroniczne obejmuje aktywne zakłócenia radioelektroniczne i prowadzenie dywersji radiowej.

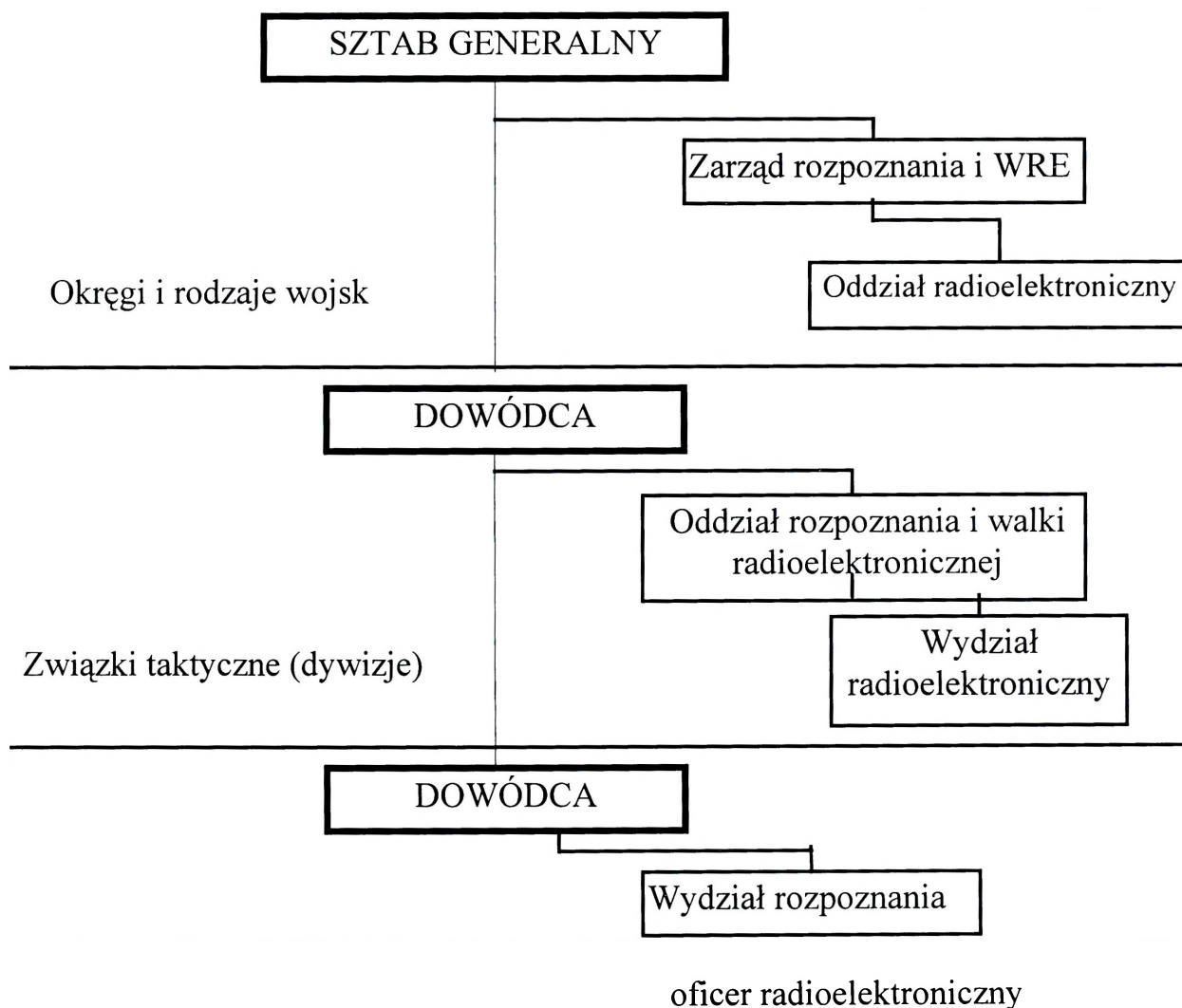
Przeciwdziałanie technicznym środkom rozpoznania przeciwnika realizuje się przez obezwładnianie ogniem i radioelektronicznie, też maskowanie i pozoracja.

Obrona radioelektroniczna środków i systemów radioelektronicznych wojsk własnych polega na niszczeniu fizycznym środków na nie oddziaływujących oraz wykonywaniu szeregu przedsięwzięć organizacyjno-technicznych utrudniających przeciwnikowi prowadzenie rozpoznania.

Tak ujęte zadania nie ujmują rozpoznania, które jest działem osobnym, a w ramach WRE rozpoznanie służy tylko celom walki radioelektronicznej.

W wojnie z Irakiem zcentralizowano kierowanie środkami rozpoznania i walki radioelektronicznej wszystkich rodzajów sił zbrojnych oraz sił kosmicznych. Oceny są pozytywne, stąd prawdopodobnie Rosja zmieni organizację kierowania rozpoznaniem i Wre.

W Siłach Zbrojnych RP od kilku lat zintegrowano pionowy rozpoznania i Wre (patrz: rys 4.).



Rys. 4. Organa kierowania walką radioelektroniczną

Środki walki radioelektronicznej znajdują się na wyposażeniu od dywizji w wojskach lądowych (w naszej armii i rosyjskiej - kompania radioelektroniczna w batalionie rozpoznawczym), w marynarce wojennej i lotnictwie od pojedynczego okrętu (samolotu). Na szczeblu korpusu wojsk lądowych wykorzystuje się pułk radioelektroniczny, na szczeblu centralnym pułk (ośrodek) radioelektroniczny i pułk zakłóceń radioelektronicznych. Niektóre zadania jednostki te realizują już w czasie pokoju. W dyspozycji korpusu znajdują się nadajniki zakłóceń jednorazowego użytku.

Coraz więcej środków walki USA, Niemiec i Rosji posiada autonomiczne środki WRE. W skład nich wchodzi najczęściej: odbiornik ostrzegania, nadajnik zakłócający, wyrzutnia flar i dipoli, odbiornik podczerwieni, urządzenie zakłócające w podczerwieni, planszet sytuacji radioelektronicznej i komputer sterujący. Montowane są na samolotach, śmigłowcach i okrętach.

Szczególne wyposażenie posiadają samoloty specjalne wojny elektronicznej.

Zestawienie ilościowe środków rozpoznania i zakłóceń wojsk lądowych wybranych państw przedstawia tab. 5.

Tabela 5. Zestawienie ilościowe środków rozpoznania i zakłóceń wojsk lądowych wybranych państw

	Rosja			Niemcy			USA		
	DZ	Armia	OW	DZ	KA	Urz. s. ląd.	rppanc	DZ	KA
	komp.	bat.	pułk	komp.	bat.	BWRe	komp	bat	GrWE
Odbiorniki KF		25	100	20	42	50	9	9	32
Odbiorniki UKF	3	6	9				9	11	36
Stacje sterowania		3	4						
Namierniki UKF	2	4		3	8	8	2	6	8
Namierniki KF								3	1
SRL rozp. s. rlok.		6		4	8				
SRL rozp. pola walki		2					6	38	15
SRL rozp syt. pow.		5						4	
stacje rozp. r-lin.		3	3						
stacje zakłóceń KF	3	12	24		10	10	2	6	3
stacje zakłóceń UKF	5	6	6	8	20		6	14	9
Stacje zakłóceń r-lok	9	28	81		10		2	3	
Stacje zakłóceń r-lin.		14	11						3
st.zakłóceń r-nawig.		3	9						

1.1.3. Zagrożenia bezpieczeństwa informacji występujące w systemach łączności i informatycznych

Aktualnie eksploatowane analogowe systemy łączności są przestarzałe, wykorzystują mocno wyeksploatowane urządzenia wykonane w starej technice, mało podatnej na dynamiczne zmiany w organizacji, a w szczególności na zarządzanie i utajnianie, zwłaszcza na utajnianie z gwarantowaną mocą kryptograficzną. Dalsze ich wykorzystywanie stanowi potencjalne i łatwo dostępne źródło, z którego można przypadkowo lub celowo pozyskać duże ilości niejawną informacji. Z kolei łączność cyfrowa i informatyka, choć bardziej podatna na skuteczną ochronę kryptograficzną, niesie nowe zagrożenia.

Analiza zagrożeń elementów systemów łączności narażonych na kompleksowe oddziaływanie w zakresie pozyskania informacji niejawną, powinna się rozpocząć od ustalenia, jakimi sposobami mogą posługiwać się osoby chcące zdobyć niezbędne informacje. Mogą to osiągnąć w wyniku:

1. Błędne działania:

- systemu;
- sprzętu łączności lub komputerów;
- personelu.

2. Awarii:

- zasilania (brak zasilania, wahania napięcia, przepięcia, przebicie);
- sieci transmisji (brak możliwości nawiązania połączenia, zerwanie połączenia, błędy komutacji, przesłuchy i zwarcia, błędy transmisji);
- sprzętu łączności lub komputerów.

3. Klęsk żywiołowych:

- powódź;
- pożar;
- silne wyładowania atmosferyczne;
- wstrząsy.

Taki sposób pozyskiwania informacji określany jest mianem infiltracji i prowadzi do zdobycia, modyfikacji lub zniszczenia informacji.

Infiltracji dokonuje się poprzez stosowanie :

- podsłuchu biernego;
- podsłuchu aktywnego.

Coraz powszechniejsze zastosowanie informatyki do sterowania funkcjonowaniem systemów łączności pozwala na zwiększenie ich możliwości funkcjonalno-użytkowych. Wraz z nimi wprowadza jednak szereg zagrożeń, które mogą wpływać bezpośrednio na właściwe funkcjonowanie sieci łączności i informatycznych.

Podstawowymi zagrożeniami, jakie niesie za sobą zastosowanie informatyki procesach przetwarzania informacji, w tym głównie niejawnej, są emisje (o dość dużym zasięgu) elektromagnetyczne ujawniające: przewodzona i promieniowana. W urządzeniach takich jak elektroniczne centrale cyfrowe, urządzenia teletransmisyjne, komputer, mikrokomputer oraz urządzenia peryferyjne, promieniują praktycznie wszystkie elementy, z których te urządzenia się składają.

Promieniowanie to ma zasięg zróżnicowany w zależności od typu ww. elementów i zawiera się w granicach do 1500 m. tzn. można na taką odległość odczytać informację. Przy tak dużym zasięgu emisji ujawniającej konieczne jest zastosowanie odpowiednich środków ochronnych w celu wyeliminowania lub zmniejszenia zasięgu promieniowania ujawniającego.

W sieciach telekomunikacyjnych, urządzeniach łączności i sieciach komputerowych dodatkowe zagrożenie stanowią przesłuchy pomiędzy obwodami i liniami transmisyjnymi. Na bezpieczeństwo i ochronę informacji wpływ ma szereg, innych nie mniej ważnych zagrożeń, do których zaliczyć możemy:

- niekontrolowany dostęp do zasobów komputerów głównych lub terminali, który może doprowadzić do kradzieży, kopiowania i modyfikowania programów lub zabezpieczeń;
- ujawnienie osobom nie upoważnionym sposobu zabezpieczenia komputera, haseł, identyfikatorów dostępu itp;
- niekontrolowany dostęp do urządzeń sterujących i zarządzających systemami łączności, co w konsekwencji może doprowadzić do okresowego lub całkowitego zablokowania funkcjonowania systemu.

Wszystkie te czynniki mają poważny wpływ na tworzenie warunków bezpieczeństwa informacji podlegającej obróbce w komputerach indywidualnych i sieciach komputerowych oraz sieciach teletransmisyjnych, a także na stan ochrony tych sieci i systemów przed celowym atakiem służb wywiadowczych lub przypadkowym działaniem amatorów-hakerów.

Zasadnicze formy ataku na system to:

1. MASKARADA - ma miejsce wtedy, gdy stacja informatyczna (terminal) udaje, że jest inną stacją (terminalem). Celem Maskarady jest nielegalne zwiększenie swoich uprawnień.
2. POWTÓRZENIA - polegają na ponownym przesłaniu wcześniej nadanej informacji, celem zwiększenia swoich uprawnień.
3. MODYFIKACJA INFORMACJI (KOMUNIKATÓW) - polega na zmianie treści transmitowanych danych w taki sposób, że modyfikacja nie zostanie wykryta. Powszechnie stosowane kodowanie nadmiarowe pozwala na detekcję i ewentualną korektę błędów (zakłóceń) przypadkowych, ale nie chroni danych przed celową modyfikacją.
4. ODMOWA USŁUGI - ma miejsce wtedy, gdy stacja w sposób nielegalny pozbawiona została całości lub części swoich uprawnień albo jej działanie ogranicza innym stacjom wykonywanie właściwych funkcji. Odmowa usługi może obejmować likwidację ruchu przez zniszczenie komunikatów kierowanych do adresata lub generowanie dodatkowego ruchu w sieci.
5. KOŃ TROJAŃSKI - polega na wprowadzeniu do systemu nieuprawnionych funkcji, np. kopiowanie informacji lub komunikatów do nieuprawnionego kanału.
6. POTRZASK - polega na utworzeniu nieuprawnionego efektu na rozkaz, określone zdarzenie lub sekwencję zdarzeń.
7. ANALIZA RUCHU - polega na wnioskowaniu informacji na podstawie obserwacji ruchu w sieci.

2. SKUTKI ODDZIAŁYWAŃ W CZASIE KRYZYSU I WOJNY

W czasie trwania kryzysu i wojny nastąpi kilka rodzajów zniszczeń. Do głównych można zaliczyć:

- a) oddziaływania niszczące - bronią konwencjonalną (w tym precyzyjną)
- b) oddziaływania niszczące - bronią masowego rażenia:
- c) oddziaływanie radioelektroniczne.

Stopień uszkodzeń systemu telekomunikacyjnego z wymienionych powodów można oszacować tylko za pomocą metod statystycznych. Można analizować skutki oddziaływania punktowego, skutki oddziaływania przestrzennego oraz prawdopodobieństwo - na jakim obszarze (rejonie) dane zagrożenia punktowe bądź przestrzenne mogą wystąpić najczęściej.

Pod tym kątem podjęto próbę ustalenia rejonów największych zagrożeń. W tym celu należy określić obszary, rejony o podwyższonym prawdopodobieństwie zaistnienia uszkodzeń i stopień możliwych zniszczeń od każdego z oddziałujących czynników.

2.1. Oddziaływanie klęsk żywiołowych i katastrof ekologicznych

Klęski żywiołowe

a) Powodzie.

Na terenie Polski notuje się przede wszystkim następujące rodzaje powodzi:

- opadowe (długotrwałe deszcze),
- roztopowe (gwałtowne topienie śniegów),
- zimowe (w wyniku zatorów lodowych),
- sztormowe.

Powodzie nie występują znenacka, można je wcześniej przewidzieć, od kilku godzin do kilku tygodni i podjąć odpowiednie kroki zaradcze. Najczęściej występują na obszarach jak rys. 2. Ulewne deszcze, oprócz powodowania powodzi, najczęściej powodują przepełnienie kanalizacji burzowej i zalanie niżej położonych rejonów, w miastach np. piwnic.

b) Zatopienia katastroficzne.

Występują w wyniku uszkodzenia (awarii) tam, zapór, wałów przeciwpowodziowych, śluz, stopni spiętrzających, jazów itp. Skutkiem tych awarii jest gwałtowne wylanie ogromnych ilości wody, w bardzo krótkim czasie, na tereny położone poniżej miejsca awarii. Powstaną również skutki pośrednie np. zniszczenie elektrowni wodnej, linii wysokiego napięcia przechodzącej przez teren zalewany. Cechą zatopień jest gwałtowność zdarzenia i często brak symptomów wskazujących na możliwość wystąpienia. Mogą być wykonane celowo w czasie kryzysu i wojny. Prawdopodobne miejsca wystąpienia przedstawia rys. 2.

Na obszarze prawdopodobnych zatopień zlokalizowanych jest 40 miast i 150 dużych zakładów przemysłowych. Zagrożone zatopieniem jest ok. 2500 km² powierzchni kraju.

c) Pożary.

Najczęściej mogą wystąpić na obszarach zalesionych lub terenach zakładów przemysłowych, skupiskach ludzkich, gdzie zgromadzone są substancje i przedmioty łatwopalne. W wyniku pożarów mogą zaistnieć zniszczenia bezpośrednie i wtórne - klęski

ekologiczne np. pożar w rafinerii naftowej, składnicy gazów przemysłowych, pożar dużych obszarów leśnych. W trakcie walki zbrojnej pożary będą wywoływane celowo.

Katastrofy ekologiczne

a) Uszkodzenia reaktorów jądrowych - radiacja promieniotwórcza. Ponadto jeżeli nastąpi wybuch, swoim zasięgiem w terenie przygranicznym może objąć oddziaływanie impulsu elektromagnetycznego. Wszystkie państwa sąsiadujące z Polską posiadają elektrownie jądrowe. Najmniejsze zagrożenie występuje w centrum Polski.

b) Zagrożenia chemiczne. Występują w pobliżu zakładów i składnic chemicznych oraz dróg transportu kolejowego, drogowego oraz lotniczego. Oddziaływanie głównie na ludzi, choć i niektóre związki chemiczne mogą spowodować awarie sprzętu elektronicznego. Rejony zagrożeń przedstawia rys. 2.

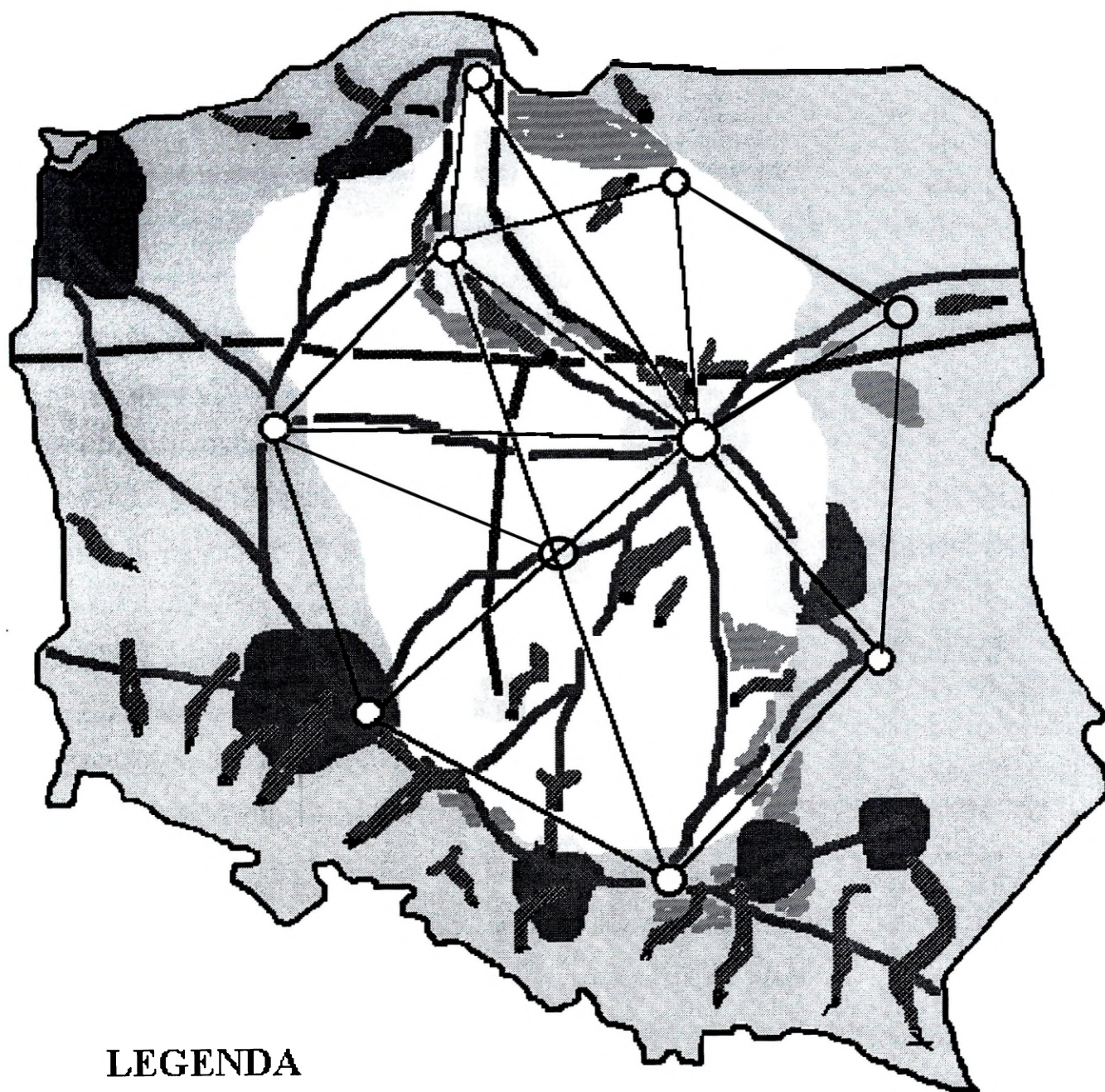
Mogą również zaistnieć inne klęski żywiołowe i katastrofy ekologiczne ale prawdopodobieństwo ich wystąpienia w Polsce jest znikome lub skutki zaistnienia pomijalnie małe.

2.2. Oddziaływanie celowe w czasie kryzysu i konfliktu zbrojnego

2.2.1. Niszczenie fizyczne

W czasie stałej gotowości obronnej państwa obce służby specjalne prowadzą ciągle rozpoznanie agenturalne i radioelektroniczne. Jego natężenie wzrośnie w czasie wyższych stanów gotowości obronnej. W początkowej fazie kryzysu może rozpocząć się niszczenie fizyczne. Największe prawdopodobieństwo zniszczeń wystąpi w rejonach: przemysłu zbrojeniowego, węzłów i ważnych tras komunikacyjnych, ośrodków administracyjnych, węzłów telekomunikacyjnych, zgrupowań sił obronnych itd. Oddziaływanie radioelektroniczne obejmie głównie najważniejsze dla systemu obronnego państwa węzły telekomunikacyjne oraz elementy łączności, rozpoznania i kierowania środkami walki sił zbrojnych.

Rejony największych prawdopodobnych zagrożeń w konfliktach lokalnych przedstawia rys. 2.



LEGENDA

-  - obszar zagrożeń konfliktami lokalnymi
-  - obszar zagrożony trującymi środkami przemysłowymi
-  - główne drogi przewozu środków trujących
-  - główne rurociągi
-  - zbiorniki wodne i obszar katastrofalnych zatopień
-  - obszary najczęściej nawiedzane przez powodzie

Rys. 6. Zestawienie miejsc występowania różnych typów zagrożeń z największym prawdopodobieństwem (stopień dokładności dla sieci warstwy krajowej)
 Podst; W. Pokruszyński i in.. „System bezpieczeństwa publicznego Polski”. AON, W-wa 1996 r.

2.2.2. Impuls elektromagnetyczny

Jednym z możliwych zagrożeń na wszelkie systemy wyposażone w technikę elektroniczną jest impuls elektromagnetyczny wybuchu jądrowego.

W wyniku wybuchu jądrowego powstaje promieniowanie gamma oraz rentgenowskie - X. Fale gamma oraz X powodują powstanie impulsowego pola elektromagnetycznego o bardzo dużych wartościach szczytowych, sięgających około 200 A/m dla pola magnetycznego i 50 - 60 kV/m dla pola elektrycznego. Największy zasięg tego typu zjawiska występuje przy wybuchu powietrznym na wysokości rzędu 100 km - impuls trwa około 500 ns.

W wyniku jego działania, w nawet krótkich odcinkach przewodników powstają napięcia o wartościach mogących powodować trwałe uszkodzenia elementów mikroelektronicznych. Napięcia takie powstają między innymi w:

- liniach transmisji sygnałów, napowietrznych, naziemnych i nawet podziemnych;
- przewodach ułożonych w obiektach stacjonarnych;
- antenach;
- przewodach zasilających;
- połączeniach między elementami elektronicznymi;
- konstrukcjach metalowych, instalacjach wodno - kanalizacyjnych, gazowych, grzewczych, uziemiających, zwłaszcza w zamkniętych pętlach.

Ścisłe określenie (przewidzenie) skutków jest trudne do określenia, zależne od wielu czynników tłumiących powodujących zmniejszenie zaindukowanego impulsu napięciowego.

Wiadomo jednak, że wspomniany już wybuch uszkodzi np. mikrokomputery niezabezpieczone, na odległość kilkuset kilometrów i więcej od epicentrum wybuchu. Dla przykładu wybuch jądrowy o sile 1 Mt na wysokości 100 km spowoduje trwałe uszkodzenia aparatury elektronicznej w promieniu do 1000 km i drobne w promieniu do 2000 km¹⁵.

2.2.3. Skutki oddziaływania radioelektronicznego

Skutki oddziaływania radioelektronicznego to rezultat prowadzenia Wre (w warunkach stosowania środków przez obie walczące strony) określony przez stosunek efektów tej walki do nakładów na jej prowadzenie.

1. ¹⁵ Bem J. „Impulsowe narażenia elektromagnetyczne”, Referat na Krajowym Sympozjum Telekomunikacji 93. ATiR Bydgoszcz, 1993 r:

$$E_f = \frac{E \text{ (efekty)}}{N \text{ (nakłady)}}$$

Jako nakłady rozumie się określone siły i środki oraz koszty wyszkolenia i przygotowania do prowadzenia działań.

Efekty bezpośrednie obezwładniania Re określa się następująco:

- wielkość utraty informacji przez dany środek (system);
- opóźnienie czasu przepływu informacji w środkach (systemach) transmisji informacji;
- wprowadzenie informacji dywersyjnej do środka (systemu) radioelektronicznego;
- ograniczenie zasięgu działania danego środka (systemu) radioelektronicznego;
- pogorszenie dokładności zbieranych informacji (działania środków).

Efektami pośrednimi obezwładniania Re możemy określić skutki, jakie wywołały efekty bezpośrednie w jego systemach i środkach walki, np. większe straty ludzi i sprzętu w wyniku braku informacji do podjęcia właściwej decyzji do działania wojsk.

Złożoność prowadzenia działań bojowych nie pozwala na precyzyjną ocenę możliwych skutków prowadzenia WRE i sprowadza się do określenia szacunkowego. Doświadczenia współczesnych wojen wskazują, że skutki te są znaczące, zależne w dużym stopniu od możliwości systemu obrony radioelektronicznej.

3. ZASADY PRZYGOTOWANIA OBRONNEGO SIECI TELEKOMUNIKACYJNEJ

Istotę przygotowania obronnego sieci jest zapewnienie pożądanego stopnia jej żywotności w warunkach oddziaływania środków walki przeciwnika. Zapewnienie pożądanego stopnia żywotności sieci osiąga się przede wszystkim w wyniku jej uodpornienia oraz przygotowania sił i środków do sprawnego odtwarzania zniszczonego potencjału łączności.

Uodpornienie sieci nie jest jednorazowym aktem, lecz musi być procesem ciągłym, realizowanym systematycznie w toku jej rozbudowy i rekonstrukcji. Precyzowanie perspektywicznego rozwoju telekomunikacji jest realizowane w następującym trybie:

- wyspecjalizowane organa resortu łączności określają rozwój sieci telekomunikacyjnej użytku publicznego przede wszystkim z punktu widzenia potrzeb okresu pokojowego / wewnątrz krajowych oraz wynikających ze współpracy

międzynarodowej / stosowanie do zakładanego rozwoju przestrzenno-gospodarczego państwa oraz

przewidywanego postępu naukowo-technicznego i produkcyjnego w dziedzinie sprzętu telekomunikacyjnego;

- wyspecjalizowane organa Sztabu Generalnego WP / Zarząd Wojsk Łączności i Informatyki/ na wyżej wymienioną prognozę nakładają telekomunikacyjne potrzeby obronne, zawarte w postulatach Sztabu Generalnego WP.

W oparciu o perspektywiczne prognozy rozwojowe opracowywane są plany rozwoju łączności, określone są zadania resortu łączności oraz wielkości nakładów finansowych. Nakłady na inwestycje postulowane przeznacza się na uodpornienie ogniw sieci łączności, zapewniając im pożądany stopień żywotności w warunkach przewidywanego oddziaływania przeciwnika. W niektórych przypadkach nakłady na inwestycje postulowane mogą być wykorzystywane do budowy linii łączności /szczególnego zainteresowania sił zbrojnych / w relacjach postulowanych przez Sztab Generalny WP.

Zazwyczaj z nakładów postulowanych budowane są uodpornione obsługiwane stacje wzmacniakowe wraz z wyposażeniem, kablowe opierścieniowanie miast, budynki techniczne o wzmocnionej konstrukcji itp. Uodpornienie wszystkich elementów składowych sieci ze względu na znaczne koszty jest zadaniem nierealnym. W związku z tym zachodzi potrzeba działania selektywnego, to jest uodporniania wybranych najważniejszych elementów składowych sieci. Analiza roli i znaczenia poszczególnych składowych sieci telekomunikacyjnej użytku publicznego wykazuje, że należy dążyć przede wszystkim do zachowania ciągłości działania dwóch składników sieci, tj. płaszczyzny międzymiastowej sieci pierwotnej (sieci stacjonarnej kablowej) uwzględniając, że w niej zawarty jest potencjał łączności dalekosieżnych oraz radiofonii ultrakrótkofalowej, uwzględniając że jest to środek masowego przekazu wiadomości najbardziej predestynowany do zachowania ciągłości emisji ze względu na możliwość zapewnienia (między innymi) awaryjnego zasilania.

W trakcie rozbudowy i rekonstrukcji sieci telekomunikacyjnej użytku publicznego, w ramach jej przygotowania do wykonania zadań w okresie wojny, stosuje się przede wszystkim uodpornienie : lokalizacyjne, punktowe, liniowe i eksploatacyjne.

3.1. Uodpornienia

3.1.1. Uodpornienia lokalizacyjne

Uodpornienie lokalizacyjne polega na kształtowaniu wielobocznej sieci łączności na terenie kraju, składającej się z co najmniej 4 - 5 równorzędnych magistral telekomunikacyjnych na kierunku „wschód - zachód” i podobnej ilości rękad „północ - południe”, przestrzennie między sobą oddalonych i powiązanych z zasadniczymi ośrodkami administracyjnymi państwa. Taka konfiguracja wielokanałowych linii kablowych i radiowych tworzy układ typu „siatka” lub „krata”, zapewniający wyższą żywotność sieci w porównaniu z układem gwieździstym.

Punkty przecięcia się magistral i rękad są zlokalizowane w rejonach dużych ośrodków administracyjnych, co umożliwia doprowadzenie do nich niezbędnej liczby łączy dalekosiężnych.

Dotychczas budowane węzły łączności w rejonach dużych miast składały się z podstawowej obsługiwanej stacji wzmacniakowej /OSW-P/ rozmieszczonej w centrum miasta oraz zastępczej /OSW-Z/ zlokalizowanej poza miastem. Od wymienionych węzłów, sprzęgających wysoko przepustowe linie łączności, rozchodziły się nisko przepustowe linie łączności, doprowadzające łączy międzymiastowe do układu wewnątrzstrefowego sieci pierwotnej. Ich rozbudowa kształtowana była w układzie wielobocznym lub mieszanym /gwiaździsto-wielobocznym/.

Przestrzenny podział węzłów oraz urządzeń teletransmisyjnych i komutacyjnych zapewniał w przypadku zniszczenia podstawowej OSW-P. /w centrum miasta/ możliwość zachowania ciągłości łączności na telestradach oraz minimum łączności w danym rejonie w wyniku wykorzystania zastępczej OSW-Z.

W związku z tym do podstawowej obsługiwanej stacji wzmacniakowej OSW-P doprowadzone były grupy pierwotne, wtórne lub trójne /lub pasma liniowe/ z poszczególnych kierunków przez OSW-Z tylko w ilościach przewidywanych do pracy w sieciach wtórnych z danego miasta /aglomeracji miejskiej/. Pozostały potencjał łączności na OSW-Z był tranzytowany pomiędzy poszczególnymi kierunkami łączności na wprost na poziomie pasm liniowych, grup trójnych, wtórnych i pierwotnych /w zależności od typu stosowanych linii i wyposażenia OSW-Z/. Ponadto na zastępczych OSW instalowało się minimalnie niezbędną ilość przemienników zakończeń kanałowych telefonii nośnej, urządzeń telegrafii wielokrotnej oraz zastępcze centrale telefoniczne i telegraficzne.

Za pomocą tych urządzeń w wypadku zniszczenia stacji podstawowej OSW-P na stacji zastępczej OSW-Z można było uruchomić minimum łączności w danym rejonie w granicach 10% potencjału łączy, doprowadzonych do centrum miasta.

Zastępcze obsługiwane stacje wzmacniakowe były lokalizowane poza strefami słabych zniszczeń tj. w następujących odległościach:

- 30 km i więcej od centrum miasta o stopniu zagrożenia I kategorii;
- 20 km i więcej od centrum miasta o stopniu zagrożenia II kategorii;
- 10 km i więcej od centrum miasta o stopniu zagrożenia III kategorii;
- co najmniej 5 km od obiektów o znaczeniu strategicznym / węzły komunikacyjne, zakłady produkcyjne, itp./.

Taka konfiguracja była przystosowana do istoty i możliwości wycofywanego już z użytku systemu analogowego i trudna już do ulepszenia, przy wzięciu pod uwagę rachunku kosztów i ryzyka.

Obecnie jest możliwy i wskazany, ze względu na rozśrodkowanie, podział dużych centrów komutacyjnych na mniejsze łącznice cyfrowe i sprzęganie ich traktami międzywęzłowymi na każdym poziomie sieci tj.: poziomie międzynarodowym, krajowym, wojewódzkim, lokalnym, miejskim. W zasadzie nie ma znaczenia dla jakości łączności ilość węzłów komutacyjnych, przez które jest realizowane połączenie. Można realizować trakty światłowodowe (odporne na szereg czynników oddziaływania zewnętrznego) o różnych przepływnościach, a drogi połączeń są wybierane automatycznie. W praktyce istnieje już w miastach rozproszona sieć komutacyjna, ale magistrale traktów często zbiegają się w jednym punkcie. Jest to co prawda okres przejściowy, metoda najtańsza, ale stanowi istotne zagrożenie, ze względu na możliwości oddziaływania punktowego. Kolejną zasadą powinno być połączenie każdego węzła komutacyjnego z innymi co najmniej dwoma traktami.

3.1.2. Uodpornienie punktowe

Uodpornienie punktowe polega przede wszystkim na zagłębianiu budynków technicznych /podziemne , półzagłębione / wzmacnianiu ich konstrukcji budowlanej stosownie do zakładanego nadciśnienia , hermetyzacji i zapewnieniu filtrowentylacji ,a także zapewnieniu ich pracy w warunkach pełnej izolacji od otoczenia zewnętrznego / w określonym limicie godzin lub dób/.

Uodpornienie punktowe obsługiwanych stacji wzmacniakowych instalowanych w mieście jest praktycznie nierealne. W celu zapewnienia ich żywotności w warunkach naziemnych uderzeń jądrowych dużej mocy należałoby budować budynki techniczne o specjalnej konstrukcji tj.:

- wytrzymującej nadciśnienie do 10 kg/cm^2 ,
- umożliwiające amortyzację efektu działania „fali sejsmicznej” wywołującej przyspieszenie o wartości 5-6 G (i więcej), powstającej w wyniku naziemnego uderzenia ładunkiem jądrowym dużej mocy.

Ze względu na ogromne koszty i materiałochłonność uodpornienia węzłów instalowanych w mieście oraz zmniejszenia obecnie prawdopodobieństwa użycia takiej broni, zabezpiecza się je tylko częściowo (wykorzystanie części podziemnej budynku o wzmocnionej konstrukcji). Uodpornienie punktowe metodą zagłębienia ułatwia też uodpornienie na impuls elektromagnetyczny, wyładowania atmosferyczne, ale nie może być stosowane w rejonie dużego zagrożenia zalaniem w wyniku katastrof, bądź klęsk żywiołowych.

Wyposażenie węzłów w autonomiczne agregaty zasilania uniezależnia sieć telekomunikacyjną od dostawy energii z wysoce wrażliwej na zniszczenia państwowej sieci energetycznej;

3.1.3 Uodpornienie liniowe

Uodpornienie liniowe ma na celu zapewnienie pożądanego stopnia żywotności dalekosiężnych linii kablowych. Ich zabezpieczenie osiąga się przez wybór odpowiedniej trasy przebiegu linii z uwzględnieniem budowy tych linii wzdłuż dróg drugorzędnych, wykonywanie rokad na przejściach rzecznych, omijanie w odpowiedniej odległości terenów miejskich i ważnych obiektów. Linie kablowe układane są na głębokości 1-1,2 m. Zabezpiecza się je przed uszkodzeniami mechanicznymi oraz wyładowaniami atmosferycznymi lub impulsem elektromagnetycznym (osiągane przez stosowanie osłony odgromowej kabla dzięki umieszczeniu przewodów odgromowych nad kablem w odległości 0,5m w odstępach 1 km dodatkowo uziemianych specjalnymi uziomami).

Stosowanie obecnie kabli światłowodowych w dużym stopniu uodparnia na celowe próby podsłuchu i uzyskania danych, bądź prowadzenia dywersji.

3.1.4 Uodpornienie eksploatacyjne

Uodpornienie eksploatacyjne stosuje się w całej sieci telekomunikacyjnej użytku publicznego i resortowych. Polega ono na zastępowaniu /w razie potrzeby/ działania danego elementu innym. Przykładowo, jeżeli zostanie uszkodzony trakt międzycentralowy to system zarządzania (utrzymania) sieci wybierze automatycznie inną drogę połączenia (pod warunkiem, że ona istnieje). Jeżeli takiej drogi nie będzie może być np. włączona rezerwowa linia radiowa. Zabezpieczenie żywotności wymienionych sieci osiąga się przez równoczesne stosowanie uodpornienia punktowego, eksploatacyjnego i lokalizacyjnego.

Ze względu na znaczne nasilenie w okresie wojny zniszczeń i awarii, drugim istotnym czynnikiem uodpornienia sieci telekomunikacyjnej jest przygotowanie sił i środków niezbędnych do odtworzenia unieruchomionych składników tej sieci. W tym celu w okresie zagrożenia, niezależnie od funkcjonujących w okresie pokojowym służb eksploatacyjnych, formuje się zmilitaryzowane oddziały odbudowy łączności, które stanowią odwód kierownictwa resortu łączności centralnej dyspozycji, przeznaczony do odtwarzania zniszczonych fragmentów sieci, najbardziej niezbędnych do kierowania państwem, kierowania jego obroną oraz utrzymania bezpieczeństwa publicznego.

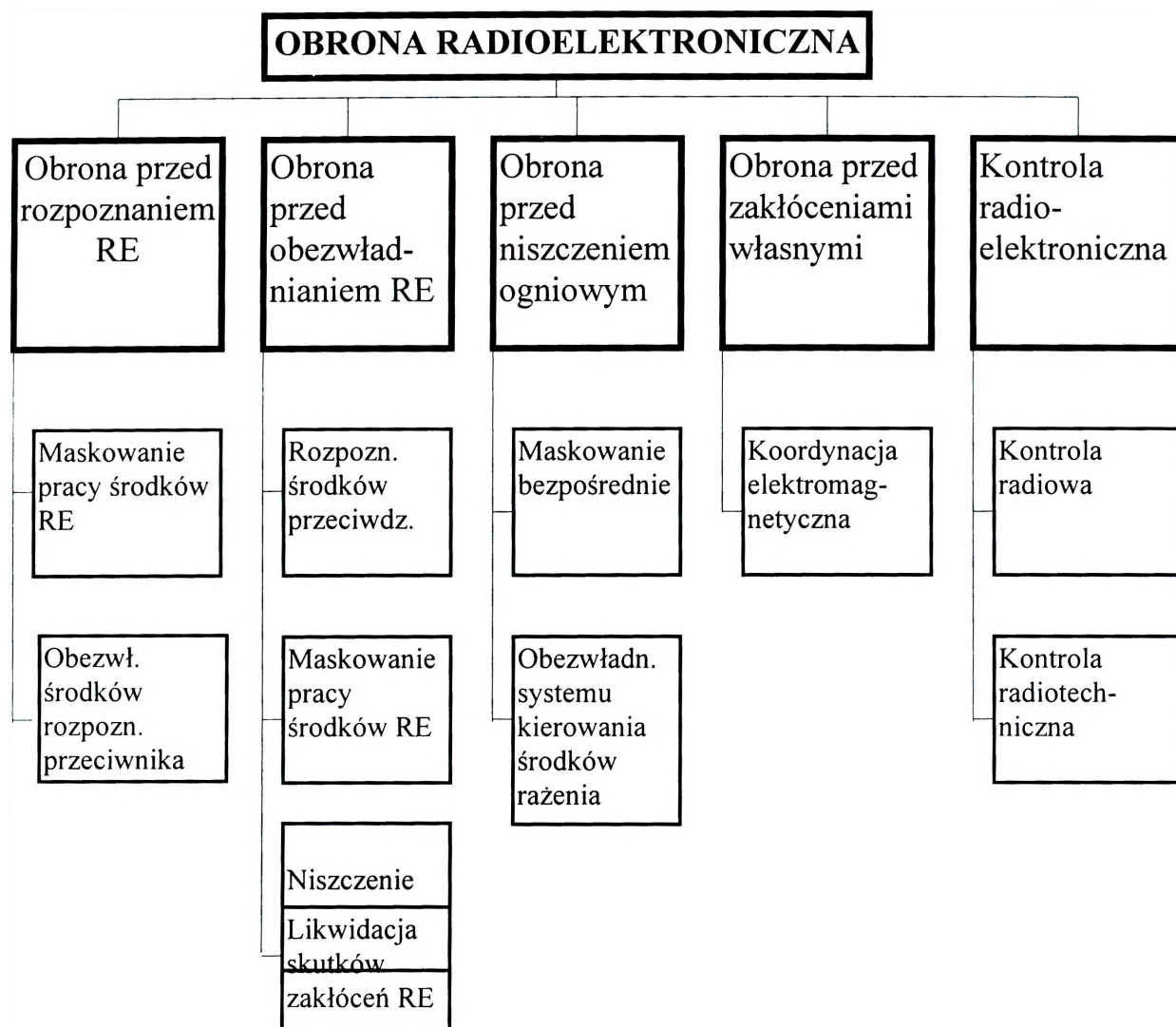
Zmilitaryzowane oddziały odbudowy łączności wyposaża się w środki będące w posiadaniu przedsiębiorstw w okresie pokoju oraz w urządzenia i materiały łączności gromadzone sukcesywnie przez resort łączności w ramach rezerw państwowych (kable, urządzenia teletransmisyjne i komutacyjne, przewoźne urządzenia łączności np.: linie radiowe zapasowe stacjonarne oraz mobilne, stacje radiowe, centrale telefoniczne, inny sprzęt oraz części zapasowe).

Przedstawione zasady przygotowania obronnego sieci telekomunikacyjnej nie wyczerpują wszystkich możliwości, a naświetlają tylko główne kierunki jej uodpornienia.

3.1.5 Uodpornienie na oddziaływanie radioelektroniczne

Na stopień uodpornienia mają wpływ następujące czynniki:

- procent elementów systemu łączności wykorzystujących fale radiowe,
- procent środków radiowych pracujących w rozproszonym widmie,
- stosowanie zabiegów uodpornienia na rozpoznanie i odporności na zakłócenia środków radiowych;



Rys. 7. Podział funkcjonalny obrony radioelektronicznej

Tabela 6.

Formy i sposoby maskowania radioelektronicznego

FORMY	MASKOWANIE BEZPOŚREDNIE	POZOROWANIE RADIOELEKTRONICZNE	DEZINFORMO- WANIE
sposoby	optyczne	tworzenie obiektów pozornych	wykorzystanie specjalnych
	radiowe	tworzenie pozornej sytuacji radioelektronicznej	kanałów informacji
	radiolokacyjne		wykorzystanie technicznych
	cieplne i świetlne	działania bojowe pododdziałów (oddziałów) wydzielonych	środków łączości
	akustyczne		wykorzystanie telewizji
	hydroakustyczne		
	rozśrodkowanie i zmiana rejonów		
	wypełnianie regulaminów pracy środków radioelektronicznych		

- wykorzystywanie linii radiowych jako zapasowych;
- aktywne stosowanie środków przeciwdziałania radioelektronicznego, obrona radioelektroniczna (rys. 7) i maskowanie radioelektroniczne (rys. 8).

3.2. Bezpieczeństwo informacji

W systemach informatycznych i łączności do niepożądanych zagrożeń zalicza się, między innymi, problemy bezpieczeństwa transmitowanej i przetwarzanej informacji.

Problemy te wynikają ze specyficznej i skomplikowanej budowy urządzeń łączności i informatyki, opartej na układach elektronicznych oraz z niepożądanego nadprodukcji przez każde urządzenie informatyczne i telekomunikacyjne energii emitowanej dookoła w eterze, oraz w liniach i kablach, która stanowi (oprócz emisji głównej - użytkowej) źródło wytwarzania i promieniowania emisji elektromagnetycznej ubocznej (szkodliwej - zwanej ujawniającą), niosącej w sobie część lub całość informacji użytkowej. Oznacza to tworzenie realnych możliwości do penetrowania naszych systemów przez wysoce wyspecjalizowane i wykwalifikowane służby wywiadowcze i to ze znacznych odległości, dochodzących nawet do kilku kilometrów, mające w swojej dyspozycji najnowocześniejsze środki i metody rozpoznania. Zagrożenia są tym większe, że w ostatnich latach w Polsce rozpoczyna się „rewolucja informacyjna” i pierwsze działania w tym zakresie to zakup sprzętu informatycznego z niesprawdzonych źródeł, korzystanie z niesprawdzonych programów, kolejne kroki to tworzenie źle zabezpieczonych sieci lokalnych a nawet rozległych. Wiele organizacji przetwarza na takim sprzęcie informacje stanowiące tajemnice firm lub państwowe.

Tworzy się więc obecnie w Polsce nowa gałąź wiedzy dotyczącej ochrony informacji w systemach telekomunikacyjnych i informatycznych. Jest to dziedzina dążąca do opracowania teorii kompleksowej ochrony informacji oraz praktycznych rozwiązań organizacyjno-technicznych, najlepiej opracowanych na bazie rozwiązań polskich.

Problemy bezpieczeństwa łączności i ochrony informacji wiążą się ściśle z bezpieczeństwem narodowym, dlatego w państwach wysoko rozwiniętych celem uniknięcia niekontrolowanego wykorzystania skutków powszechnej automatyzacji objęto je specjalnymi programami rządowymi. Zajmują się one wyłącznie

opracowywaniem i zastosowaniem nowoczesnych środków łączności i metod ochrony informacji oraz zachowania jej w ścisłej tajemnicy (w Stanach Zjednoczonych program rządowy „TEMPEST”).

Zadaniem systemu bezpieczeństwa i ochrony informacji w systemach telekomunikacyjnych i informatycznych jest zapewnienie¹⁶:

- poufności, tj. udostępnianie danych niejawnych tylko osobom uprawnionym;
- integralności, tj. ochrony systemu przed wprowadzaniem nieuprawnionych zmian;
- dostępności, tj. dostarczenia usług informacyjnych w wymaganym miejscu i czasie;
- zabezpieczenie przed dekonspiracją:

wymagania dodatkowe:

- rozliczalność, tj. możliwość ustalenia wszystkich zdarzeń, które zaistniały w systemie;
- kontrolowalność, tj. możliwość sprawdzenia czy w systemie są przestrzegane ustalone procedury zabezpieczeń.

3.2.1. Ochrona informacji (bezpieczeństwo łączności)

BEZPIECZEŃSTWO ŁĄCZNOŚCI (termin używany w siłach zbrojnych) lub polityka ochrony informacji (termin zaczerpnięty z literatury zachodniej) jest to całokształt działalności zmierzającej do uodpornienia systemu łączności na przypadkowe lub celowe nieuprawnione oddziaływanie mogące doprowadzić do:

- ujawnienia informacji niejawnej, przetwarzanej przy pomocy systemów informatycznych i przesyłanej za pomocą technicznych środków łączności;
- modyfikacji parametrów funkcjonalnych systemu;
- modyfikacji lub zniszczenia informacji podlegających ochronie;
- wprowadzenia do systemu fałszywych informacji (danych);
- ponadto w siłach zbrojnych do rozpoznania lokalizacji węzłów i linii.

Odporność systemu z punktu widzenia bezpieczeństwa łączności osiąga się przez kompleksowe zastosowanie technicznych, programowych, kryptograficznych i organizacyjnych (w tym personalnych) metod ochrony¹⁷.

¹⁶ Na podstawie opracowań literatury zachodniej m.in. Data Security Letter Nr 71, May 1996.

Celem bezpieczeństwa łączności jest stworzenie jednolitego, gwarantowanego systemu ochrony informacji i nadzoru, a przez to zapewnienie skrytości transmisji i tajności przetwarzania informacji niejawnej w systemach łączności i informatycznych, oraz zachowania jej integralności (zabezpieczenie przed dezinformacją), a także przywrócenie jej właściwej roli po awariach i dekonspiracji.

Zastosowanie odpowiednich środków i metod uwarunkowane jest przeprowadzeniem odpowiednich analiz i ocen z punktu widzenia zagrożeń i ryzyka.

Zintegrowane i zautomatyzowane podsystemy łączności nowej generacji wymagają zaprojektowania i budowy nowych jakościowo urządzeń szyfrujących, utajniających i zabezpieczeń takich jak programowe, techniczne itp. oraz redukcji emisji ujawniającej. Zwłaszcza zautomatyzowane systemy dowodzenia oraz systemy informatyczne narzucają ostre wymagania co do budowy urządzeń i pozostałych systemów ochrony zapewniających gwarantowaną moc ochronną i minimalny zasięg szkodliwej działalności emisji ujawniającej.

Przy wyborze mechanizmów ochrony informacji w systemach łączności i informatycznym systemie łączności należy przyjąć, że **informacja powinna być chroniona od momentu jej powstania do czasu wykorzystania i celowego jej zniszczenia**. Zapewnienia bezpieczeństwa informacjom przetwarzanym, przesyłanym i przechowywanym w systemach łączności i informatycznych niezbędne jest stworzenie jednolitego, spójnego i szczelnego systemu bezpieczeństwa informacji.

Metody ochrony informacji można podzielić na cztery grupy:

- techniczne;
- programowe;
- kryptograficzne;
- organizacyjne.

Żadna z wymienionych metod nie występuje w czystej postaci. Najczęściej metody lub ich elementy są łączone, wówczas mamy do czynienia z kompleksowym systemem ochrony.

¹⁷ W siłach zbrojnych zasady postępowania w celu zachowania bezpieczeństwa informacji określają między innymi instrukcje [1,2,3,...]

3.2.2. Metody techniczne

Metody techniczne to pewien układ techniczny i określony sposób postępowania. Mają one zabezpieczyć zbiory przed infiltracją lub sam sprzęt informatyczny lub łącznościowy przed uszkodzeniem. Dlatego przez układ techniczny rozumiemy takie urządzenie, które chroni przed dostępem osób nie upoważnionych, wykrywa przypadki zagrożenia zbiorów lub pomieszczeń.

Zabezpieczenie fizyczne:

- kontrola wstępu do pomieszczeń;
- kontrola dostępu do terminali;
- kontrola dostępu do zbiorów i nośników oprogramowania systemowego
- zabezpieczenie instalacji przed klęskami żywiołowymi;
- zapewnienie niezawodności źródeł energii elektrycznej i klimatyzacji;
- kontrola dostępu personelu nadzorującego do zastrzeżonych obszarów systemu;
- stosowanie orurowań do okablowania sieci informatycznych i abonenckich sieci łączności utajnionej.
- stosowanie urządzeń szyfrujących i deszyfrujących;
- stosowanie wymiennych dysków HDD.

Zabezpieczenie w zakresie redukcji emisji ujawniającej:

- stosowanie urządzeń w specjalnym wykonaniu charakteryzujących się obniżonym poziomem emisji ujawniającej;
- stosowanie filtrów i transformatorów separujących;
- stosowanie odrębnych uziomów dla obiektów i urządzeń specjalnych;
- stosowanie osłon i kabin ekranujących;
- stosowanie ekranowania pomieszczeń;
- stosowanie łączy światłowodowych;
- stosowanie stref kontrolowanych.

3.2.3. Metody programowe

Spośród wszystkich metod ochrony zbiorów metody programowe posiadają szereg zalet. Do głównych należą:

- możliwość zaprogramowania i wdrożenia własnymi siłami w poszczególnych ośrodkach;
- różne możliwości stosowania szyfrów, kodów, identyfikatorów, systemów kontroli, itp;
- nie komplikowanie procesu przetwarzania danych;
- duże prawdopodobieństwo ochrony.

Programowe metody ochrony zbiorów są na pewnych etapach procesu przetwarzania jedynymi metodami, które mogą skutecznie chronić zbiory informacji.

Można wyróżnić dwie główne metody ochrony zbiorów informacji.

1. Ochrona dostępu do sprzętu informatycznego, w której wyróżniamy:

- identyfikację i hasła dostępu (każdy użytkownik posiada przydzielony identyfikator wraz z hasłem bez którego nie może rozpocząć pracy w systemie);
- ograniczenie dostępu do danych (właściciel danych ogranicza dostęp do nich innym użytkownikom);
- monitorowanie pracy w czasie sesji użytkownika (pozwala na odtworzenie wszystkich poleceń dla systemu, a w tym wykrycie rozkazu niewłaściwie wydanego lub użytego), systemowe jądro ochrony - ewidencja zdarzeń w systemie;
- hierarchiczny dostęp do danych (ustalenie wielu szczebli uprawnień dostępu, z których użytkownicy o wyższym statusie uprawnień mają nieograniczoną możliwość ingerencji w dane użytkowników o niższym statusie);
- zabezpieczenie indywidualne (specjalistyczne oprogramowanie).

2 Ochrona systemowa, która stawia następujące wymagania:

- programy użytkowników powinny być kodowane;
- adresy przesyłane pomiędzy użytkownikami powinny być adresami logicznymi, rzeczywiste adresy nie mogą być akceptowane.
- dane powinny być przechowywane w postaci zaszyfrowanej;

3.2.4. Metody kryptograficzne

Metody kryptograficzne chronią przed przeglądaniem i podsłuchiwaniami, czyniąc informację niezrozumiałą. Takie metody mogą uzupełniać kontrolę dostępu. Należy jednak pamiętać, że metody kryptograficzne nie chronią informacji w czasie ich przetwarzania.

Metody kryptograficzne wykorzystujemy do:

- automatycznego szyfrowania informacji przesyłanych kanałami łączności między obiektami sieci informatycznej;
- ochrony informacji przechowywanych w bazach (zbiorach) danych;
- zachowania integralności przesyłanych i przechowywanych danych;
- uwierzytelnienia (identyfikacji) obiektów systemu informatycznego oraz ich użytkowników;
- maskowania ruchu (maskowania trafiku);
- uwierzytelniania podpisu cyfrowego.

3.2.5. Metody organizacyjne

Zadaniem metod organizacyjnych jest stworzenie podstaw organizacyjno-prawnych dla tworzenia kompleksowego systemu ochrony.

Regulacje prawne w zakresie:

- ochrony systemów łączności i informatycznych, wiadomości przetwarzanych i przesyłanych w tych systemach;
- wprowadzania do eksploatacji atestowanego oprogramowania oraz sprzętu informatycznego i łączności;
- wydawanie przepisów organizacyjnych dotyczących funkcjonowania służb bezpieczeństwa łączności i ochrony informacji w tych systemach:
 - opracowanie zadań i obowiązków poszczególnych osób funkcyjnych;
 - opracowanie procedur doboru i postępowania poszczególnych osób funkcyjnych oraz zasad zmiany ich uprawnień;
- opracowanie wymogów związanych z rozwijaniem i projektowaniem sieci teletransmisyjnej, abonenckiej i informatycznej.

- Wydanie norm w zakresie bezpieczeństwa łączności i ochrony informacji w tych systemach, dotyczących organizacji:
 - ochrony fizycznej;
 - ochrony programowej;
 - ochrony kryptograficznej;
 - redukcji emisji ujawniającej.
- Opracowanie procedur i algorytmów:
 - odtwarzania systemu po awariach i dekonspiracji;
 - składowanie i archiwizacja danych.
- Zabezpieczenie personalne:
 - właściwy system doboru kadr: zgodny z określoną procedurą z wymaganymi i posiadanymi kwalifikacjami i z określonymi oraz posiadanymi cechami charakterologicznymi.
 - stabilność kadr poprzez prowadzenie właściwej polityki personalnej;
 - wysoki poziom szkolenia w ramach kursów organizowanych w ośrodkach oraz wewnętrznego szkolenia doskonalącego kadry w oparciu o systematycznie aktualizowane programy szkolenia w miarę rozwoju i postępu technicznego;
 - okresowe sprawdzanie umiejętności i bieżące egzekwowanie wysokiego poziomu umiejętności fachowych.

BIBLIOGRAFIA

1. Analiza systemów dostępu radiowego. WAT, czerwiec 1996r.
2. Balcerowicz B., Strategiczna obrona Rzeczypospolitej Polskiej lat dziewięćdziesiątych. AON, Warszawa 1993r.
3. Bem J. „Impulsowe narażenia elektromagnetyczne” , Referat na Krajowym Sympozjum Telekomunikacji 93. ATiR Bydgoszcz, 1993 r:
4. Brzeziński S., Cajbel K., Chomicki W., Tadeusiak Z., Koncepcja realizacji zadań obronnych w dziedzinie łączności, MŁ, Warszawa 1997r.
5. Dąbrowski A., Kula S., Systemy i sieci SDH, WKiŁ, Warszawa 1996r.
6. Dziennik Ustaw Rzeczypospolitej Polskiej Nr 94, Warszawa 1996r.
7. Gawlikowski W. Zagrożenia systemu telekomunikacyjnego w czasie pokoju, kryzysu i wojny. Zeszyty Naukowe nr 3/97. AON 1997.
8. Handel R., Rozwój sieci opartych na wykorzystaniu techniki ATM, PT nr 2/96.
9. Jemioło T., Koziej S., Sienkiewicz P., Wystarczalność obronna, Bellona, Warszawa 1996r.
10. Kompendium łączności cywilnej, Komisja Planowania Łączności cywilnej, NATO 1995r.
11. Konstytucja Rzeczypospolitej Polskiej, Warszawa 1997r.
12. Kościelnik A., ISDN cyfrowe sieci zintegrowane usługowo, WKiŁ, Warszawa 1996.
13. Koziej S., „Kierowanie obronnością państwa”. DSO MON, Warszawa 1996r.
14. Koziej S., Wołkowicz „Podstawowe założenia obronności Rzeczypospolitej Polskiej”. AON, Warszawa 1995 r.
15. Krauze M., Wojskowe aspekty współczesnych zagrożeń ekologicznych. ZN nr 1/90, AON, Warszawa 1990r.
16. Kulczycki R., Piedziuk E., Wojnarowski J. Praca n-b „Model systemu obronnego państwa. AON, W-wa 1994 r.
17. Laszczkowski Cz., „Kształtowanie bezpieczeństwa narodowego RP” BBN, W-wa 1993 r.
18. Latek J., Jaroszyński M., Systemy łączności i taktyka ich użycia w wojnie nad Zatoką Perską, Wiadomości telekomunikacyjne, Warszawa 1992r.
19. Magnucki Z., Scheffs W., Charakterystyka struktur organizacyjnych i środków walki radioelektronicznej w wybranych państwach. AON, Warszawa 1996r.

20. Marczak J., Dworecki S., Piedziuk E., Duda W., Operacyjne przygotowanie obszaru kraju do obrony. Wiedza Obronna nr 2/181/, Warszawa 1997 r.
21. Materiały z konferencji naukowej, Systemy łączności na potrzeby obrony i bezpieczeństwa RP, WSOWŁ, Zegrze 1992 - 1996r.
22. Metody oceny efektywności systemów łączności na potrzeby obronności państwa pk. WENA-1, CZ 1 - 4 oraz słownik pojęć. AON, Warszawa 1996.
23. Naczelny Komitet ds. Planowania Zagrożeń Cywilnych NATO, SCEPC-struktura i cele, Materiały NATO, Bruksela 1996r.
24. Ochrona informacji w systemach telekomunikacyjnych. Materiały III Szkoły Ochrony Informacji. IŁ, Pułtusk 1997.
25. Pach A., Lasoń K., Współpraca sieci ATM z innymi systemami telekomunikacyjnymi, WFPT, Kraków 1995.
26. Pawłowski J., Marczak J., O obronie militarnej Polski przełomu XX-XXIw., Bellona, Warszawa 1995r.
27. Perspektywiczny model systemu obronnego RP. Kierunki, Moduł kierowania. Moduł dowodzenia SZ RP, AON, Warszawa 1992r.
28. Piedziuk E., System telekomunikacyjny państwa i jego wykorzystanie przez wojska operacyjne, Materiał studyjny, AON, Warszawa 1993r.
29. Podstawowe założenia polityki obronnej i strategii obronności. Struktura, zadania i funkcjonowanie systemu obronnego państwa w czasie pokoju oraz zagrożeń i wojny. Praca zbiorowa. DSO MON, Warszawa 1994r.
30. Pokruszyński i in. System bezpieczeństwa publicznego Polski. AON, W-wa 1996 r.
31. Praca zbiorowa, Strategia rozwoju telekomunikacji Rzeczypospolitej Polskiej do roku 2000, MŁ, Praca niepublikowana, Warszawa 1997r.
32. Praca zbiorowa, Strategia rozwoju telekomunikacji w Rzeczypospolitej Polskiej do roku 2000, MŁ, Warszawa 1993r.
33. Przepisy o ochronie tajemnicy w siłach zbrojnych RP. Cz. V. Przekazywanie wiadomości przez techniczne środki łączności. Szt. Gen. 763/76.
34. Rączkiewicz M., Bezpieczeństwo sieci komputerowych. WFPT, Kraków 1995.
35. Robling E., Denning D., Kryptografia i ochrona danych. WNT, Warszawa 1993.
36. Rozporządzenie Rady Ministrów w sprawie szczegółowych zadań MON, Warszawa 1996r.

37. Schatt S., Zrozumieć sieci lokalne, Intersoftland, Warszawa 1994r.
38. Sieci z komutacją pakietów od X.25 do Frame Relay i ATM pod red. Z. Papira, WFPT, Kraków 1995.
39. Sienkiewicz P., Stańczuk S., Flanek Cz. i inni, Metody oceny efektywności systemów łączności na potrzeby obronności Państwa, AON, Warszawa 1995r.
40. Skład i struktura systemu obronnego Rzeczypospolitej Polskiej oraz zadania realizowane przez jego główne elementy. Praca zbiorowa. DSO MON, Warszawa 1993r.
41. Sowa M., Zagrożenia piorunowe urządzeń elektronicznych. Referat na Krajowym Sympozjum Telekomunikacji 93. ATiR Bydgoszcz, 1993 r:
42. Standarization Agreement STANAG 1008. MAS 1994
43. Steibrink B., Multimedia u progu technologii XXI wieku. Robomatic, Wrocław 1993
44. Syc C., Metodyka projektowania sieci telekomunikacyjnych, WKiŁ, Warszawa 1997r.
45. Systemy i sieci SDH, red. A. Dąbrowski i S. Kula, WKiŁ, Warszawa 1996.
46. Telecom forum 7/8 96
47. Telekomunikacja w Polsce - stan, inwestycje, perspektywy. Raport Teleinfo - wrzesień 1997.
48. Ungerer H., Telekomunikacja w Europie, MŁ, Warszawa 1992r.
49. Urządzenia i systemy łączności na potrzeby kierowania obronnością i bezpieczeństwem państwa. AON, Warszawa 1996
50. Ustawa z dnia 14 grudnia 1995r. o urzędzie Ministra Obrony Narodowej.
51. Walka radioelektroniczna w Siłach Zbrojnych RP. AON, W-wa 1997.
52. Warsztaty Instytutu Łączności Postępy Telekomunikacji i Informatyki, Materiały. Podstawy szerokopasmowych sieci telekomunikacyjnych BISDN. Warszawa - Miedzeszyn 12/13 marca 1997.
53. Wojciechowski W., Kierowanie i strategiczne dowodzenie w systemie obronnym państwa /Infrastruktura telekomunikacyjna/, Rozprawa doktorska, AON, Warszawa 1993r.
54. Zagrobelny T., Dąbrowski A., Rozwój SDH w Polsce oraz problemy jej synchronizacji, IX KSO Gdańsk-Sobieszewo 1995r.