AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

ORGANIZACJA ŁĄCZNOŚCI DLA POTRZEB KIEROWANIA REAGOWANIEM KRYZYSOWYM NA OBSZARZE KRAJU

pk. „ŁĄCZ-KRYZ"

WARSZAWA 2004

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH

INSTYTUT ZARZĄDZANIA I DOWODZENIA

ORGANIZACJA ŁĄCZNOŚCI DLA POTRZEB KIEROWANIA REAGOWANIEM KRYZYSOWYM NA OBSZARZE KRAJU

Pk. „ŁĄCZ-KRYZ"

Praca naukowo - badawcza

Warszawa 2004

SPIS TREŚCI

Recenzent:

- **płk prof. dr hab. Adam TOMASZEWSKI**

Opracował zespół autorski w składzie:

• **płk dr hab. inż. Józef MICHNIAK**	**kierownik naukowy** - wstęp - rozdz. 1 - rozdz. 2 - rozdz. 3 - zakończenie
• **ppłk dr inż. Zbigniew FIOŁNA**	- rozdz. 4 - rozdz. 5
• sierż. szt. mgr Dariusz GOŁAWSKI	sekretarz zespołu - skład komputerowy - redakcja techniczna - korekta - druk

Okładka i oprawa: Akademia Obrony Narodowej – Wydział Wydawniczy
00-910 Warszawa, Al. Gen. A. Chruściela 103, tel.681-40-55, tel./faks 681-37-52

WSTĘP

płk dr hab. inż. Józef Władysław MICHNIAK

Wieloletnie dążenia Polski do pełnej integracji ze strukturami NATO zostały uwieńczone pełnoprawnym członkostwem w tym Sojuszu. Jest to niewątpliwie jedno z najważniejszych wydarzeń w dziejach najnowszej historii naszego państwa i które wywiera istotny wpływ na zmiany w sztuce wojennej, która musi być obecnie postrzegana nie tylko w kategoriach narodowych, ale przede wszystkim w sojuszniczych. Zmiany te w stosownym zakresie dotyczą również organizacji łączności dla potrzeb kierowania (dowodzenia, zarządzania) reagowaniem kryzysowym na obszarze kraju.

Koncepcja metodologiczna niniejszej pracy ma charakter złożony. Zakres problemowy pracy obejmuje funkcjonowanie państwa w sytuacji kryzysowej oraz system kierowania obronnością, a w tym system kierowania reagowaniem kryzysowym z użyciem wojsk wraz z przewidywanymi relacjami informacyjnymi w tym systemie. Informacje aby mogły być wykorzystane w procesie kierowania (dowodzenia, zarządzania) oprócz tego, że muszą mieć nadawcę i odbiorcę, to muszą być jeszcze do nich i od nich przesłane. We współczesnej dobie problem ten rozwiązują dobrze zorganizowane środki i urządzenia łączności i informatyki. Kierowanie reagowaniem kryzysowym, aby mogło być realizowane musi posiadać określoną bazę materialną, ogólne zasady działania i stałe procedury operacyjne. Dlatego też w tym celu organizuje się s y s t e m k i e r o w a n i a. Przedmiotem badań musiał być, zatem obecny stan teorii kierowania reagowaniem kryzysowym, uwarunkowania funkcjonowania systemu kierowania reagowaniem kryzysowym i nasze zobowiązania sojusznicze oraz zadania w wymiarze narodowym i koalicyjnym.

Dlatego w odniesieniu do będącej przedmiotem zainteresowania naukowego organizacji łączności dla potrzeb kierowania reagowaniem kryzysowym na obszarze kraju zaistniała potrzeba porządkowania wiedzy o możliwościach organizacji systemu łączności z wykorzystaniem nowoczesnego potencjału telekomunikacyjnego znajdującego się na terytorium kraju.

Założono, że opracowanie pisarskie pracy ma stanowić sumę wniosków uzyskanych w wyniku zastosowania różnorodnych metod badawczych. Już początkowe prace wykazały istnienie szeregu luk w istniejącej wiedzy w zakresie stanowiącym obszar zainteresowania zespołu autorskiego. W konsekwencji ujawniła się sytuacja problemowa, dając początek

pierwszemu dosyć ograniczonemu etapowi procesu badań naukowych ze względu na szczupłość zespołu i ograniczone środki finansowe oraz czas.

Bazując na wytycznych zawartych w treści zadania, dotychczasowej wiedzy oraz wynikach badań wstępnych za **cel główny pracy** przyjęto: **„identyfikację zasad funkcjonowania i zadań wykonywanych przez organa w systemie kierowania reagowaniem kryzysowym, określenie zasadniczych więzi informacyjnych oraz przedstawienie koncepcji organizacji łączności dla potrzeb kierowania reagowaniem kryzysowym na bazie potencjału telekomunikacyjnego kraju".**

Tak sformułowany cel główny determinował określenie szeregu celów cząstkowych, mających umożliwić jego osiągnięcie. Cele te sprecyzowane zostały następująco:

1. ***Zidentyfikować zasady funkcjonowania i zadania wykonywane przez organa kierowania reagowaniem kryzysowym w systemie kierowania reagowaniem kryzysowym;***
2. ***Wypracować dane o podstawowych relacjach informacyjnych funkcjonujących w systemie reagowania kryzysowego;***
3. ***Zidentyfikować organizację i podsystemy funkcjonalne systemu łączności kraju wraz z możliwościami świadczenia przez nie usług na rzecz organów kierowania reagowaniem kryzysowym;***
4. ***Dokonać identyfikacji środków i systemów technicznych, które mogą być wykorzystane w koncepcji organizacji łączności dla potrzeb kierowania reagowaniem kryzysowym na obszarze kraju.***

Już w trakcie badań wstępnych (zgodnie z przyjętą procedurą badawczą[1]) autorzy pracy określili sytuację kryzysową i funkcjonowanie w niej państwa oraz wypracowali pogląd na strukturę organizacyjną systemu kierowania reagowaniem kryzysowym, w którym stanowiąca przedmiot rozważań organizacja łączności znaleźć mogłaby swoje zastosowanie.

W toku dalszej pracy, dążąc do osiągnięcia zakreślonych wcześniej celów, autorzy sformułowali problem badawczy w postaci pytania:

Jaką łączność i w jakiej postaci organizacyjno-sprzętowej powinno posiadać kierownictwo i organa reagowania kryzysowego niezbędną do sprawnego przebiegu procesu kierowania reagowaniem kryzysowym MON (porównaj problem etapu II w treści zadania 3.36.0.0)?

---

[1] **Procedura** to „(...) unormowany przepisami, zwyczajami sposób prowadzenia, załatwienia jakiejś sprawy, tok, tryb, przebieg czegoś". *Słownik języka polskiego, Warszawa, PWN 1993, s. 65.*

Kolejny, drugi etap badań, będący w swej istocie etapem badań porównawczych, stanowił w głównej mierze ciąg analiz, porównań i analogii oraz dalsze, dogłębne studiowanie dostępnej literatury przedmiotu. W konsekwencji tych badań autorzy utwierdzili się w przekonaniu o konieczności podziału głównego problemu naukowego na kilka mniejszych, ograniczonych w zakresie rozpatrywanych zagadnień. W ten sposób zostały zidentyfikowane i wyodrębnione następujące problemy szczegółowe:

1. ***Jak struktura systemu kierowania reagowaniem kryzysowym wpływa na ilość i rodzaj relacji informacyjnych w tym systemie?***
2. ***Jakie są podstawowe relacje informacyjne w systemie reagowania kryzysowego?***
3. ***Jaka jest organizacja i jakie są możliwości krajowego systemu łączności?***
4. ***Jakie środki i systemy techniczne operatorów telekomunikacyjnych oraz na jakich zasadach prawnych można wykorzystać do zabezpieczenia łączności na potrzeby kierowania reagowaniem kryzysowym na obszarze kraju?***

Rezultaty dalszych studiów literatury przedmiotu oraz wnioski z doświadczeń będących konsekwencją udziału w ćwiczeniach ze strukturami reagowania kryzysowego stanowiły podstawę sformułowania **hipotezy**.

Bazując na posiadanej wiedzy oraz wynikach poprzedniego etapu badań, autorzy założyli, że: ***„Do organizacji łączności na potrzeby kierowania reagowaniem kryzysowym, oprócz etatowych mobilnych środków i urządzeń łączności wojskowych zgrupowań antykryzysowych, można i należy wykorzystywać potencjał telekomunikacyjny operatorów funkcjonujących na obszarze kraju. Środki łączności przydatne i możliwe do wykorzystania w tym systemie występują na obszarze całego kraju i są coraz nowocześniejsze ale aby mogły spełniać przypisywaną im rolę należy je zidentyfikować i opisać”.***

W trzecim etapie badań autorzy zastosowali szereg metod badawczych prowadzących do rozwiązania określonych uprzednio problemów szczegółowych.

Specyfika zidentyfikowanych problemów badawczych rzutowała bezpośrednio na fakt, iż wśród użytych metod znalazły się zarówno metody teoretyczne, jak i empiryczne.

Zastosowane metody teoretyczne to: analiza, synteza, wnioskowanie, porównanie, analogia oraz uogólnienie.

Analiza zastosowana została w głównej mierze do badań literatury dotyczącej problematyki funkcjonowania państwa w sytuacji kryzysowej, jak i organizacji systemu kierowania reagowaniem kryzysowym, w celu identyfikacji obecnych ustaleń i możliwych kierunków zmian w rozpatrywanym obszarze.

Syntezie poddane zostały wnioski z badań teoretycznych i empirycznych, porównywane następnie z przyjętymi założeniami.

W wydobywaniu podobieństw i różnic w rozwiązaniach z zakresu organizacji łączności w różnych państwach członkowskich NATO szczególnie pomocne było **porównanie**.

Poszukiwanie podobieństw badanych uwarunkowań organizacji łączności na potrzeby kierowania reagowaniem kryzysowym ułatwione zostało przez zastosowanie metody **wnioskowania**. Specyfika materiału badawczego jednoznacznie wskazywała na konieczność stosowania takiego schematu wnioskowania, w którym prawdziwość przesłanek nie przesądzała o prawdziwości wniosku. Stąd też, uwzględniając takie kryterium, zastosowanie znalazło przede wszystkim **wnioskowanie zawodne**.

Z kolei, biorąc pod uwagę kryteria rodzaju zdań stanowiących przesłanki oraz zdań będących konkluzjami, wnioskowanie (zawodne) realizowane było głównie przez **analogię**.

Uogólnienie wykorzystane zostało w trakcie badań do ujawnienia cech i zjawisk powtarzalnych, a przez to do formułowania zasad uniwersalnych dotyczących organizacji łączności na potrzeby kierowania reagowaniem kryzysowym.

W zakresie metod empirycznych szczególne znaczenie miała **obserwacja** ćwiczeń dowódczo-sztabowych w których uczestniczyły elementy systemu reagowania kryzysowego. Uwzględniając pozycję podmiotu obserwacji wobec przedmiotu obserwowanego zastosowanie znalazła zarówno obserwacja bierna, jak i uczestnicząca. Biorąc natomiast pod uwagę kryterium sposobu zaangażowania podmiotu obserwacji w proces badawczy, wykorzystana została obserwacja bezpośrednia i pośrednia. Przedmiotem obserwacji były:

- ćwiczenie dowódczo-sztabowe CZERWIEC 2002, mające miejsce w AON,
- ćwiczenie dowódczo-sztabowe CANNON CLOUD 2002 w 2KZ,
- ćwiczenie dowódczo-sztabowe AKADEMICKI PIRŚCIEŃ 2003 i 2004, mające miejsce na bazie 9 pdow w Białobrzegach.

Wyniki obserwacji wymienionych ćwiczeń pozwoliły autorom dokonać weryfikacji zasadności przyjętych założeń w zakresie występujących relacji i więzi informacyjnych. Rozwiązywanie problemów szczegółowych powodowało uzyskiwanie kolejnych faktów naukowych. Te zaś z kolei dawały możliwość zweryfikowania hipotezy i przedstawienia potencjalnego rozwiązania problemu głównego.

Kolejny, czwarty etap badań polegał na weryfikacji hipotezy w celu jej ostatecznego uzasadnienia i sprawdzenia.

Piąty, ostatni etap prac obejmował podsumowanie wyników badań, ich uogólnienie i syntezę. Przyjęto określoną, wiarygodną interpretację rozwiązania problemu badawczego, która zawarta została w pisarskim opracowaniu wyników badań.

Przedstawiona w niniejszym opracowaniu koncepcja wykorzystania środków i systemów technicznych do organizacji podsystemu łączności dla potrzeb kierowania reagowaniem kryzysowym stanowi w swej istocie logiczny ciąg twórczej pracy skromnego ilościowo zespołu badawczego w krótkim okresie czasowym.

Struktura niniejszej pracy obejmuje wstęp, pięć rozdziałów oraz zakończenie.

We **wstępie** zawarto wprowadzenie w problematykę pracy i uzasadnienie wyboru tematu oraz metodologiczne aspekty badań wraz z konstrukcją opracowania pisarskiego pracy i przyjętą procedurę badawczą.

Rozdział pierwszy zawiera prezentację wyników badań dotyczących funkcjonowania państwa w sytuacji kryzysowej.

W rozdziale drugi zawarto wyniki badań dotyczących identyfikacji elementów systemu kierowania reagowaniem kryzysowym i ich zasadniczych zadań.

Rozdział trzeci zawiera prezentację zidentyfikowanych relacji i więzi informacyjnych w systemie reagowania kryzysowego.

W **rozdziale czwartym** ujęto wyniki badań dotyczące identyfikacji systemu łączności kraju i jego infrastruktury organizacyjno technicznej.

W **rozdziale piątym** przedstawiono i dokonano charakterystyki urządzeń, środków i systemów telekomunikacyjnych oraz teleinformatycznych, a także koncepcję ich wykorzystania do organizacji łączności dla potrzeb kierowania reagowaniem kryzysowym na obszarze kraju.

W **zakończeniu** ujęto wnioski z przeprowadzonych badań.

1. FUNKCJONOWANIE PAŃSTWA W SYTUACJI KRYZYSOWEJ

płk dr hab. inż. Józef Władysław MICHNIAK

Kierowanie obronnością stanowi integralną część systemu kierowania państwem i jest realizowane przez te same organy władzy i administracji publicznej. Różny jest natomiast zakres udziału tych organów w sprawowaniu funkcji kierowania obronnością. „Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej"[1] stanowi „...podstawę i punkt wyjścia do opracowania poszczególnych strategii sektorowych w dziedzinach mających podstawowe znaczenie dla bezpieczeństwa i obronności państwa ...".
W systemie obronności państwa wyróżnia się struktury - podmiotową i przedmiotową.

Strukturę podmiotową tworzą elementy, którymi są w zasadzie wszystkie organa państwowe, jednostki organizacyjne oraz obywatele. Natomiast strukturę przedmiotową stanowią zadania realizowane przez podmioty w poszczególnych dziedzinach obronności, tj. militarnej (siłach zbrojnych) i pozamilitarnej (polityczno-administracyjnej i społecznej, ochronnej, gospodarczo-obronnej).

W realizacji przedsięwzięć związanych z obronnością państwa uczestniczą, w stosownym zakresie, organy władzy, organy administracji rządowej i samorządowej, podmioty gospodarcze, jednostki organizacyjne, organizacje społeczne, a także obywatele. Aby system obronności państwa sprawnie funkcjonował wszystkie te ogniwa powinny być powiązane informacyjnie, mieć precyzyjnie określone zadania w zakresie obronności i być właściwie przygotowane do ich realizacji na wypadek zagrożeń czasu pokoju kryzysu i wojny. Ponieważ system obronności państwa nie stanowi wyizolowanej, działającej samoistnie struktury państwowej, zadania obronności zostały wkomponowane w zadania merytoryczne (kompetencyjne) wszystkich organów państwowych oraz sfery działania podmiotów gospodarczych.

Kierowanie obronnością państwa jest procesem skomplikowanym, obejmującym całokształt działalności państwa zarówno w okresie pokoju, kryzysu, jak i wojny. Wymaga ono zorganizowania, efektywnego systemu kierowania, stanowiącego integralną część systemu kierowania państwem.

---

[1] Podpisana przez prezydenta RP 8 września 2003 r.

System kierowania obronnością państwa obejmuje: wzajemnie powiązane organizacyjnie i informacyjnie organa kierowania wraz z urzędami i instytucjami wykonawczymi, techniczne środki kierowania oraz specjalnie przygotowane stanowiska kierowania. Jego rola polega na sprzężeniu wszystkich elementów i ogniw systemu obronnego państwa w jednolitą, sprawnie funkcjonującą całość umożliwiającą realizację wszystkich zadań obronnych w okresie pokoju, kryzysu (zagrożenia) i wojny.

Podstawowymi ogniwami systemu kierowania obronnością państwa są:

- naczelne organy władzy i administracji państwowej;
- centralne organy administracji rządowej;
- terenowe organy administracji rządowej;
- organy samorządu terytorialnego.

Organy te podejmują decyzje w sprawach obronności w obszarze i zakresach określonych Konstytucją i ustawami. Ponadto w razie zagrożeń niemilitarnych i pośredniego militarnego zagrożenia bezpieczeństwa państwa (regionu, województwa) organa mogą doraźnie tworzyć na poszczególnych szczeblach kierowania „Zespoły" lub „Sztaby Kryzysowe". Tworzy się dla nich odpowiedni system powiązanych informacyjnie stanowisk kierowania, zapewniający ich właściwe funkcjonowanie w każdych warunkach w okresie pokoju, kryzysu i wojny oraz wydziela się odpowiednie siły i środki zabezpieczenia. Ich podstawowe zadanie to zebranie informacji, monitoring, przygotowanie projektu decyzji dla organu (ministra, wojewody, wójta), przekazanie wykonawcom zadań wynikających z decyzji oraz kontrola ich wykonania.

1.1. Funkcjonowanie państwa w sytuacji kryzysowej

„Kryzys" to pojęcie, które w ostatnich latach zrobiło szczególnie zawrotną „karierę" mimo, że używane było od ... wieków do określania pewnych sytuacji, stanów w dziedzinie medycyny, ekonomii, polityki, nauki a nawet teologii. „Czy dzisiaj nie doszło wręcz do kryzysu w pojęciu kryzysu" - zastanawia się prof. Andrea K. Smutek - Riemer[2], skoro kryzys spotyka nas praktycznie codziennie, na każdym kroku, w rozmaitych odcieniach - słyszy się codziennie: „kryzys w gospodarce", „kryzys w państwie", „kryzys rządu", „kryzys w UE" itp.

[2] A.K.Smutek - Riemer, Die Kriese des Kriesenbegriffes, OMZ 3/1995, s. 275 (tłumaczenie własne).

Nie jest istotą opracowania i intencją autora podjęcie próby systematyzowania szerokiego pojęcia kryzysu. Istnieją na ten temat bogate opracowania teoretyczne. Natomiast dla potrzeb głównego wątku opracowania zasadnicze rozważania skupione zostaną na **„kryzysie"** jako okresie funkcjonowania państwa wynikającymi z określonej sytuacji polityczno-militarnej.

Spośród wielu opublikowanych definicji kryzysu poniższa wydaje się, być zdaniem autorów, najpełniejsza dla określenia jego istoty:

KRYZYS to takie tylko zjawisko, którego przewidywane skutki mogą nadać organizacji nowy jakościowo wymiar, a więc przekształcić diametralnie istniejący stan rzeczy tworząc de facto nową jakość organizacyjną (organizację nową, choć funkcjonującą na bazie poprzedniej, np.: po zmianie zasadniczych celów organizacji, systemu preferowanych wartości albo radykalnej zmianie struktury organizacyjnej lub przebiegu i wartości procesów dynamicznych zachodzących w tej strukturze).[3]

Kryzysem są, więc sytuacje zagrożenia dla istniejącego status quo struktury systemu, jego otoczenia i wzajemnych między nimi relacji. Z powyższego wynika, że zagrożenia chociażby prowadziły do najbardziej katastrofalnych skutków, jeśli nie prowadzą do zmiany organizacji, nie mogą być uznane za kryzys. W wypadku państwa kryzysem jest sytuacja, w której państwo musi troszczyć się o dalsze przetrwanie. Stąd tylko władze państwowe są uprawnione do wyrokowania i określania konkretnych zjawisk w sferze międzynarodowych i wewnątrzpaństwowych stosunków społecznych jako zjawiska kryzysowe.

Kryzys - *jako okres funkcjonowania państwa* - oznacza rozwój wydarzeń wewnętrznych lub zewnętrznych, stanowiących bezpośrednie zagrożenie żywotnych interesów społeczeństwa (państwa) i następujących tak szybko, że wymuszają one na władzach politycznych natychmiastowe podjęcie przez nie szczególnych działań.[4] Zasadnicze źródła kryzysów to:

- zagrożenia naturalne (klęski żywiołowe, katastrofy naturalne);
- zagrożenia techniczne (związane z rozwojem cywilizacyjnym i gospodarczym);
- terroryzm międzynarodowy;
- inne zagrożenia, w tym związane z:

---

[3] C.Rutkowski, A.Kasprzewski, Siły Zbrojne w sytuacji kryzysowej, *AON 1996, s. 71.*
[4] R.Wróblewski, Zarys teorii kryzysu, *AON 1996, s. 10.*

- zasobami oraz niekontrolowanym przepływem broni masowego rażenia (BMR) i komponentów do jej wytwarzania,
- waśniami etnicznymi i religijnymi,
- sporami granicznymi, zacofaniem gospodarczo-cywilizacyjnym.

Zagrożenia są więc warunkiem koniecznym choć niewystarczającym do wystąpienia sytuacji kryzysowej. Dopiero kumulacja intensywnych lub długotrwałych zagrożeń może prowadzić do sytuacji kryzysowej[5].

Z przytoczonej definicji wynika, że w pojęciu kryzysu państwa mieszczą się zarówno zdarzenia zachodzące wewnątrz państwa, jak i w jego otoczeniu - bliższym i dalszym. Kryzys może obejmować więc zbiór wydarzeń zarówno z dominacją czynników wewnętrznych, jak i zewnętrznych.

a/ z dominacją czynników wewnętrznych:

- zamieszki lub strajki o znaczeniu państwowym;
- duże klęski żywiołowe i katastrofy ekologiczne;
- kryzys ekonomiczny i kryzys polityczny;
- zbrojne przewroty polityczne

b/ z dominacją czynników zewnętrznych:

- zbrojne starcia graniczne nie mające charakteru wojny;
- interwencja zbrojna państwa;
- jawne przygotowania jednego państwa do inwazji na inne;
- wojna między państwami sąsiadującymi z danym państwem;
- konflikt zbrojny między państwami z dalszego otoczenia danego państwa, zagrażający wprost lub pośrednio jego interesom bezpieczeństwa i angażujący to państwo po jednej z walczących stron;
- interwencja militarna danego państwa w ramach koalicji, wynikająca z jego zobowiązań międzynarodowych, realizowana w ramach przywracania lub wymuszania pokoju.[6]

---

[5] Tamże, s. 10. - Sytuacja kryzysowa to stan narastającej destabilizacji, niepewności i napięcia społecznego, charakteryzujący się naruszeniem więzi społecznych, możliwością utraty kontroli nad przebiegiem wydarzeń oraz eskalacją zagrożeń.
[6] Tamże, s. 11.

Wydarzenia zawarte w powyższych zbiorach można z kolei podzielić, uwzględniając ich charakter, na grupę kryzysowych zagrożeń militarnych i grupę kryzysowych zagrożeń cywilnych.

Ten podział jest istotny z punktu widzenia sposobu rozwiązywania sytuacji kryzysowych i roli w tym procesie poszczególnych resortów ministerialnych państwa. Rozwiązywanie sytuacji kryzysowych państwa z dominacją sił „cywilnych" (niemilitarnych) nawet przy zaangażowaniu sił zbrojnych jest przede wszystkim domeną Ministerstwa Spraw Wewnętrznych i Administracji jako wykonawcy woli władz państwa przy współudziale innych resortów w tym także Obrony Narodowej. Stąd też problem ten nie będzie rozpatrywany w dalszej części opracowania.

Zdecydowana większość sytuacji w jakich może znaleźć się państwo w okresie kryzysu ma charakter polityczno-militarny.

W tym przypadku resort Obrony Narodowej spełniać będzie rolę instytucji wiodącej jako wykonawca woli władz państwa w zakresie użycia sił zbrojnych i podporządkowanych sił sektorów pozamilitarnych.

Kryzys polityczno-militarny i tylko taki będzie więc istotą dalszych rozważań w pracy, niezależnie od skali zaangażowania sił zbrojnych do rozwiązywania sytuacji kryzysowych o innym podłożu.

Kryzys polityczno-militarny nie jest pokojem i nie może - ale nie musi - przerodzić się w wojnę. Jedną ze stron (podmiotem) tego kryzysu jest zawsze państwo, drugą natomiast może być określona siła wewnętrzna lub najczęściej zewnętrzna prowadząca walkę z państwem.

Sytuacje kryzysowe są rozwinięciem sytuacji, w których pojawiają się i zaczynają oddziaływać czynniki zagrażające bezpieczeństwu państwa. Z reguły czynniki te objawiają się najpierw we wszystkich niemilitarnych sektorach społecznych i jeśli skutki ich działania nie zostaną zrównoważone lub nie zostaną usunięte same przyczyny zagrożeń, to rozwój sytuacji może doprowadzić do przeniesienia kryzysu do sektora militarnego. Oznacza to, że strony (strona) objęte kryzysem decydują się na użycie siły zbrojnej do ostatecznego rozwiązania kryzysu zgodnie ze swoimi oczekiwaniami i potrzebami. Jakakolwiek więc próba użycia siły militarnej w tej sytuacji do osiągnięcia celów politycznych przez państwo lub grupę państw oznacza wejście w militarny etap kryzysu, który w ostateczności może przyjąć charakter konfliktu zbrojnego poniżej „poziomu wojny".

Podstawową zasadą przyjętą w tym względzie jest nieangażowanie do działań antykryzysowych całości sił zbrojnych, w przeciwnym razie oznacza to wojnę.

Nie można natomiast określić bliżej rodzaju i charakteru zagrożeń, przeciwko którym mogą być użyte siły zbrojne. W każdym przypadku tylko i wyłącznie najwyższe władze państwowe określają, co jest zagrożeniem, do którego nie można dopuścić; co jest zagrożeniem, któremu trzeba przeciwdziałać oraz co jest zagrożeniem, które może rozwinąć się w zagrożenie wojenne, które trzeba bezzwłocznie zlikwidować.

W sytuacji kryzysowej, gdy następuje bezpośrednie zagrożenie bezpieczeństwa państwa i brana jest pod uwagę możliwość użycia sił zbrojnych, elementy zbiorczej procedury postępowania powinny (wg kryteriów NATO) spełniać następujące warunki:

- pełna kontrola polityczna nad działaniami wojskowymi;
- podejmowane działania wojskowe muszą być spójne z celami dyplomatycznymi;
- ruchy wojsk muszą być starannie skoordynowane z działaniami dyplomatycznymi;
- działania dyplomatyczne i wojskowe powinny wskazywać na wolę negocjacji, a nie poszukiwania rozwiązań w opcji militarnej;
- należy unikać działań dających przygotowania działań wojennych na dużą skalę.[7]

Możliwości prowadzenia działań antykryzysowych w konkretnych sytuacjach będą każdorazowo zależały od ustaleń odnośnie do charakteru sytuacji kryzysowej i prawdopodobnych scenariuszy dalszego jej rozwoju.

W działaniach antykryzysowych niezwykle istotnym jest wczesne rozpoznanie jego symptomów, analiza zdarzeń i prognoza możliwego rozwoju sytuacji, podjęcie decyzji odnośnie do sposobów przeciwdziałania zagrożeniom, a więc wszystko to co mieści się w pojęciu „zarządzania kryzysem" *(ang. crisis management)*. Wielu autorów zajmujących się tym problemem wyraża swój sceptycyzm co do możliwości odpowiedniego wczesnego wykrywania oznak sytuacji kryzysowej, tłumacząc to wręcz nieprzewidywalnością zdarzeń szczególnie polityczno-militarnych. Pewnym wyjątkiem pod tym względem jest publikacja wspomnianej wcześniej prof. A.K. Smutek-Riemer, która na podstawie analizy sytuacji w b. Jugosławii i w Turcji zdefiniowała cztery rodzaje sygnałów - według ich „siły" - świadczących o narastaniu sytuacji kryzysowej i prowadzących do powstania kryzysu polityczno-militarnego:[8]

---

[7] Tezy na konferencję: Kierowanie reagowaniem kryzysowym, MON, maj 1996.
[8] Andrea K. Smutek-Riemer, Kreiesnfruerkennung: „Die Quadratur des Kreises? Soldat und Technik 5/1995 (tłumaczenie własne).

Sygnały dostrzegalne (ang. Fade Signals) - pojawiają się sporadycznie, są niepełne i nieuporządkowane. Dostrzec je mogą tylko wybitni fachowcy, długoletni korespondenci radiowi i telewizyjni akredytowani w danym kraju, dziennikarze prasowi oraz służby wywiadowcze. Istnieje wystarczająco dużo czasu na reakcje antykryzysowe pod warunkiem dostrzeżenia ich oznak. Przykładem była tu erozja władzy i rodzenie się ruchów nacjonalistycznych w byłej Jugosławii po śmierci marszałka Tito.

Sygnały słabe (ang. Weak Signals) - pojawiają się fragmentarycznie, bywa cyklicznie, z wyraźną jednoznacznością w swej treści. Konsekwencje zdarzeń powinny być czytelne dla fachowców nawet spoza rejonu (kraju), w którym narasta kryzys. Przy dostrzeżeniu tego rodzaju sygnałów jest również wystarczająco dużo czasu na odpowiednią reakcję władz i podjęcie potencjalnych akcji. Za taki sygnał uważa się zaistnienie studenckich protestów w b. Jugosławii, które zostały brutalnie stłumione.

Sygnały silne (ang. Strong Signals) - pojawiają się systematycznie, najczęściej są to publiczne i gwałtowne wystąpienia polityków stron, a możliwość dialogu między nimi sprowadza się do zera. Fakt zaistnienia kryzysu jest oczywisty dla tych, którzy znają jego historyczne i polityczne podłoże. Uważa się, że przy wystąpieniu silnych sygnałów jest jeszcze czas na podjęcie stosownych akcji i wykonanie odpowiednich posunięć. Za przykład silnych sygnałów uważa się gwałtowną retorykę różnych polityków b. Jugosławii, zapowiedź ogłoszenia niepodległości niektórych republik, pierwsze operacje sił zbrojnych.

Super sygnały (ang. Hyper Signals) to sygnały bezpośrednio poprzedzające wybuch kryzysu. Informacje o kryzysie są jednoznaczne, ustrukturyzowane, prawie pełne. Czytelność informacji jest oczywista nawet dla niefachowców, łącznie z możliwością przewidzenia konsekwencji swobodnego rozwoju sytuacji (przy braku reakcji na rozwój wypadków). Czas reakcji na kryzys jest bardzo krótki, a możliwość podjęcia potencjalnych akcji jest skrajnie ograniczony. Przykładem była gwałtowność reakcji ośrodków władz centralnych i republikańskich wokół sporu o Chorwację, uniemożliwienie rotacji na stanowiskach w prezydium rządu b. Jugosławii, zapowiedź separacji Słowenii i Chorwacji w drodze referendum czy groźba rządu federalnego wprowadzenia stanu wyjątkowego w kraju.

W powyższej klasyfikacji zauważa się wiele zależności i występujących prawidłowości w procesie narastania a właściwie rozwoju sytuacji kryzysowej aż do fazy zaistnienia kryzysu. Przede wszystkim zauważa się zależność pomiędzy czytelnością sygnałów (ich mocą) a czasem reakcji. Im sygnał o narastaniu zdarzeń kryzysowych jest silniejszy tym czas reakcji na nie jest krótszy. Kolejną zależnością jest stopień wiedzy o zjawiskach kryzysowych i możliwościach ich dostrzeżenia - im wyższa jest wiedza

o kryzysach i zdarzeniach im towarzyszących, tym większa jest możliwość dostrzeżenia i zarejestrowania sygnałów słabych i ich prawidłowe zinterpretowanie. Wreszcie im bliżej „krawędzi" kryzysu tym sygnały są coraz bardziej konkretne i jednoznaczne.

Pozostaje zadać pytanie, czy fakt wczesnego rozpoznania symptomów sytuacji kryzysowej równa się możliwości im przeciwdziałania i nie dopuszczenia do zaistnienia kryzysu? Odpowiedź nie może być jednoznaczna, bowiem zagrożenia kryzysowe już z definicji są zagrożeniami niedającymi się często określić aż do momentu wystąpienia. Do sytuacji kryzysowych nie można się przygotować w sensie tworzenia i mnożenia zbioru wariantów kryzysowych i stosownych koncepcji im przeciwdziałania.

Zapobieganie sytuacjom kryzysowym, a w wypadku jej zaistnienia, zawrócenie kierunku rozwoju nagłych i niebezpiecznych wydarzeń, zagrażających żywotnym interesom państwa, to domena „zarządzania sytuacją kryzysową" jako integralnej części kierowania obronnością państwa. Zarządzanie sytuacją kryzysową obejmuje trzy komplementarne zespoły działań:

- zapobieganie sytuacjom kryzysowym;
- sterowanie rozwojem tej sytuacji;
- kierowanie likwidacją skutków wynikłych z zaistnienia sytuacji kryzysowej.[9]

Zapobieganie sytuacjom kryzysowym polega na monitorowaniu sytuacji wewnętrznej i zewnętrznej oraz ostrzeganiu władz i społeczeństwa przed zbliżającą się sytuacją kryzysową oraz usuwaniu czynników kryzysogennych. Działania te obejmują wszystkie sfery funkcjonowania państwa: polityczną, ekonomiczną, społeczną, militarną i inne. Z tego też względu zapobieganie sytuacjom kryzysowym jest podstawowym zadaniem polityki bezpieczeństwa państwa.

Sterowanie rozwojem sytuacji kryzysowej ma na celu zmniejszenie szkodliwych skutków oraz możliwie najszybsze przywrócenie warunków normalnych (pokoju).

Kierowanie likwidacją skutków wynikłych z zaistnienia sytuacji kryzysowej ma istotne znaczenie społeczne, ekonomiczne i polityczne. Nie likwidowanie ich może spowodować powrót sytuacji kryzysowej.

Do pełniejszego zobrazowania problemu kryzysu, jego istoty i sposobów rozwiązywania autor zdecydował włączyć do opracowania wybrane poglądy w tej dziedzinie reprezentowane przez NATO.

---

[9] R.Wróblewski, Zarys ..., wyd. cyt. S. 41.

Według poglądów NATO - *„Kryzys to narodowa lub międzynarodowa sytuacja, w której istnieje zagrożenie wartości, interesów lub celów państwa (państw)".*

Z punktu widzenia interesów NATO jako paktu polityczno-wojskowego definicja ta interpretowana jest jako działalność, która bezpośrednio lub pośrednio wpływa lub może wpływać na bezpieczeństwo lub stabilność sprzymierzonych.

Z prezentowanych definicji wynika, iż kryzys charakteryzowany jest przez:

- zagrożenie rzeczywiste, wystarczająco ważne i tworzące poczucie pilności działania dla zagrożonego państwa lub państw (pilność zagrożenia jest tworzona przez jego wielkość i natychmiastowość);
- zagrożenia niespodziewane i tylko takie przekształcić się mogą w kryzys;
- skrajnie mały czas reakcji wynikający z faktu zaistnienia zagrożeń niespodziewanych;
- „mgłę niepewności" ponieważ wynik zależy od kompleksu interakcji między dwoma lub więcej antagonistycznymi stronami, których motywy i stanowiska są trudne do przewidzenia i mogą się zmienić w czasie;
- intensywność kryzysu, która może wzrastać w czasie.[10]

Zagrożenie użycia lub faktyczne użycie sił zbrojnych jest charakterystyczne dla intensyfikacji rozwoju procesu kryzysowego. Im bardziej agresywne są podjęte działania przez jedną ze stron, tym większa jest intensywność kryzysu i tym bardziej prawdopodobny jest wybuch konfliktu zbrojnego.

Z powyższych rozważań wynika kilka implikacji dla postępowania w sytuacjach kryzysowych:

- można i trzeba minimalizować „niespodzianość" zagrożeń kryzysowych poprzez efektywne rozpoznanie zdarzeń;
- nieokreśloność i często niejasność sytuacji w zagrożeniach kryzysowych wymaga elastycznego zastosowania wcześniej opracowanych procedur postępowania,

  tzn. zaadaptowania ich do określonej sytuacji w zależności od rozwoju zdarzeń;
- ponieważ kryzys może zintensyfikować się w czasie, powinny być przygotowane mniej lub bardziej stanowcze opcje postępowania.

---

[10] Na podstawie materiałów prezentowanych przez oficerów NATO podczas konferencji w AON, październik 1996.

Zarządzanie w sytuacji kryzysowej zdefiniowano w NATO jako - „***skoordynowane działania podjęte w celu likwidacji zagrożeń i zapobieganie ich eskalacji w kierunku wybuchu konfliktu zbrojnego***".

Mechanizm zarządzania sytuacją kryzysową zapewnić ma decydentom dopływ niezbędnej informacji oraz zaoferować właściwe instrumenty (polityczne, dyplomatyczne, ekonomiczne i militarne), których należy użyć w odpowiednim czasie i odpowiednio skoordynowanych do rozwiązania sytuacji kryzysowych.

Próbując dokonać pewnej „adopcji" poglądów i metod postępowania w państwach Europy Zachodniej odnośnie do oceny i rozwiązywania sytuacji kryzysowych należy uwzględnić, iż metody te zdeterminowane są przez:

- ustabilizowaną sytuację wewnętrzną tych państw: ekonomiczną, polityczną, społeczną i „wygranym bojem" o ekologię;
- praktycznie brakiem zagrożeń realnych ze strony państw sąsiednich;
- przynależność do struktury zbiorowego bezpieczeństwa;
- posiadanie nowoczesnych armii zarówno pod względem organizacyjnym, jak i wyposażenia technicznego.

Wynika stąd, iż w większości rozwiązania systemowe przeciwdziałania sytuacjom kryzysowym i działań antykryzysowych nakierowane są przede wszystkim na „zewnątrz" państw NATO. Oznacza to, że możliwe, realne zagrożenia o skali destabilizującej porządek demokratyczny upatrywane są poza blokiem państw NATO, głównie w obszarze Europy Środkowej, Południowo-wschodniej i w b. ZSRR. Owe uwarunkowania determinują organizację i zakres monitoringu sytuacji polityczno-militarnej, przyjęcie nowych struktur sił NATO i narodowych sił zbrojnych, modernizację systemów dowodzenia i łączności.

2. SYSTEM KIEROWANIA REAGOWANIEM KRYZYSOWYM

płk dr hab. inż. Józef Władysław MICHNIAK

Od niedawna rozwiązania w sferze kierowania obronnością państwa, a w tym dowodzenie siłami zbrojnymi odnoszą się do czasu pokoju, kryzysu i wojny. Jeszcze dwa lata temu brak było systemowych rozwiązań dotyczących powyższego problemu na okres kryzysu. Obecnie finalizuje się tworzenie w państwie całej struktury reagowania w sytuacjach kryzysowych, także również warunku uczestnictwa Polski w organizacjach międzynarodowych i sojuszniczych. Tworzony w Polsce praktycznie od początku państwowy kompleksowy system reagowania kryzysowego w skład którego wchodzą:

- organy kierowania („zintegrowany system kierowania i zarządzania na wypadek kryzysu");
- siły i środki przewidziane do działania w sytuacjach kryzysowych, zorganizowane w dwa zasadnicze podsystemy tj.:
  - militarny,
  - pozamilitarny (cywilny).

System reagowania kryzysowego będzie zdolny do wypełnienia wszystkich warunków umów międzynarodowych wynikających z potrzeb organizacji międzynarodowych dla zapewnienia sprawnej koordynacji działań w sytuacjach kryzysowych.

Rozwiązania strukturalne i systemowe w sferze zarządzania sytuacją kryzysową powinny zapewnić wymianę informacji pomiędzy państwem a organizacją międzynarodową oraz stworzyć mechanizmy pozwalające przede wszystkim na zarządzanie[1] wewnątrz państwa jego strukturami.

W jakim więc kierunku powinny pójść rozwiązania systemowe odnośnie do kierowania reagowaniem kryzysowym:

- tworzenia odrębnych centrów kierowania sytuacjami kryzysowymi o charakterze niemilitarnym;
- tworzenia jednego centrum kierowania sytuacją kryzysową państwa?

[1] Zarządzanie w sytuacjach kryzysowych to uporządkowana działalność polegająca na zapobieganiu sytuacjom kryzysowym lub przejmowaniu nad nimi kontroli i kształtowaniu ich przebiegu w drodze zaplanowanych działań oraz na odtwarzaniu zasobów lub przywróceniu im pierwotnego charakteru

Wydaje się, że odpowiedź na powyższe pytanie i wątpliwości tkwi w definicji kryzysu. Jeśli kryzys jest stanem, który najogólniej mówiąc decyduje o „być albo nie być" państwa, to powinno istnieć jedno centrum decyzyjne stanowiące o użyciu (zastosowaniu) odpowiednich środków (przedsięwzięć) adekwatnych do zagrożenia (o charakterze militarnym bądź niemilitarnym). Jakakolwiek propozycja tworzenia na szczeblu państwa wielu centrów zapobiegania i rozwiązywania sytuacji kryzysowych zależnie od ich źródeł są, co najmniej kontrowersyjne.

W NATO-wskim systemie zapobiegania i rozwiązywania kryzysów (ang. crisis management anc conflikt prevention) duże znaczenie ma wczesne ostrzeganie. Głównym źródłem wczesnego ostrzegania są narodowe systemy zbierania i analizy informacji, które po przetworzeniu dostarczane są do Kwatery Głównej w Brukseli. Połączone grupy sztabowe, takie jak Stałe Grupy Wywiadowcze (ang. Current Intelogence Groups - CIG) opracowują dzienne raporty wysyłane z kolei do poszczególnych stolic.

NATO-wski System Ostrzegawczy (ang. Precautinary System) uruchamia działanie, które stanowi pierwszy krok procesu zarządzania sytuacją kryzysową, stanowiącą zagrożenie dla bezpieczeństwa państw Sojuszu. Poza tym państwa członkowskie NATO posiadają mechanizm koordynacji i konsultacji w sytuacjach kryzysowych w formie Komitetu Weryfikacji i Koordynacji (ang. Verification Coordination Committee).

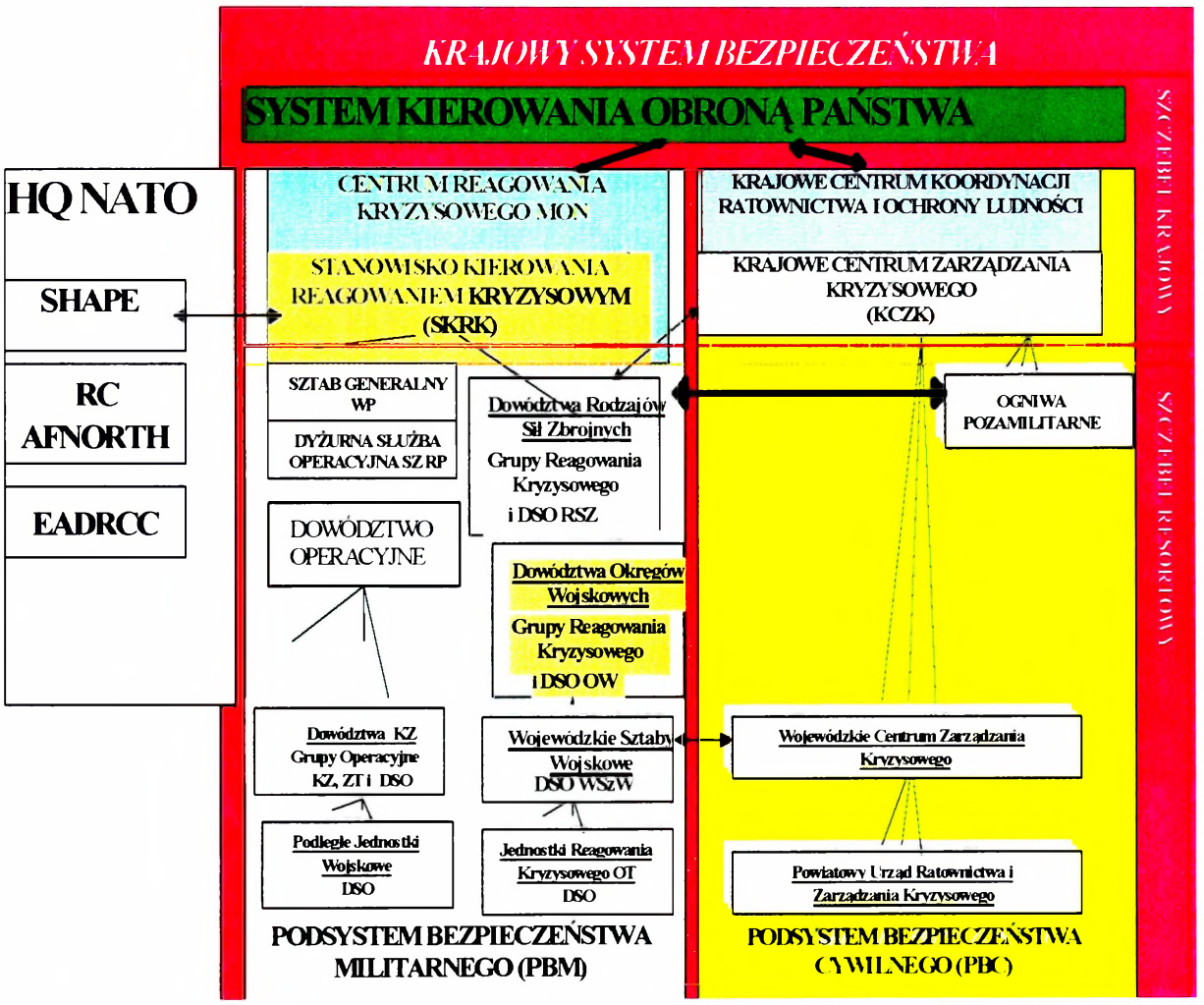
Monitoring rozwoju sytuacji kryzysowych prowadzony jest przez NATO-wskie Centrum Sytuacyjne z wykorzystaniem zautomatyzowanego systemu przetwarzania danych transmitowanych w łączach Zintegrowanego Systemu Łączności NATO.

Powyższy, z konieczności krótki, opis NATO-wskiego systemu zapobiegania i rozwiązywania kryzysów uzmysławia szereg zadań w sferze organizacyjnej i technicznej, w jakie w procesie włączania Polski do powyższego systemu musieliśmy wykonać. Dotyczy to zarówno konieczności współpracy etatowego organu antykryzysowego na szczeblu państwa z odpo-wiednim sztabem NATO, jak również zapewnienia łączności między nimi i współoperacyjności podsystemów przetwarzania i transmisji danych.

2.1. System Reagowania Kryzysowego Ministerstwa Obrony Narodowej (SRK MON)

System Reagowania Kryzysowego MON (SRK MON) stanowi podsystem bezpieczeństwa militarnego (PBM) w ramach Krajowego Systemu Bezpieczeństwa.

Obejmuje on swym zasięgiem wszystkie systemy wspomagania dowodzenia (w tym, w szczególności systemy reagowania kryzysowego) wchodzące w skład dowództw w pionie powoływanego Dowództwa Operacyjnego i dowództw rodzajów sił zbrojnych. Ściśle współpracuje z podsystemem bezpieczeństwa cywilnego (PBC) oraz z adekwatnymi systemami reagowania kryzysowego krajów NATO i PfP. (rys. 2.1.1.).



Rys. 2.1.1. Ogólna struktura systemu reagowania kryzysowego państwa

Naczelnym zadaniem SRK MON jest wykrywanie militarnych zagrożeń kryzysowych oraz jak najskuteczniejsze im przeciwdziałanie, przy wykorzystaniu wszystkich dostępnych sił i środków (militarnych i niemilitarnych) przeznaczonych do reagowania kryzysowego od momentu narastania kryzysu, poprzez okres jego trwania, aż do jego wygaśnięcia lub przejścia do fazy wojny. W okresie wojny SRK MON będzie elementem działającym w strukturach wojennych. Powyższe zadanie jest realizowane przez Centrum Reagowania Kryzysowego MON.

Zaproponowana struktura systemu bazująca na współpracujących ze sobą dwóch podsystemach wymaga ustalenia, co najmniej na poziomie centralnym pomiędzy Rządowym

Centrum Reagowania Kryzysowego a Centrum Reagowania Kryzysowego MON reguł i zasad współdziałania związanych z wymianą informacji między nimi oraz określeniem kierownika działań kryzysowych i wiodącego Centrum, w przypadku konieczności opanowania bądź likwidacji sytuacji kryzysowych „niejednorodnych" tzn. takich, w których uczestniczą siły i środki obu podsystemów. W przypadku sytuacji kryzysowych „jednorodnych" tzn. wymagających użycie tylko sił i środków jednego podsystemu obowiązywałyby zasady koordynacji i współdziałania przyjęte w tym podsystemie. W każdej sytuacji, w całym systemie obowiązuje generalna zasada jednoosobowego kierownictwa (dowodzenia) i ponoszenia odpowiedzialności za podejmowane decyzje. Natomiast w sytuacjach kryzysowych „niejednorodnych" powinny obowiązywać następujące zasady:

1. Zakres, sposób i reguły wymiany informacji między podsystemami byłyby określone w przepisach (regulaminie) funkcjonowania każdego podsystemu – dla podsystemu bezpieczeństwa militarnego najlepszym rozwiązaniem jest przyjęcie wzorów dokumentów zgodnie z PN – 02-A002 zgodną ze STANAG -2014.
2. W przypadku kryzysu „cywilnego" powstałego w wyniku zagrożeń i zdarzeń o charakterze niemilitarnym, wiodącym ośrodkiem w kierowaniu działaniami kryzysowymi jest odpowiedni element podsystemu bezpieczeństwa cywilnego (np.: Centrum Zarządzania Kryzysowego (CZK) wojewody, starosty lub RCKK) a struktury podsystemu militarnego będą podwykonawcami wspierającymi te działania swoimi niezbędnymi w danej sytuacji siłami i środkami.
3. W przypadku kryzysu militarnego wiodącym ośrodkiem w kierowaniu działaniami kryzysowymi jest CRK MON, a struktury podsystemu cywilnego, w przypadku konieczności ich użycia, są podwykonawcami w zakresie prowadzenia działań ratowniczych i ochrony ludności.
4. W przypadku jednoczesnego wystąpienia obu rodzajów kryzysów kierowanie i koordynowanie działaniami kryzysowymi przejmuje Rządowy Zespół Koordynacji Kryzysowej.
5. Głównym kryterium uruchomienia reagowania kryzysowego jest pierwszeństwo uzyskania informacji o zdarzeniu, które uznane zostało za rodzące kryzys lub, którego następstwem może być kryzys.
6. W sytuacji konieczności zaangażowania sił sojuszu zarówno cywilnych jak i wojskowych zgodnie z zasadami obowiązującymi w NATO siły te w przypadku

zaangażowania na terenie państwa NATO oddawane są pod kierownictwo danego państwa, chyba, że zdecyduje ono inaczej i powierzy ono kierowanie działaniami kryzysowymi NATO, a konkretnie Euro-Atlantic Disaster Response Coordination Centre (EADRCC) w przypadku kryzysu niemilitarnego i Supreme Headquarters Allied Powers Europe (SHAPE) w przypadku kryzysu o charakterze militarnym.

2.2. Ogniwa Systemu Reagowania Kryzysowego Ministerstwa Obrony Narodowej (SRK MON)

Celem funkcjonowania podsystemu bezpieczeństwa militarnego jest ochrona i obrona przed zagrożeniami integralności terytorialnej państwa, jego niezależności politycznej, a w skrajnych przypadkach przetrwanie narodu i państwa. Głównym gwarantem realizacji powyższego celu są Siły Zbrojne RP. Ich użycie wymaga jednak wczesnego wykrycia i monitorowania zagrożeń polityczno – militarnych mogących być przyczyną powstania konfliktowych sytuacji kryzysowych (kryzysu militarnego), to jest takich, w których narzędziem rozstrzygania konfliktu są siły zbrojne i mamy do czynienia ze świadomym przeciwnikiem. Sytuacje te w zasadzie nie wybuchają nagle, a narastają i mogą być w ekstremalnym przypadku przyczyną wojny. Dlatego w przeciwdziałaniu im w systemie wyróżniamy następujące etapy reagowania kryzysowego:

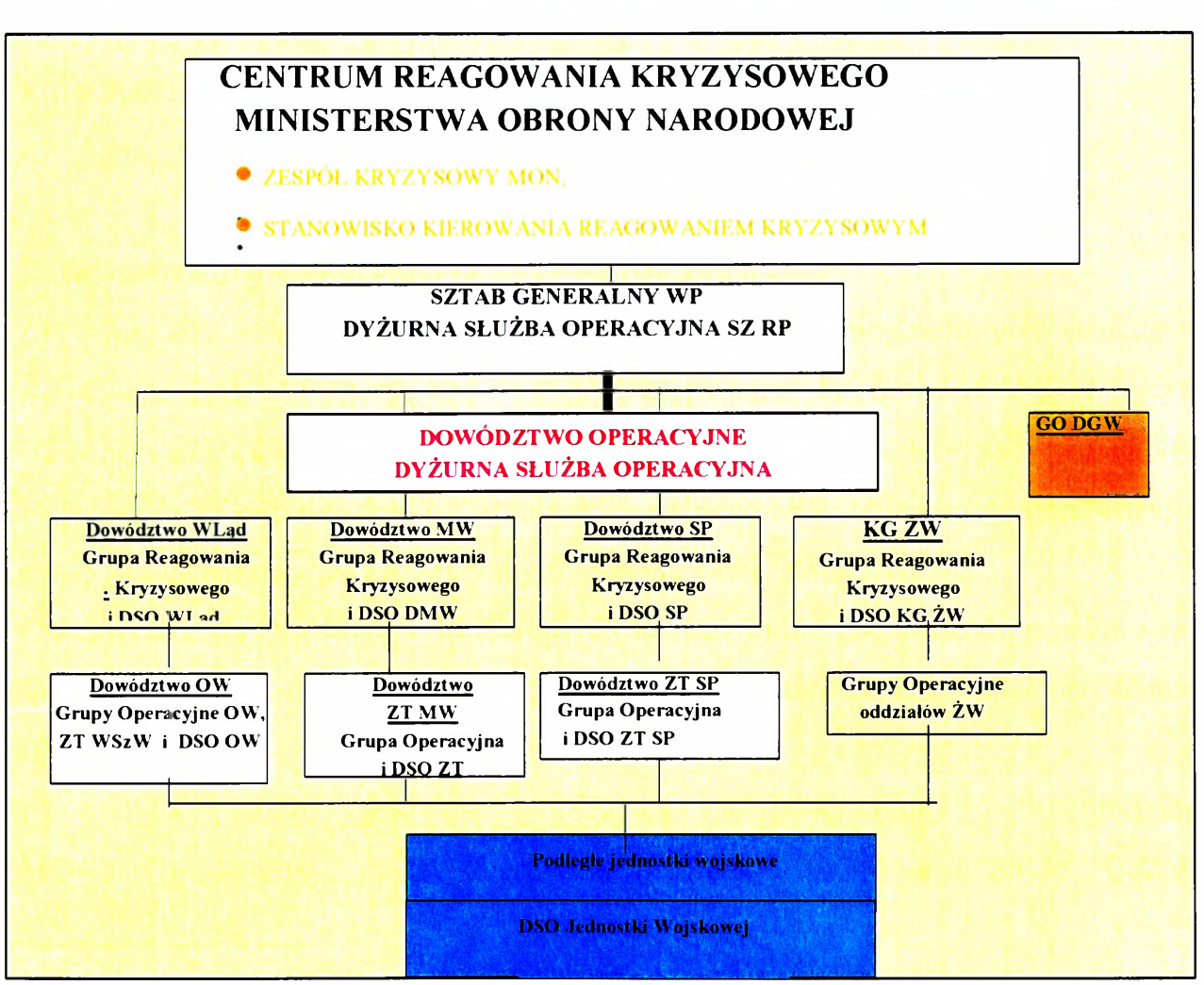
- etap przedkryzysowy – funkcjonowania normalnego systemu;
- etap narastania kryzysu;
- etap sytuacji kryzysowej;
- etap pokryzysowy.

W każdym z tych etapów prowadzone jest zbieranie informacji o zagrożeniach z różnych źródeł (wywiad, prasa, radio, telewizja, meldunki) ich ocena oraz planowanie i koordynowanie przedsięwzięć zmierzających do likwidacji zagrożeń lub zaistniałych zdarzeń. Tak rozumiane reagowanie kryzysowe podsystemu bezpieczeństwa militarnego powinno bazować na funkcjonujących w sytuacjach normalnych i kryzysowych dyżurnych służbach operacyjnych (DSO) poszczególnych szczebli dowodzenia Sił Zbrojnych oraz Zespole Kryzysowym MON („dowództwie Ministra Obrony Narodowej rozmieszczonym na „stanowisku dowodzenia" tzn. Stanowisku Kierowania Reagowaniem Kryzysowym MON) kierującym w zależności od wielkości i rodzaju sytuacji kryzysowej Grupami Reagowania

Kryzysowego (GRK): Sztabu Generalnego; Dowództw Rodzajów Sił Zbrojnych i Grupami Operacyjnymi (GO): Okręgów Wojskowych; Związków Taktycznych; Oddziałów.

Zadaniem DSO poszczególnych szczebli dowodzenia jest zbieranie informacji o zmianie w stanie sił i środków jednostek wojskowych oraz zaistniałych nadzwyczajnych zdarzeniach i zagrożeniach, a następnie przedstawienie meldunków o nich przełożonym. Na podstawie zebranych z różnych źródeł meldunków sytuacyjnych dokonywana jest ocena sytuacji oraz podejmowane są decyzje dotyczące sposobu likwidacji zagrożeń lub rozwiązania sytuacji kryzysowej. Ogólna struktura reagowania kryzysowego podsystemu bezpieczeństwa militarnego pokazana jest na rys.2.2.1.

Centrum Reagowania Kryzysowego MON (CRK MON) jest komórką organizacyjną Ministerstwa Obrony Narodowej powołaną decyzją ministra ON. Stanowi ono zabezpieczenie funkcjonalne działania sztabu kryzysowego szczebla MON powoływanego na wypadek konieczności użycia Sił Zbrojnych RP oraz innych sił i środków niemilitarnych w kolejnych etapach sytuacji kryzysowej w zakresie bezpieczeństwa militarnego i jest odpowiednikiem National Military Command Center (NMCC) w rozumieniu koncepcji US Air Force Electronic System Center, Hanscom AFB oraz MITRE Corporation.



Rys.2.2.1. Podsystem bezpieczeństwa militarnego

Podstawowym stanowiskiem zarządzania dla obsady personalnej CRK MON jest Stanowisko Kierowania Reagowaniem Kryzysowym.

Podstawę rozwijania Systemu Reagowania Kryzysowego MON stanowią:

1) decyzje Ministra Obrony Narodowej,
2) rozkazy Szefa Sztabu Generalnego WP.

Projekty decyzji i rozkazów przygotowują:

1) decyzji Ministra Obrony Narodowej – Dyrektor Departamentu Polityki Obronnej lub szef innej komórki organizacyjnej MON, wskazanej przez Ministra Obrony Narodowej,
2) rozkazu Szefa Sztabu Generalnego WP – Szef Generalnego Zarządu Operacyjnego Sztabu Generalnego WP.

Stopień rozwinięcia elementów Systemu Reagowania Kryzysowego MON określają stany gotowości kryzysowej:

- stała gotowość kryzysowa - ALFA;
- podwyższona gotowość kryzysowa - ALFA 1;
- gotowość zagrożenia kryzysowego – BRAVO;
- pełna gotowość kryzysowa – CHARLIE.

Poszczególne stany gotowości kryzysowej oznaczają:

1) **ALFA** – stałą gotowość komórek MON oraz wydzielonych struktur Sił Zbrojnych do rozwinięcia Systemu Kierowania Reagowaniem Kryzysowym MON w czasie pokoju. Za przygotowanie Stanowiska Kierowania Reagowaniem Kryzysowym (SKRK) MON do rozwinięcia odpowiada Szef Sztabu Generalnego WP, organem wykonawczym w tym zakresie jest Generalny Zarząd Operacyjny Sztabu Generalnego WP.

Dyżurna Służba Operacyjna Sił Zbrojnych RP utrzymuje gotowość do przekazywania sygnałów o podwyższeniu gotowości kryzysowej Kierownictwu SKRK MON oraz zmianie dyżurnej[2] SKRK MON.

2) **ALFA 1** – gotowość polegającą na zwiększeniu – w godzinach pozasłużbowych - dyspozycyjności Kierownictwa SKRK MON oraz obsad: Oddziału

[2] Zmiana dyżurna – obsada I lub II lub III zmiany Sztabu Kryzysowego MON utrzymywana w gotowości do stawiennictwa w systemie dekadowym: I zmiana: 1-10 dzień miesiąca, II zmiana: 11-20 dzień miesiąca, III zmiana: 21-31 (ostatni dzień miesiąca).

Analityczno – Technicznego Sekretariatu Ministra Obrony Narodowej, Oddziału Gotowości Obronnej Departamentu Polityki Obronnej, Oddziału Operacji Kryzysowych Zarządu Operacji Bieżących Generalnego Zarządu Operacyjnego Sztabu Generalnego WP, szefów zespołów SKRK MON i zmiany dyżurnej[3].

Gotowość tę wprowadza się w przypadku wystąpienia zagrożeń mogących doprowadzić do sytuacji kryzysowej. Sygnał o wprowadzeniu gotowości ALFA 1 przekazywany jest na polecenie Szefa Sztabu Generalnego WP poprzez Dyżurną Służbę Operacyjną Sił Zbrojnych RP.

3) **BRAVO** – gotowość wprowadzaną w przypadku wzrostu zagrożenia niewymagającego pełnego rozwinięcia SKRK MON. Szczegółowe zadania SKRK MON oraz jego obsadę określa decyzja Ministra Obrony Narodowej i rozkaz Szefa Sztabu Generalnego WP (w zależności od charakteru zagrożenia). Sygnał o wprowadzeniu gotowości BRAVO przekazywany jest na polecenie Szefa Sztabu Generalnego WP poprzez Dyżurną Służbę Operacyjną Sił Zbrojnych RP do Kierownictwa SKRK MON oraz obsad zespołów.

Czas stawiennictwa w miejscu pracy wynosi:

- I zmiana - do 3 godzin;
- II zmiana - do 15 godzin;
- III zmiana - do 27 godzin.

4) **CHARLIE** – gotowość wprowadzaną w razie nieuchronności wystąpienia kryzysu, wymagającego zaangażowania pełnej obsady SKRK MON. Pełne rozwinięcie SKRK MON może nastąpić z pominięciem gotowości BRAVO.

Szczegółowe zadania SKRK MON określa decyzja Ministra Obrony Narodowej i rozkaz Szefa Sztabu Generalnego WP. Sygnał o wprowadzeniu gotowości CHARLIE przekazywany jest na polecenie Szefa Sztabu Generalnego WP poprzez Dyżurną Służbę Operacyjną Sił Zbrojnych RP. Czas stawiennictwa – jak w stanie gotowości kryzysowej BRAVO.

Za powiadamianie obsady SKRK MON o wprowadzonych stanach gotowości kryzysowej odpowiada Dyżurna Służba Operacyjna Sił Zbrojnych RP. Powiadamianie odbywa się poprzez dyżurne służby operacyjne dowództw rodzajów Sił Zbrojnych, Wojskowych Służb Informacyjnych, Komendy Głównej Żandarmerii Wojskowej, Dowództwa Garnizonu Warszawa oraz służby dyżurne komórek MON, wydzielających przedstawicieli do SKRK MON.

---

[3] Z takim wyliczeniem, aby czas stawiennictwa w miejscu pracy nie przekraczał 3 godzin.

2.3. Stanowisko Kierowania Reagowaniem Kryzysowym (SKRK)

Przeznaczeniem Stanowiska Kierowania Reagowaniem Kryzysowym jest wspomaganie osób funkcyjnych CRK MON w zakresie podejmowania decyzji podczas prowadzenia działań w całodobowym reżimie codziennego ich funkcjonowania (monitoringu), a także podczas działania rozszerzonego sztabu dowodzącego operacją antykryzysową zarówno na terenie kraju jak i poza jego granicami. SKRK.

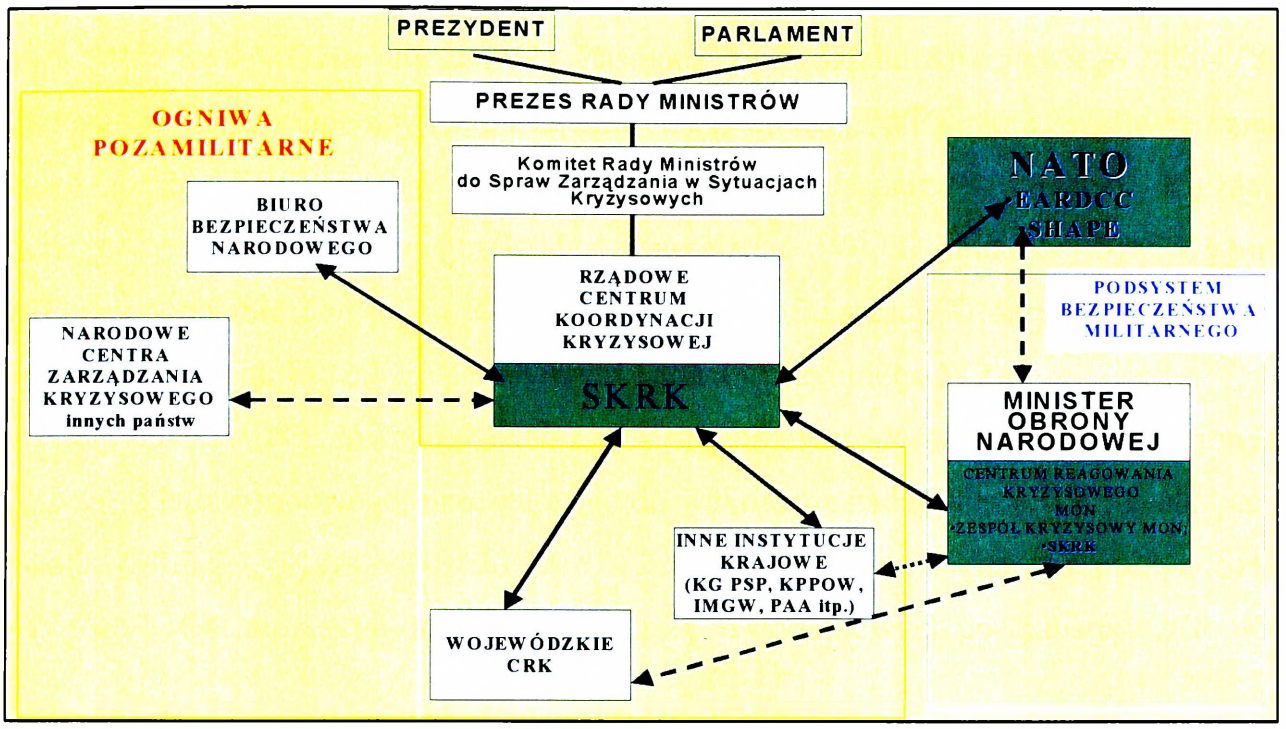
Stanowisko Kierowania Reagowaniem Kryzysowym (SKRK) stanowi główny komponent systemu informatycznego dla sztabów kryzysowych, zabezpieczający funkcjonalne wspomaganie wykonywania zadań z zakresu reagowania kryzysowego na szczeblu MON i jest powiązany informacyjnie z niższymi szczeblami Systemu Reagowania Kryzysowego oraz systemami kryzysowymi innych państw współpracujących (zarówno w ramach NATO jak i PfP).

Przewiduje się, że SKRK będzie stanowić przede wszystkim zasadniczy element CRK MON. Natomiast w przyszłości może również stanowić element centrów reagowania kryzysowego działających w ramach niższych szczebli planowanego Dowództwa Operacji Połączonych i Dowództwa Wparcia.

SKRK jest lokalną siecią Zautomatyzowanych Stanowisk Pracy (ZSP) oraz serwerów (struktura techniczna) obsługiwanych przez System Informatyczny SKRK (struktura programowa), zabezpieczający i wspomagający efektywne wykonywanie zadań personelu sztabu kryzysowego.

W skład SKRK MON wchodzą: Kierownictwo; Zespół do Spraw Polityki Bezpieczeństwa; Zespół Operacyjny; Zespół do Spraw Logistyki; Zespół Kierowania Łącznością i Informatyką; Zespół do Spraw Ochrony; Zespół Zabezpieczenia.

Usytuowanie SKRK MON w strukturze Systemu Reagowania Kryzysowego określono na rys.2.3.1.



Rys.2.3.1. Usytuowanie SKRK MON w strukturze Systemu Reagowania Kryzysowego

W zależności od rodzaju kryzysu i stopnia jego narastania, mogą być tworzone różne komórki wewnętrzne Sztabu Kryzysowego MON. Sposób ich powoływania i zakres działania określa Szef Sztabu Generalnego WP w rozkazie. Strukturę organizacyjną SKRK MON przedstawiono na rys.2.3.2.

Rys. 2.3.2. Struktura organizacyjna SKRK MON

Kierownictwo Sztabu Kryzysowego MON stanowią: Szef Sztabu Kryzysowego MON (Zastępca Szefa Sztabu Generalnego WP), Zastępca Szefa Sztabu Kryzysowego MON (Szef Generalnego Zarządu Operacyjnego Sztabu Generalnego WP) oraz szefowie zmian dyżurnych Sztabu Kryzysowego MON (I zmiana - Szef Zarządu Operacji Bieżących Generalnego Zarządu Operacyjnego Sztabu Generalnego WP, II zmiana – Szef Dyżurnej Służby Operacyjnej Sił Zbrojnych RP, III zmiana - Szef Zarządu Doktryn i Szkolenia Sił Zbrojnych Generalnego Zarządu Operacyjnego Sztabu Generalnego WP).

Szef Sztabu Kryzysowego MON może organizować doraźne grupy funkcjonalne, z podległego składu osobowego, przeznaczone do wykonania zadań bieżących, wynikających z rozwoju sytuacji kryzysowej. Ponadto, na jego wniosek, skład zespołów Sztabu Kryzysowego MON może być czasowo poszerzany o dodatkowych specjalistów z komórek MON.

Przykładem funkcjonalnego podziału SKRK może być podział stanowiska kierowania na dwie części, z których każda będzie pełniła inne funkcje.

Część pierwsza zwana dalej „część operacyjna" powinna pełnić swoje obowiązki w trybie ciągłym- 24 godziny, przez 7 dni w tygodniu. Szef zmiany dyżurnej pełni jednocześnie obowiązki szefa części operacyjnej SKRK. Część druga natomiast zwana dalej „część analizy danych i opracowywania planów reagowania" funkcjonować powinna w trybie dziennym, z zadaniem analizy dane zbierane przez część operacyjną, oraz opracowywać na tej podstawie alternatywne plany reagowania kryzysowego. Część ta uzupełnia w trakcie etapu narastania kryzysu część Operacyjną, natomiast w etapie przedkryzysowym, ta bierze udział w szkoleniach i ćwiczeniach. Szef zespołu operacyjnego pełni jednocześnie obowiązki szefa części analizy danych i opracowywania planów reagowania.

Kierownictwo Sztabu Kryzysowego MON kieruje pracą Zespołów Sztabu Kryzysowego MON. Szef Sztabu Kryzysowego MON jest przełożonym składu osobowego Sztabu Kryzysowego MON. W przypadku jego nieobecności obowiązki Szefa Sztabu Kryzysowego MON pełni zastępca Szefa Sztabu Kryzysowego MON.

Szefowie zmian dyżurnych odpowiadają za sprawne, merytoryczne i terminowe wykonywanie zadań przez Zespoły Sztabu Kryzysowego MON.

Do zadań Kierownictwa Sztabu Kryzysowego MON należy w szczególności:

1. Informowanie Ministra Obrony Narodowej o zagrożeniach mogących prowadzić do powstania sytuacji kryzysowych oraz wnioskowanie o rozwinięcie Sztabu Kryzysowego MON.

2. Terminowe rozwinięcie oraz właściwa organizacja pracy Sztabu Kryzysowego MON.

3. Przedstawianie wariantowych propozycji rozwiązań sytuacji kryzysowych.

4. Koordynowanie działań elementów Systemu Kierowania Reagowaniem Kryzysowym MON z działaniami komórek organizacyjnych MON i organami NATO (innych wojskowych organizacji uczestniczących w rozwiązywaniu sytuacji kryzysowej).

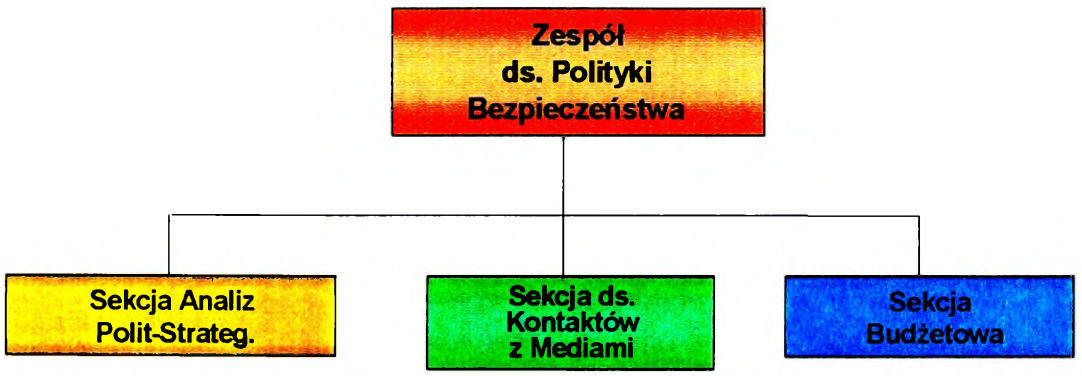
5. Nadzór nad wykonywaniem dokumentów i ich dystrybucją do naczelnych organów władzy państwowej oraz dowództw rodzajów Sił Zbrojnych odpowiedzialnych za reagowanie kryzysowe.

6. Uczestnictwo w odprawach organizowanych przez Zespół Kierownictwa MON oraz innych - według potrzeb.

Zespół do Spraw Polityki Bezpieczeństwa składa się z:

- Sekcji Analiz Polityczno-Strategicznych,
- Sekcji Budżetowej,
- Sekcji do Spraw Kontaktów z Mediami.

W skład Zespołu wchodzą przedstawiciele departamentów: Polityki Obronnej, Współpracy Międzynarodowej, Prawnego, Wychowania i Promocji Obronności, Budżetowego oraz Biura Prasy i Informacji, a także Generalnego Zarządu Planowania Strategicznego.



Rys.2.3.3. Struktura organizacyjna Zespołu ds. Polityki Bezpieczeństwa SKRK MON

Obowiązki Szefa Zespołu ds. Polityki Bezpieczeństwa pełni Szef Sekcji Analiz Polityczno-Strategicznych (przedstawiciel Departamentu Polityki Obronnej), który podlega bezpośrednio szefowi zmiany dyżurnej.

Obowiązki szefów pozostałych sekcji sprawują:

- Sekcji Budżetowej – przedstawiciel Departamentu Budżetowego, który podlega szefowi Zespołu,
- Sekcji do Spraw Kontaktów z Mediami – przedstawiciel Biura Prasy i Informacji, który podlega Szefowi Zespołu.

Zadania Zespołu do Spraw Polityki Bezpieczeństwa

Zespół do Spraw Polityki Bezpieczeństwa przeznaczony jest do wsparcia procesu decyzyjnego Sztabu Kryzysowego MON poprzez wszechstronną ocenę sytuacji polityczno-militarnej oraz przygotowanie, uzgodnionych pod względem prawnym i finansowym, propozycji rozwiązań sytuacji kryzysowej zgodnie z polityką obronną państwa.

Do zadań Zespołu do Spraw Polityki Bezpieczeństwa należy:

1. Dokonywanie ocen sytuacji kryzysowych i prognozowanie ich rozwoju.

2. Wypracowywanie propozycji stanowiska Ministerstwa Obrony Narodowej w celu rozwiązania sytuacji kryzysowych.

3. Przygotowywanie projektów dokumentów decyzyjnych Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów oraz Ministra Obrony Narodowej.

4. Organizowanie i koordynowanie prac związanych z wdrażaniem decyzji i wytycznych Ministra Obrony Narodowej w zakresie realizacji zadań kryzysowych.

5. Opracowywanie propozycji współpracy z organizacjami międzynarodowymi lub organami państw obcych, działającymi w rejonie kryzysu.

6. Opracowywanie propozycji finansowania zadań przewidzianych do realizacji podczas sytuacji kryzysowych.

7. Udział w opracowywaniu projektów aktów prawnych oraz umów międzynarodowych w zakresie użycia sił i środków w operacjach kryzysowych.

8. Uzgadnianie pod względem prawnym podejmowanych decyzji.

9. Aktualizacja koncepcji (planów) ustalających funkcjonowanie systemu obronnego państwa w czasie zagrożenia bezpieczeństwa (kryzysu).

10. Współdziałanie z pozamilitarnymi ogniwami obronnymi krajowego systemu kierowania reagowaniem kryzysowym.

11. Planowanie działań w zakresie wykorzystania sił i środków pozamilitarnych ogniw obronnych.

12. Opracowywanie materiałów informacyjnych dla potrzeb kontaktów z mediami.

Zadania poszczególnych sekcji Zespołu do Spraw Polityki Bezpieczeństwa:

1) do zadań Sekcji Analiz Polityczno - Strategicznych należy:

1.1. Analizowanie, ocena, prognozowanie i monitorowanie rozwoju sytuacji kryzysowych oraz przedstawianie wniosków Szefowi Sztabu Kryzysowego MON.

1.2. Współudział w wypracowywaniu propozycji stanowiska resortu Obrony Narodowej w rozwiązywaniu sytuacji kryzysowej.

1.3. Wymiana informacji w zakresie zagrożeń bezpieczeństwa państwa (sytuacji kryzysowych) z Kwaterą Główną NATO oraz strukturami wojskowymi innych organizacji międzynarodowych - komórkami odpowiedzialnymi za reagowanie kryzysowe.

1.4. Wymiana informacji z Krajowym Sztabem Kryzysowym w zakresie realizacji zadań wynikających z polityki obronnej oraz strategii obronności państwa w sytuacjach kryzysowych.

1.5. Koordynowanie wdrażania decyzji i wytycznych Ministra Obrony Narodowej w zakresie reagowania kryzysowego.

1.6. Opracowywanie projektów dokumentów wykonawczych (postanowień Prezydenta Rzeczypospolitej Polskiej, rozporządzeń Prezesa Rady Ministrów, zarządzeń i decyzji Ministra Obrony Narodowej, itp.) dotyczących polityczno - militarnego rozwiązywania sytuacji kryzysowych.

1.7. Udział w opracowywaniu projektów umów w zakresie użycia sił i środków w sytuacjach kryzysowych.

1.8. Udział w opracowywaniu wytycznych dotyczących sygnałów NPS (ang. NATO Precautionary System) oraz monitorowanie ich realizacji w zakresie podwyższania gotowości obronnej państwa.

1.9. Ocena przestrzegania międzynarodowych umów i porozumień dotyczących kontroli zbrojeń, rozbrojenia, budowy środków zaufania oraz przedstawianie opinii i wniosków Szefowi Sztabu Kryzysowego MON.

1.10. Współudział w opracowywaniu projektów aktów prawnych oraz umów międzynarodowych przygotowywanych przez resort Obrony Narodowej.

1.11. Koordynowanie prac związanych z przygotowywaniem dokumentów na posiedzenia Komitetu Rady Ministrów w czasie kryzysu.

1.12. Opiniowanie projektów umów dotyczących udziału Sił Zbrojnych RP w przedsięwzięciach podejmowanych przez resort Obrony Narodowej.

1.13. Współudział w przygotowywaniu materiałów dotyczących polityki obronnej państwa w okresie kryzysu.

1.14. Monitorowanie realizacji zadań obronnych wykonywanych przez pozamilitarne ogniwa systemu obronnego państwa.

1.15. Prowadzenie dziennika działań Zespołu do Spraw Polityki Bezpieczeństwa.

2) do zadań Sekcji Budżetowej należy:

2.1. Analizowanie kosztów udziału Sił Zbrojnych RP w rozwiązywaniu kryzysu oraz składanie meldunków i propozycji w tym zakresie Szefowi Sztabu Kryzysowego MON.

2.2. Analizowanie rozliczeń międzynarodowych i międzyresortowych z tytułu umów oraz wzajemnych świadczeń i zobowiązań.

2.3. Nadzór nad wykorzystywaniem przydzielonego limitu środków finansowych przez resort Obrony Narodowej.

2.4. Współudział w opracowywaniu projektów aktów prawnych, umów międzynarodowych i innych dokumentów dotyczących użycia sił i środków w operacjach kryzysowych.

3) do zadań Sekcji do Spraw Kontaktów z Mediami należy:

3.1. Organizowanie kontaktów Sztabu Kryzysowego MON z mediami.

3.2. Kształtowanie, wspólnie z Biurem Prasy i Informacji, jednolitej polityki informacyjnej resortu Obrony Narodowej mającej na celu pozyskiwanie poparcia społecznego dla działań podejmowanych w celu przezwyciężania kryzysu w kraju i poza jego granicami.

3.3. Utrzymywanie stałych kontaktów z Biurem Prasy i Informacji Kwatery Głównej NATO oraz służbami prasowo – informacyjnymi państw partnerskich.

3.4. Przygotowywanie komunikatów i materiałów informacyjnych dotyczących sytuacji kryzysowej.

3.5. Redagowanie, wspólnie z Biurem Prasy i Informacji, strony internetowej MON w części dotyczącej sytuacji kryzysowej.

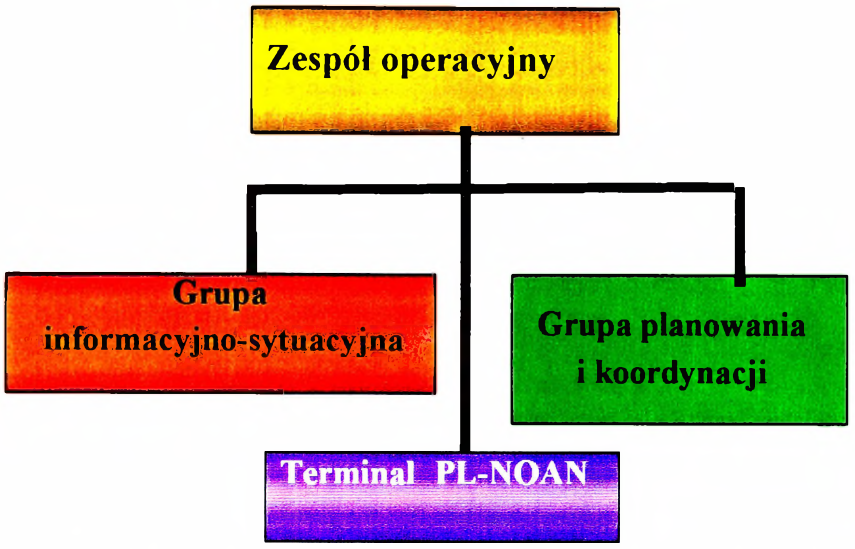
3.6. Monitorowanie informacji zawartych w publikacjach oraz audycjach prezentowanych przez krajowe i zagraniczne środki masowego przekazu.

3.7. Aktualizowanie bazy danych o stowarzyszeniach i fundacjach w zakresie możliwości wykorzystania ich potencjału do realizacji zadań w sytuacjach kryzysowych.

3.8. Koordynowanie przedsięwzięć w zakresie ochrony dóbr kultury narodowej będących w dyspozycji resortu oraz współdziałanie z ogniwami krajowego systemu reagowania kryzysowego w tej dziedzinie.

Zespół Operacyjny składa się z (rys. 2.3.4.):

- Grupy Planowania i Koordynacji;
- Grupy Informacyjno-Sytuacyjnej;
- Obsługi Terminalu PL-NOAN.



Rys.2.3.4. Struktura organizacyjna Zespołu Operacyjnego SKRK MON

W skład Zespołu wchodzą przedstawiciele: Generalnych Zarządów Sztabu Generalnego WP (za wyjątkiem Generalnego Zarządu Logistyki), Dyżurnej Służby Operacyjnej Sił Zbrojnych RP, Komendy Głównej Żandarmerii Wojskowej oraz oficerowie łącznikowi dowództw rodzajów Sił Zbrojnych.

Obowiązki Szefa Zespołu Operacyjnego pełni Szef Grupy Planowania i Koordynacji (przedstawiciel Generalnego Zarządu Operacyjnego Sztabu Generalnego WP), który podlega bezpośrednio szefowi zmiany dyżurnej.

Obowiązki szefa Grupy Informacyjno-Sytuacyjnej sprawuje przedstawiciel Generalnego Zarządu Rozpoznania Wojskowego Sztabu Generalnego WP, który podlega szefowi Zespołu.

Obowiązki operatora Terminalu PL-NOAN sprawuje przedstawiciel Generalnego Zarządu Operacyjnego Sztabu Generalnego WP, który podlega szefowi Zespołu.

Zadania Zespołu Operacyjnego

Zespół Operacyjny - przeznaczony jest do wsparcia procesu decyzyjnego Sztabu Kryzysowego MON, planowania i koordynowania działań wydzielonych sił i środków Sił Zbrojnych RP, zaangażowanych w rozwiązywanie sytuacji kryzysowych, zarówno w kraju jak i za granicą.

Do zadań Zespołu Operacyjnego należy:

- *monitorowanie i ocena sytuacji kryzysowych;*
- *zbieranie i aktualizowanie danych o stopniu gotowości sił przewidywanych do użycia;*
- *gromadzenie, przetwarzanie, przygotowywanie i dystrybucja informacji o sytuacji kryzysowej do elementów Systemu Kierowania Reagowaniem Kryzysowym MON;*
- *uaktualnianie planów lub opracowywanie propozycji użycia wojsk, stosownie do potrzeb wynikających z sytuacji kryzysowej;*
- *przygotowywanie projektów dokumentów decyzyjnych Ministra Obrony Narodowej oraz wykonawczych Szefa Sztabu Generalnego WP;*
- *przekazywanie zadań, nadzorowanie oraz koordynowanie działań sił wydzielonych do rozwiązania sytuacji kryzysowych.*

Zadania poszczególnych grup Zespołu Operacyjnego:

1) Grupa Planowania i Koordynacji przeznaczona jest do planowania i koordynowania działań Sił Zbrojnych RP zaangażowanych w realizację zadań kryzysowych, do jej zadań należy:

- *opracowywanie propozycji użycia sił i środków w celu przeciwdziałania zagrożeniom militarnym i pozamilitarnym oraz przedkładanie ich Szefowi Sztabu Kryzysowego MON;*
- *przygotowywanie projektów dokumentów wykonawczych Szefa Sztabu Generalnego WP;*
- *przekazywanie sygnałów alarmowania i powiadamiania, zarządzeń i rozkazów w ramach działań antykryzysowych;*
- *znajomość miejsc pobytu osób funkcyjnych Zespołu Kierownictwa MON oraz alarmowanie i powiadamianie ich o wprowadzeniu wyższych stanów gotowości kryzysowej;*
- *nadzorowanie i koordynowanie przedsięwzięć realizowanych przez rodzaje Sił Zbrojnych;*

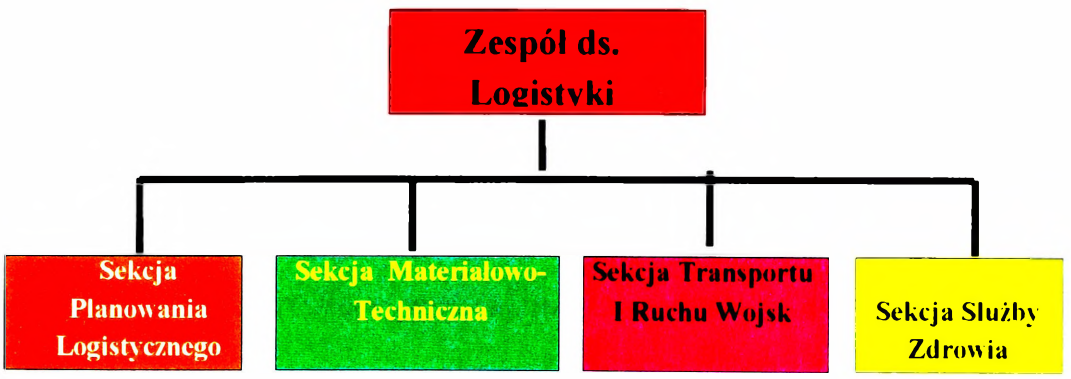
- *monitorowanie procesu osiągania wyższych stanów gotowości bojowej, mobilizacyjnego oraz operacyjnego rozwinięcia Sił Zbrojnych;*
- *współdziałanie z Krajowym Sztabem Kryzysowym, Polskim Przedstawicielem Wojskowym przy Komitecie Wojskowym Organizacji Traktatu Północnoatlantyckiego oraz Polskim Narodowym Przedstawicielem Wojskowym przy SHAPE w zakresie użycia Sił Zbrojnych RP.*

2) Grupa Informacyjno - Sytuacyjna przeznaczona jest do zbierania oraz analizowania informacji o zagrożeniach, rozwoju sytuacji kryzysowej oraz warunkach geograficznych i hydrometeorologicznych obszaru zainteresowania. Współuczestniczy on w procesie wymiany informacji z elementami Systemu Kierowania Reagowaniem Kryzysowym MON, Krajowym Sztabem Kryzysowym, Kwaterą Główną NATO i SHAPE w zakresie uaktualniania oceny zagrożeń, do jej zadań należy:

- *zdobywanie informacji o zagrożeniach związanych sytuacją kryzysową oraz ich ocena;*
- *opracowywanie wniosków z oceny warunków geograficznych i hydro-meteorologicznych obszaru zainteresowania;*
- *opracowywanie meldunku sytuacyjnego dla Szefa Sztabu Kryzysowego MON;*
- *prowadzenie mapy informacyjno - sytuacyjnej Sztabu Kryzysowego MON;*
- *przygotowywanie narad (odpraw) roboczych w Sztabie Kryzysowym MON.*

Zespół do Spraw Logistyki (rys. 2.3.5.) składa się z:

- Sekcji Planowania Logistycznego;
- Sekcji Materiałowo-Technicznej;
- Sekcji Transportu i Ruchu Wojsk;
- Sekcji Służby Zdrowia.



Rys. 2.3.5. Struktura organizacyjna Zespołu ds. Logistyki SKRK MON

W skład Zespołu wchodzą przedstawiciele Generalnego Zarządu Logistyki i Zarządu Wojskowej Służby Zdrowia Sztabu Generalnego WP. Obowiązki Szefa Zespołu do Spraw Logistyki pełni Szef Sekcji Planowania Logistycznego (przedstawiciel Generalnego Zarządu Logistyki), który podlega bezpośrednio szefowi zmiany dyżurnej.

Obowiązki pozostałych szefów sekcji sprawują:

- Sekcji Materiałowo-Technicznej – przedstawiciel Zarządu Materiałowo-Technicznego Generalnego Zarządu Logistyki Sztabu Generalnego WP, który podlega szefowi Zespołu,
- Sekcji Transportu i Ruchu Wojsk – przedstawiciel Zarządu Transportu i Ruchu Wojsk Generalnego Zarządu Logistyki Sztabu Generalnego WP, który podlega szefowi Zespołu,
- Sekcji Służby Zdrowia – przedstawiciel Zarządu Wojskowej Służby Zdrowia Sztabu Generalnego WP, który podlega szefowi Zespołu.

Zadania Zespołu do Spraw Logistyki

Zespół do Spraw Logistyki jest przeznaczony do wsparcia procesu decyzyjnego Sztabu Kryzysowego MON - w uzgodnieniu z Szefem Generalnego Zarządu Logistyki - w zakresie dotyczącym użycia systemu logistycznego Sił Zbrojnych RP w działaniach kryzysowych.

Do zadań Zespołu do Spraw Logistyki należy:

1. *Monitorowanie operacyjnych i logistycznych aspektów sytuacji kryzysowej.*
2. *Śledzenie, analizowanie i ocenianie sytuacji logistycznej sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowej.*
3. *Precyzowanie zadań logistycznych i przekazywanie ich właściwym organom kierowania*
   i dowodzenia logistyką - do niezwłocznego rozwiązania.
4. *Współdziałanie z Generalnym Zarządem Logistyki w zakresie planowania wsparcia logistycznego dla sił i środków przewidzianych (użytych) do rozwiązywania sytuacji kryzysowych.*

5. *Przygotowywanie specjalistycznych danych do meldunków i sprawozdań oraz przekazywanie ich do Grupy Informacyjno-Sytuacyjnej.*
6. *Współdziałanie z Grupą Planowania i Koordynacji w zakresie planowania i koordynowania wysiłku logistycznego.*
7. *Przedstawianie planów wsparcia logistycznego sił i środków przewidzianych (użytych) do rozwiązywania sytuacji kryzysowych, wstawek logistycznych do rozkazów oraz zarządzeń logistycznych, jeśli są wymagane.*
8. *Prowadzenie mapy sprawozdawczej (sytuacyjnej) oraz innej dokumentacji według potrzeb.*

Zadania poszczególnych sekcji Zespołu do Spraw Logistyki:

1) do zadań Sekcji Planowania Logistycznego należy:

- *gromadzenie, analizowania i opracowywanie ocen i wniosków, wynikających z monitorowania stanu kryzysowego w zakresie ogólnowojskowym, operacyjnym i logistycznym oraz przedstawianie ich Szefowi Zespołu;*
- *gromadzenie, analizowanie oraz opracowywanie ocen i wniosków, dotyczących sytuacji materiałowej, technicznej, medycznej, transportu i ruchu wojsk w odniesieniu do sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych oraz dotyczących możliwości wsparcia logistycznego w ramach HNS;*
- *klasyfikowanie i nadawanie priorytetów problemom i zadaniom wyspecyfikowanym w poszczególnych sekcjach Zespołu ds. Logistyki oraz przekazywanie ich właściwym organom kierowania i dowodzenia logistyką - do niezwłocznego rozwiązania;*
- *współdziałanie z Zarządami Generalnego Zarządu Logistyki w zakresie planowania i realizacji wsparcia logistycznego sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *przygotowywanie specjalistycznych danych do meldunków i sprawozdań oraz przedstawianie ich Szefowi Zespołu;*
- *współdziałanie z Grupą Planowania i Koordynacji w zakresie planowania i koordynowania wysiłku logistycznego;*
- *opracowywanie projektów wstawek logistycznych do rozkazów oraz zarządzeń logistycznych, jeśli są wymagane;*
- *prowadzenie logistycznej mapy sprawozdawczej (sytuacyjnej) oraz innej dokumentacji według potrzeb lub wymaganej określonymi procedurami;*
- *prowadzenie dziennika działań Zespołu do Spraw Logistyki.*

2) do zadań Sekcji Materiałowo-Technicznej należy:

- *gromadzenie, analizowanie oraz opracowywanie ocen i wniosków dotyczących sytuacji materiałowej i technicznej w odniesieniu do sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych oraz możliwości HNS w zakresie materiałowo-technicznym;*
- *aktualizowanie bazy danych o zasobach materiałowych i technicznych sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *precyzowanie zadań dotyczących zabezpieczenia (wsparcia) materiałowo-technicznego oraz przekazywanie ich do Zarządu Materiałowo-Technicznego Generalnego Zarządu Logistyki – do niezwłocznego rozwiązania;*
- *współdziałanie z Zarządem Materiałowo-Technicznym Generalnego Zarządu Logistyki w zakresie planowania i realizacji wsparcia logistycznego sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *przygotowywanie specjalistycznych danych do meldunków i sprawozdań oraz przedstawianie ich Szefowi Zespołu;*
- *współdziałanie z Grupą Planowania i Koordynacji w zakresie planowania i koordynowania wysiłku związanego z zaopatrywaniem i obsługą specjalistyczną sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *opracowywanie projektów wstawek materiałowo-technicznych do rozkazów oraz zarządzeń logistycznych, jeśli są wymagane;*
- *prowadzenie mapy sprawozdawczej o sytuacji materiałowo-technicznej oraz innej dokumentacji według potrzeb.*

3) do zadań Sekcji Transportu i Ruchu Wojsk należy:

- *gromadzenie, analizowanie oraz opracowywanie ocen i wniosków dotyczących sytuacji transportowej i ruchu wojsk w odniesieniu do sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych oraz możliwości HNS w zakresie wsparcia transportowego i ruchu wojsk;*
- *aktualizowanie bazy danych o zasobach podsystemu transportu i ruchu wojsk;*
- *precyzowanie zadań dotyczących zabezpieczenia (wsparcia) transportowego i ruchu wojsk oraz przekazywanie ich do Zarządu Transportu i Ruchu Wojsk Generalnego Zarządu Logistyki (lub Narodowego Centrum Koordynacji Transportu i Ruchu Wojsk) – do niezwłocznego rozwiązania;*

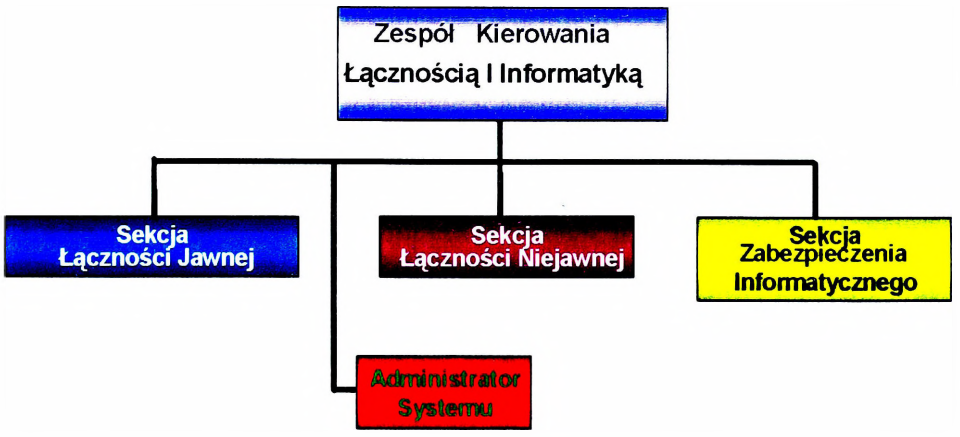
- *współdziałanie z Zarządem Transportu i Ruchu Wojsk Generalnego Zarządu Logistyki w zakresie planowania i realizacji wsparcia (zabezpieczenia) transportowego i ruchu sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *przygotowywanie specjalistycznych danych do meldunków i sprawozdań oraz przedstawianie ich Szefowi Zespołu;*
- *współdziałanie z Grupą Planowania i Koordynacji w zakresie planowania i koordynowania wysiłku związanego ze wsparciem transportowym i ruchem sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *opracowywanie projektów wstawek z zakresu wsparcia transportowego i ruchu wojsk do rozkazów oraz zarządzeń logistycznych, jeśli są wymagane;*
- *prowadzenie mapy sprawozdawczej o sytuacji transportowej i ruchu wojsk oraz innej dokumentacji według potrzeb.*

4) do zadań Sekcji Służby Zdrowia należy:

- *gromadzenie, analizowanie oraz opracowywanie ocen i wniosków dotyczących sytuacji medycznej w odniesieniu do sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych oraz możliwości HNS w zakresie wsparcia medycznego;*
- *aktualizowanie bazy danych o zasobach medycznych sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *precyzowanie zadań dotyczących zabezpieczenia (wsparcia) medycznego oraz przekazywanie ich do Zarządu Wojskowej Służby Zdrowia, celem niezwłocznego rozwiązania;*
- *współdziałanie z Zarządem Wojskowej Służby Zdrowia Generalnego Zarządu Logistyki w zakresie planowania i realizacji wsparcia (zabezpieczenia) medycznego sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *przygotowywanie specjalistycznych danych do meldunków i sprawozdań oraz przedstawianie ich Szefowi Zespołu;*
- *współdziałanie z Grupą Planowania i Koordynacji w zakresie planowania i koordynowania wysiłku związanego ze wsparciem medycznym sił i środków planowanych (użytych) do rozwiązywania sytuacji kryzysowych;*
- *opracowywanie projektów wstawek z zakresu wsparcia medycznego do rozkazów oraz zarządzeń logistycznych, jeśli są wymagane;*
- *prowadzenie mapy sprawozdawczej o sytuacji medycznej oraz innej dokumentacji według potrzeb.*

Zespół Kierowania Łącznością i Informatyką (rys. 2.3.6.) składa się z:

- Sekcji Łączności Jawnej;
- Sekcji Łączności Niejawnej;
- Sekcji Zabezpieczenia Informatycznego;
- Administratora Systemu.



Rys.2.3.6. Struktura organizacyjna Zespołu Kierowania Łącznością i Informatyką SKRK MON

W skład Zespołu wchodzą przedstawiciele Generalnego Zarządu Dowodzenia i Łączności Sztabu Generalnego WP.

Obowiązki Szefa Zespołu Kierowania Łącznością i Informatyką pełni Szef Sekcji Łączności Jawnej (przedstawiciel Zarządu Łączności i Informatyki Generalnego Zarządu Dowodzenia i Łączności), który podlega bezpośrednio szefowi zmiany dyżurnej.

Obowiązki szefów pozostałych sekcji sprawują:

- Sekcji Łączności Niejawnej – przedstawiciel Zarządu Łączności i Informatyki Generalnego Zarządu Dowodzenia i Łączności Sztabu Generalnego WP, który podlega szefowi Zespołu,
- Sekcji Zabezpieczenia Informatycznego – przedstawiciel Zarządu Łączności i Informatyki Generalnego Zarządu Dowodzenia i Łączności Sztabu Generalnego WP, który podlega szefowi Zespołu.

Zadania Zespołu Kierowania Łącznością i Informatyką

Zespół Kierowania Łącznością i Informatyką przeznaczony jest do planowania i organizowania systemu łączności i informatyki na potrzeby Sztabu Kryzysowego MON oraz koordynowania przedsięwzięciami mającymi na celu zapewnienie ich funkcjonowania.

Do zadań Zespołu Kierowania Łącznością i Informatyką należy:

1. *Koordynowanie działalności podsystemu łączności i informatyki w ramach Systemu Kierowania Reagowaniem Kryzysowym MON.*
2. *Utrzymywanie sprawności technicznej sprzętu łączności, komputerów i sieci informatycznych, będących na wyposażeniu Sztabu Kryzysowego MON.*
3. *Sprawowanie nadzoru nad funkcjonowaniem systemu wideokonferencji.*
4. *Obsługa serwera graficznego zobrazowania sytuacji.*
5. *Zabezpieczenie funkcjonowania utajnionej łączności telefonicznej i telefaksowej.*

Zadania poszczególnych sekcji Zespołu Kierowania Łącznością i Informatyką:

1) do zadań Sekcji Łączności Jawnej należy:

- *opracowanie planu systemu łączności jawnej na potrzeby Sztabu Kryzysowego MON;*
- *koordynowanie prac mających na celu zorganizowanie i funkcjonowanie systemu łączności jawnej Sztabu Kryzysowego MON;*
- *wypracowywanie i przedkładanie propozycji organizacji łączności jawnej wojsk planowanych do użycia w ramach reagowania kryzysowego.*

2) do zadań Sekcji Łączności Niejawnej należy:

- *opracowanie planu systemu łączności niejawnej na potrzeby Sztabu Kryzysowego MON;*
- *koordynowanie prac mających na celu zorganizowanie i funkcjonowanie systemu łączności niejawnej Sztabu Kryzysowego MON;*
- *wypracowywanie i przedkładanie propozycji organizacji łączności niejawnej wojsk planowanych do użycia w ramach reagowania kryzysowego.*

3) do zadań Sekcji Zabezpieczenia Informatycznego należy:

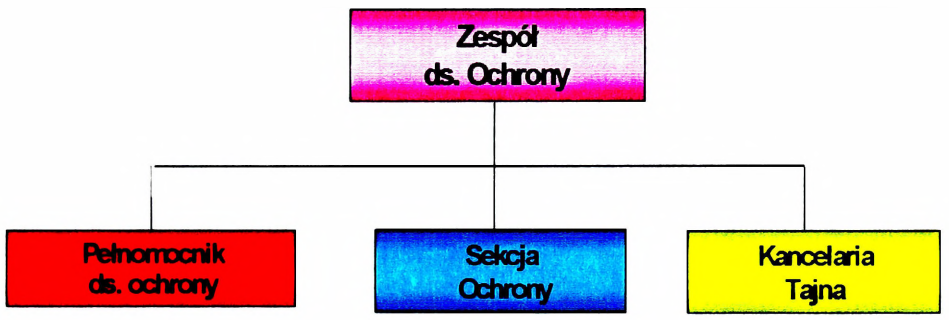
- *opracowanie planu wsparcia informatycznego na potrzeby Sztabu Kryzysowego MON;*
- *koordynowanie prac mających na celu zorganizowanie i funkcjonowanie systemu informatycznego Sztabu Kryzysowego MON.*

4 do zadań Administratora Systemu należy:

- *wdrażanie procedur bezpieczeństwa w systemach i sieci teleinformatycznej oraz nadzór nad ich przestrzeganiem zgodnie ze „Szczególnymi Wymaganiami Bezpieczeństwa" (SWB) i „Procedurami Bezpieczeństwa" (PB);*
- *aktualizowanie listy autoryzowanych użytkowników systemu i sieci teleinformatycznej;*
- *zapewnienie zgodności systemów teleinformatycznych z wymaganiami określonymi w "Szczególnych Wymaganiach Bezpieczeństwa" i „Procedurach Bezpieczeństwa";*
- *prowadzenie szkoleń i udzielanie porad użytkownikom systemów teleinformatycznych i sieci w zakresie bezpieczeństwa teleinformatycznego;*
- *aktualizowanie „Wykazu osób zapoznanych z Procedurami Bezpieczeństwa" i przekazywanie go Szefowi Zespołu ds. Ochrony;*
- *zapewnienie niszczenia odpadów niejawnych w regularnych odstępach czasu, zgodnie z obowiązującymi procedurami;*
- *nadzorowanie utrzymywania sprawności technicznej sprzętu i sieci teleinformatycznych, będących na wyposażeniu Sztabu Kryzysowego MON;*
- *prowadzenie „Dziennika przeglądów" usług serwisowych sprzętu;*
- *opracowywanie planów awaryjnych i planu napraw dla systemów i sieci teleinformatycznych;*
- *wdrażanie procedur ochrony antywirusowej;*
- *proponowanie zmian mających na celu poprawę bezpieczeństwa sieci;*
- *meldowanie o stwierdzonych naruszeniach i zagrożeniach bezpieczeństwa informacji niejawnych szefowi Zespołu ds. Ochrony.*

Zespół do Spraw Ochrony (rys.2.3.7.) składa się z:

- Sekcji Ochrony,
- Kancelarii Tajnej.



Rys.2.3.7. Struktura organizacyjna Zespołu ds. Ochrony SKRK MON

W skład Zespołu wchodzą przedstawiciele Biura Ochrony Informacji Niejawnych i Wojskowych Służb Informacyjnych.

Obowiązki Szefa Zespołu do Spraw Ochrony pełni Szef Sekcji Ochrony (przedstawiciel Biura Ochrony Informacji Niejawnych), który jest jednocześnie Pełnomocnikiem Szefa Sztabu Kryzysowego MON do Spraw Ochrony Informacji Niejawnych. Podlega on bezpośrednio szefowi zmiany dyżurnej. Kierownik Kancelarii Tajnej podlega szefowi Zespołu.

Zadania Zespołu do Spraw Ochrony

Zespół do Spraw Ochrony odpowiada za zapewnienie kompleksowej ochrony Sztabu Kryzysowego MON, w tym przestrzegania przepisów o ochronie informacji niejawnych.

Zadania Sekcji i Kancelarii Zespołu do Spraw Ochrony:

1) do zadań Sekcji Ochrony należy:

- *ochrona informacji niejawnych w Sztabie Kryzysowym MON;*
- *kontrola przestrzegania przepisów w zakresie ochrony informacji niejawnych przez komórki wewnętrzne Sztabu Kryzysowego MON;*
- *zapewnienie fizycznego bezpieczeństwa systemom i sieciom teleinformatycznym do przetwarzania informacji niejawnych;*
- *sprawowanie nadzoru nad funkcjonowaniem ochrony fizycznej Sztabu Kryzysowego MON;*
- *zorganizowanie i nadzorowanie systemu przepustkowego;*
- *przeszkalanie obsady Sztabu Kryzysowego MON w zakresie ochrony informacji niejawnych;*
- *kontrolowanie i ewidencjonowanie sprawdzeń obecności klasyfikowanych mediów magnetycznych i poprawności ich opisu.*

2) do zadań Kancelarii Tajnej należy:

- *ewidencja dokumentów zgodnie z obowiązującymi w tym zakresie przepisami;*
- *prowadzenie wykazu osób posiadających stosowne poświadczenia bezpieczeństwa umożliwiające dostęp do informacji niejawnych;*
- *udostępnianie dokumentów niejawnych osobom upoważnionym;*
- *reprodukcja niezbędnych dokumentów;*
- *doręczanie i wysyłanie dokumentów do adresatów;*
- *zapewnienie ochrony dokumentów przechowywanych w kancelarii;*

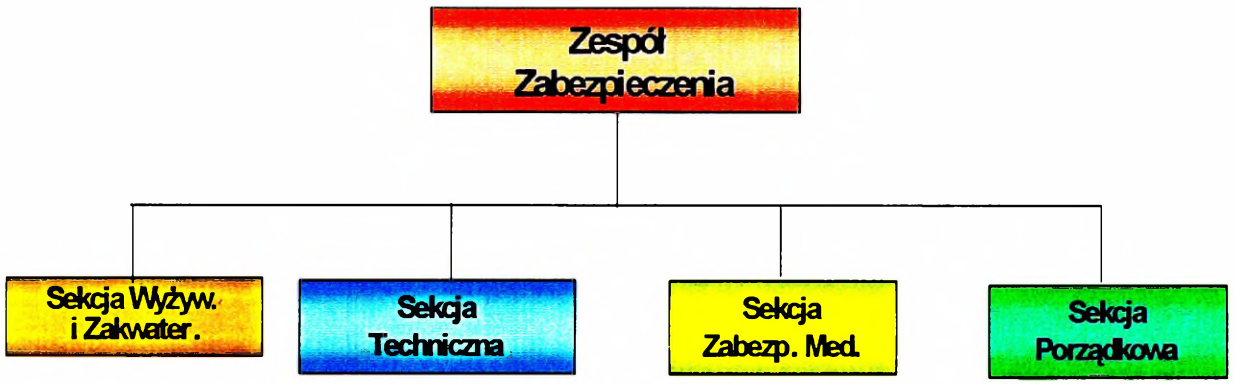
• *prowadzenie bieżącej kontroli wykonawców w zakresie wytwarzania oraz postępowania z materiałami zawierającymi informacje niejawne;*

• *rozliczanie wykonawców z wytworzonych przez nich dokumentów w Sztabie Kryzysowym MON;*

• *kompletowanie i archiwizacja dokumentów.*

Zespół Zabezpieczenia składa się z:

- Sekcji Technicznej,
- Sekcji Wyżywienia i Zakwaterowania,
- Sekcji Zabezpieczenia Medycznego,
- Sekcji Porządkowej.



Rys. 2.3.8. Struktura organizacyjna Zespołu Zabezpieczenia SKRK MON

W skład Zespołu wchodzą przedstawiciele Dowództwa Garnizonu Warszawa.

Obowiązki Szefa Zespołu Zabezpieczenia pełni Szef Sekcji Technicznej (przedstawiciel Oddziału Zabezpieczenia Sztabu Generalnego WP), który podlega bezpośrednio szefowi zmiany dyżurnej.

Obowiązki szefów pozostałych sekcji sprawują:

• Sekcji Wyżywienia i Zakwaterowania – przedstawiciel Oddziału Zabezpieczenia Sztabu Generalnego WP, który podlega szefowi Zespołu,

• Sekcji Zabezpieczenia Medycznego – lekarz dyżurny Ambulatorium Jednostki Wojskowej Nr 2063, który podlega szefowi Zespołu,

• Sekcji Porządkowej – przedstawiciel Oddziału Zabezpieczenia Sztabu Generalnego WP, który podlega szefowi Zespołu.

Zadania Zespołu Zabezpieczenia

Zespół Zabezpieczenia przeznaczony jest do zapewnienia funkcjonowania Sztabu Kryzysowego MON.

Zadania poszczególnych sekcji Zespołu Zabezpieczenia:

1) do zadań Sekcji Technicznej należy:

- *przygotowywanie pomieszczeń oraz miejsc pracy dla osób funkcyjnych Sztabu Kryzysowego MON;*
- *przygotowywanie miejsc odpraw i wyposażenie ich w niezbędne środki audiowizualne;*
- *wydzielanie środków transportu dla potrzeb Sztabu Kryzysowego MON.*

2) do zadań Sekcji Wyżywienia i Zakwaterowania należy:

- *zabezpieczenie wyżywienia obsady Sztabu Kryzysowego MON;*
- *zabezpieczanie miejsc odpoczynku dla wybranego personelu.*

3) do zadań Sekcji Zabezpieczenia Medycznego należy zapewnienie opieki lekarskiej stanowi osobowemu Sztabu Kryzysowego MON.

4) do zadań Sekcji Porządkowej należy utrzymywanie właściwego stanu higieniczno-sanitarnego oraz zapewnienie bezpieczeństwa przeciwpożarowego w pomieszczeniach Sztabu Kryzysowego MON.

3. RELACJE INFORMACYJNE W SYSTEMIE REAGOWANIA KRYZYSOWEGO

płk dr hab. inż. Józef Władysław MICHNIAK

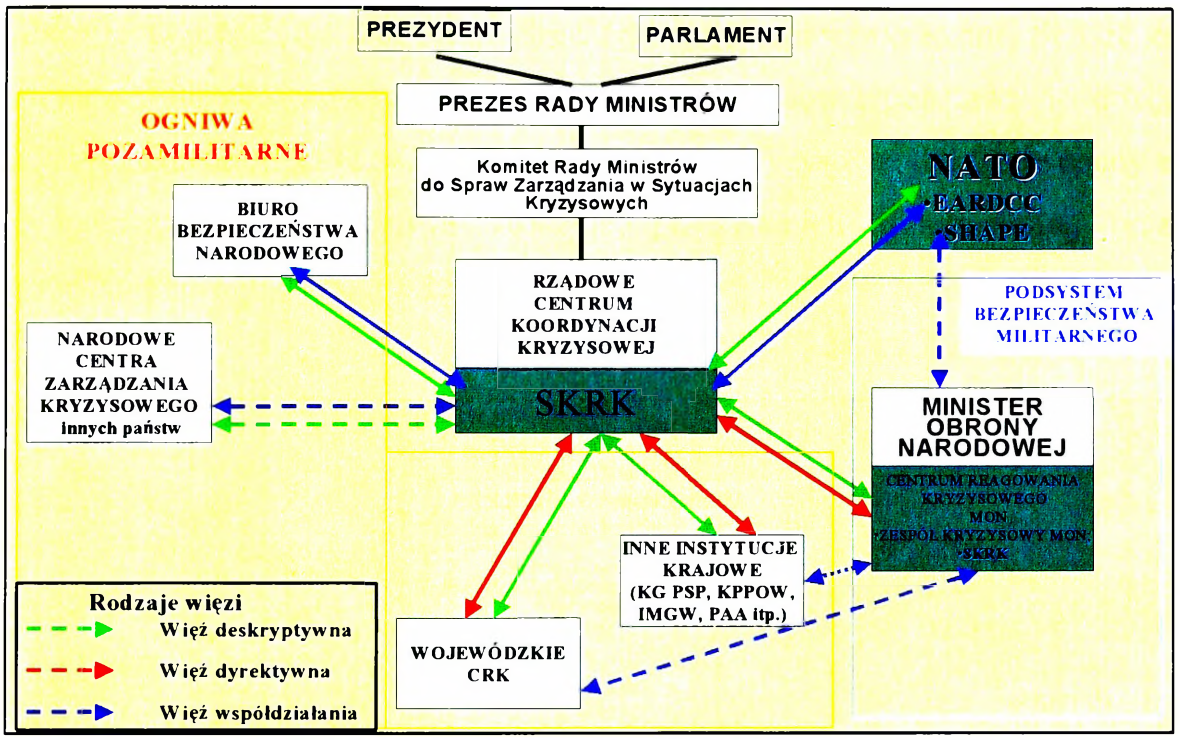
3.1. Relacje informacyjne Systemu Reagowania Kryzysowego Ministerstwa Obrony Narodowej (SRK MON) z otoczeniem (zasilanie informacyjne systemu)

System bezpieczeństwa państwa polskiego, zwany również krajowym systemem bezpieczeństwa jest kompleksem wydzielonych sił i środków, ujętych w określone struktury organizacyjne oraz przewidziane ustawowo procedury niezbędne do zapewnienia bezpieczeństwa państwa i narodu w aspekcie zewnętrznym i wewnętrznym, w obliczu zarówno zagrożeń militarnych jak i niemilitarnych. Zarówno procedury jak i organizacje tego systemu zapewniają wymianę informacji w poszczególnych więziach informacyjnych.

Krajowy system bezpieczeństwa składa się przede wszystkim z sił militarnych odpowiedzialnych za zewnętrzne bezpieczeństwo państwa (podsystem bezpieczeństwa militarnego (PBM) oraz siły i środki niemilitarne (cywilne), odpowiedzialne za wewnętrzne bezpieczeństwo państwa (podsystem bezpieczeństwa cywilnego – PBC). Istotną rolę, szczególnie w fazie przedkryzysowej i wczesnego rozwoju kryzysu będą odgrywały oddziaływania polityczno – militarne. Jak określono to wcześniej podsystem bezpieczeństwa militarnego który scala system reagowania kryzysowego MON obejmujący swym zasięgiem wszystkie systemy wspomagania dowodzenia wchodzące w skład dowództw w pionie powoływanego Dowództwa Połączonego jak też Wojewódzkie Sztaby Wojskowe i bazy zaopatrzenia. Elementem łączącym System Reagowania Kryzysowego MON (w ramach którego poprzez dyżurną służbę operacyjną prowadzony jest między innymi stały monitoring ewentualnych zagrożeń) z podsystemem bezpieczeństwa cywilnego jest Centrum Reagowania Kryzysowego MON które w więzi deskryptywnej przekazuje meldunki sytuacyjne z podsystemu bezpieczeństwa militarnego do Rządowego Centrum Koordynacji Kryzysowej. W tej samej więzi CRK MON otrzymuje oceny ze wszystkich elementów podsystemu bezpieczeństwa cywilnego.

Stanowisko Kierowania Reagowaniem Kryzysowym (SKRK) stanowi główny komponent systemu informacyjnego dla sztabów kryzysowych, zabezpieczający funkcjonalne

wspomagania wykonywania zadań z zakresu reagowania kryzysowego na szczeblu MON i jest powiązany informacyjnie z niższymi szczeblami systemu Reagowania Kryzysowego oraz systemami kryzysowymi innych państw współpracujących (zarówno w ramach sojuszu jak i PdP). Dlatego też SKRK jest lokalną siecią zautomatyzowanych stanowisk pracy oraz serwerów (tzw. struktura techniczna) obsługiwanych przez System Informatyczny SKRK (tzw. struktura programowa), który zabezpiecza i wspomaga efektywne wykonywania zadań przez personel SKRK.

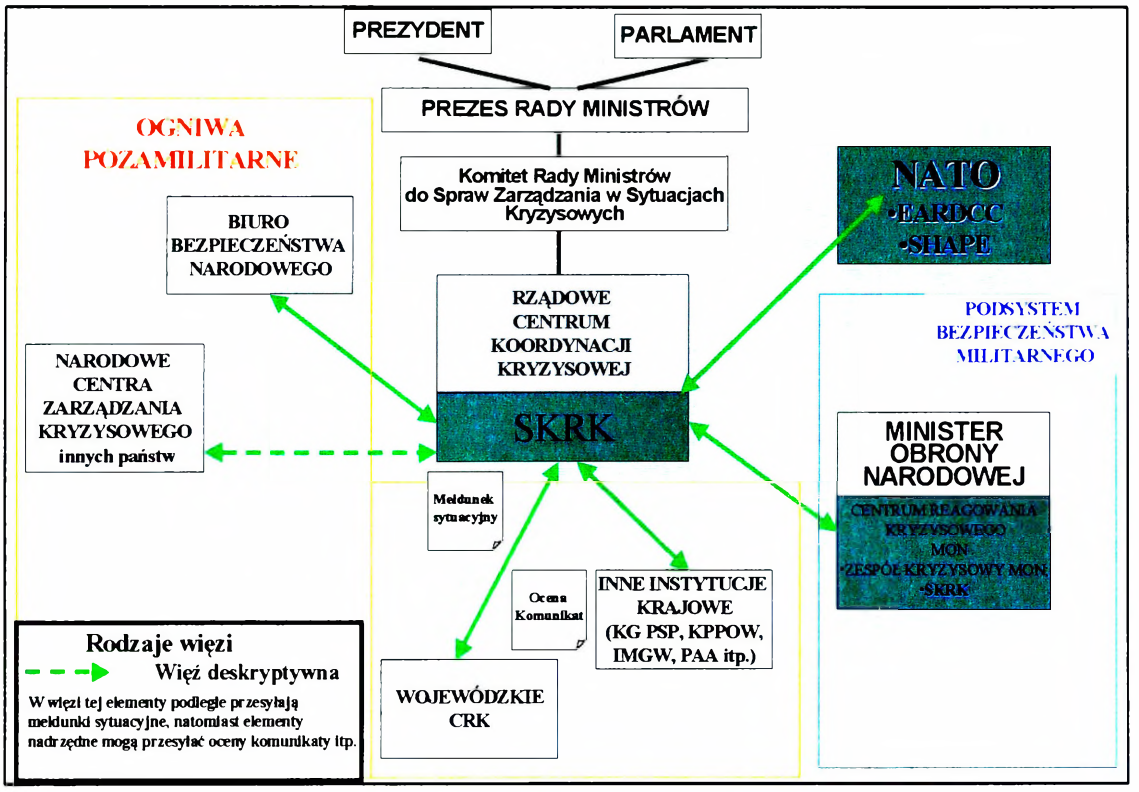


Rys. 3.1.1. Więzi informacyjne SRK MON z otoczeniem

3.2. Rodzaje informacji w poszczególnych rodzajach więzi informacyjnych Systemu Reagowania Kryzysowego Ministerstwa Obrony Narodowej (SRK MON) z otoczeniem (zasilanie informacyjne systemu)

3.2.1. Więź deskryptywna

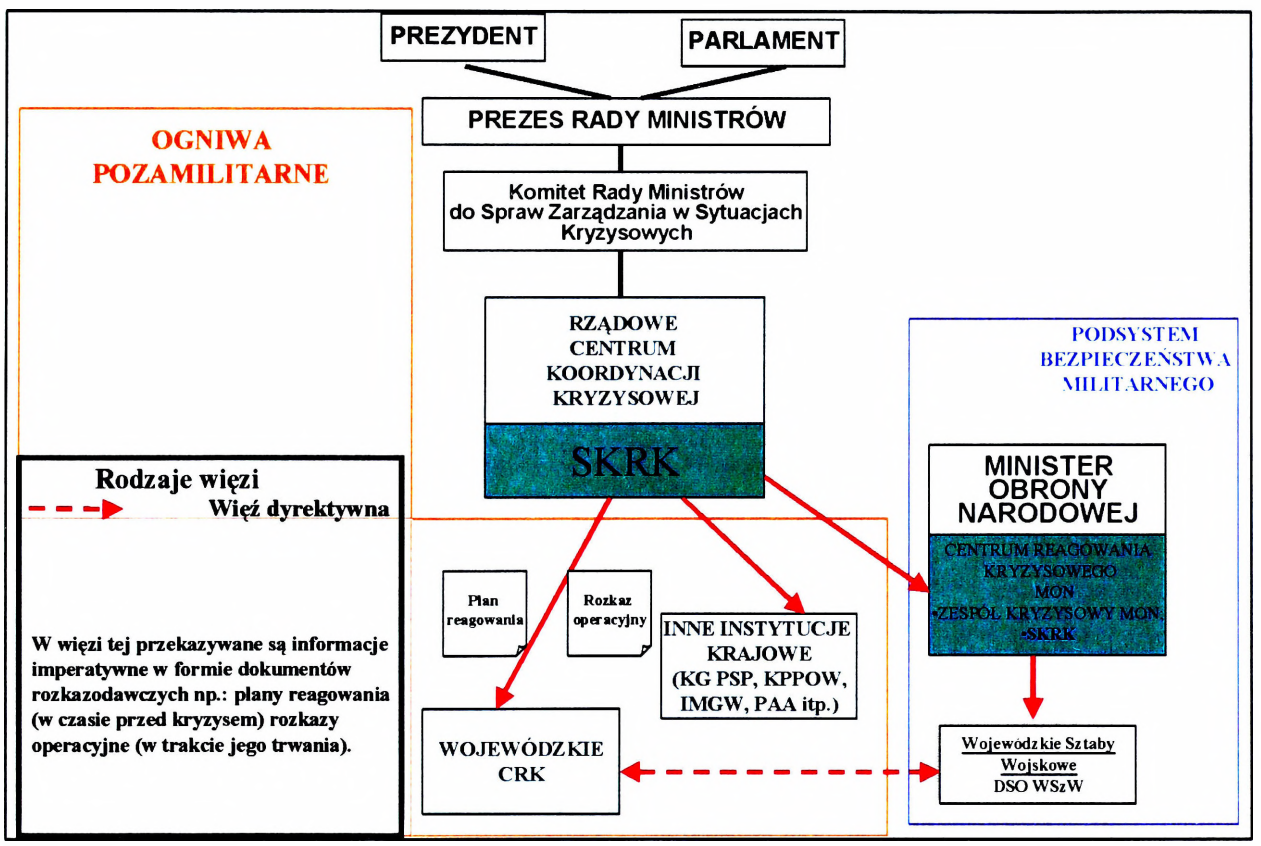
Więzią tą przesyłane są informacje sytuacyjne, opisowe. Przede wszystkim w formie meldunków sytuacyjnych, które przesyłane są w obu podsystemach tzn. PBC i PBM do centrów reagowania kryzysowego w ramach prowadzonego monitoringu. W PBM meldunki te przesyłane są poprzez Dyżurną Służbę Operacyjną do części operacyjnej SKRK, meldunki te pozwalają na bieżąco prowadzić oceny zagrożeń i stanowią podstawę do dokonywania analiz na tej podstawie Rządowe Centrum Koordynacji Kryzysowej dokonuje oceny zagrożeń systemu bezpieczeństwa państwa. Rodzaje przesyłanych dokumentów oraz więzi deskryptywne przedstawia rys. 3.2.1.



Rys. 3.2.1. Więzi deskryptywne SRK i SRK MON

3.2.2. Więź dyrektywna

W przypadku zaistnienia sytuacji kryzysowej i konieczności podania jej rozwiązania, dokonuje się tego poprzez więź dyrektywną, gdyż ta więź służy do przekazywania informacji imperatywnej opracowywanej w formie dokumentów rozkazodawczych takich jak Rozkaz Operacyjny – który jest opracowany na podstawie planu reagowania. Więź ta zasadniczo łączy elementy jednego z podsystemów, jednak w pewnych sytuacjach może łączyć elementy obu podsystemów na różnych poziomach w zależności od charakteru kryzysu (militarny czy też niemilitarny) oraz od tego kto tzn. który z poziomów kieruje podjętym działaniem (tzn.: czy sytuacja wymaga podjęcia działania na szczeblu krajowym, resortowym, czy też może tylko na szczeblu regionalnym – wojewódzkim). Rodzaje przesyłanych dokumentów oraz więzi deskryptywne przedstawia rys.3.2.2.

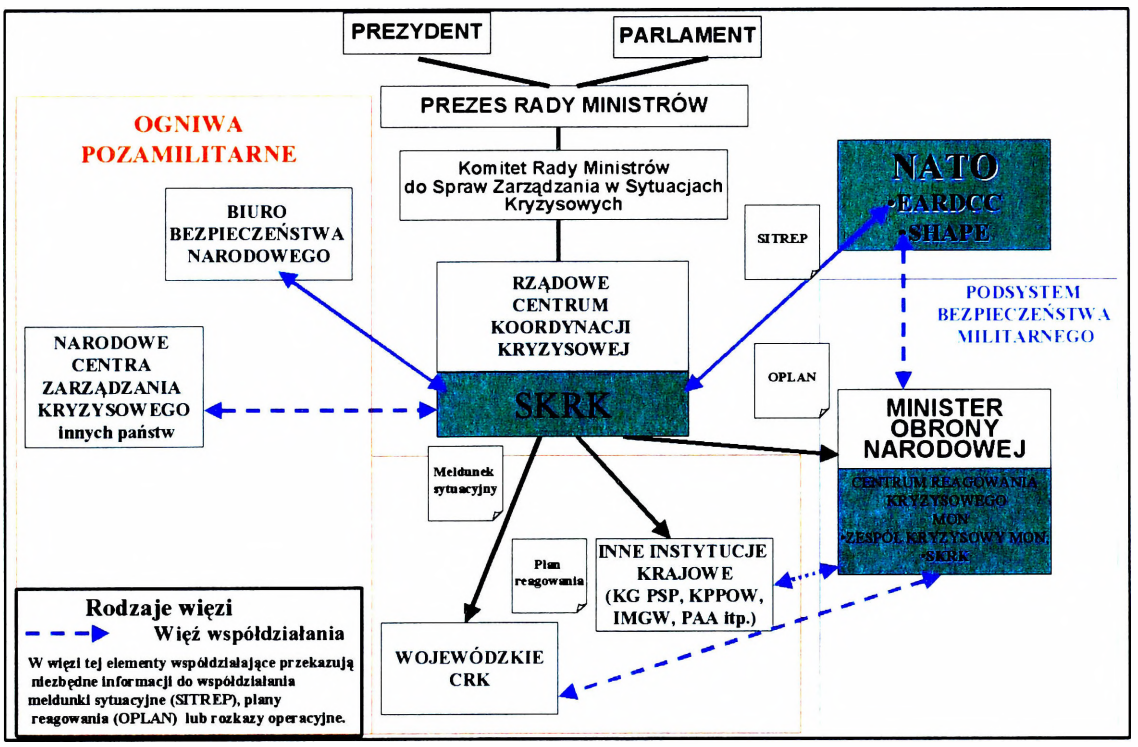


Rys. 3.2.2. Więzi dyrektywna SRK i SRK MON

3.2.3. Więź współdziałania

W trakcie rozwiązywania sytuacji kryzysowych, oraz w okresie zapobiegania sytuacjom kryzysowym, zarówno elementy obu podsystemów bezpieczeństwa wewnętrznego, jak i cały system bezpieczeństwa państwa może współdziałać z elementami zewnętrznymi zarówno
w ramach NATO, jaki z państwami z PdP w rozwiązywaniu sytuacji kryzysowych. Z tego celu służy więź współdziałania, którą mogą być przesyłane wszystkie niezbędne informacje w następującej formie: w formie dokumentów informacyjnych np.: meldunków sytuacyjnych, w których można przekazać informację o zaistniałym zagrożeniu oraz podjętym działaniu; w formie dokumentów planistycznych np.: planu reagowania w trakcie przygotowywania się do rozwiązania sytuacji kryzysowej; w formie dokumentów rozkazodawczych np.: Rozkaz Operacyjny, w którym zawarte są wszystkie niezbędne informacje dotyczące podjętego przez nas sposobu rozwiązanie danej sytuacji kryzysowej.

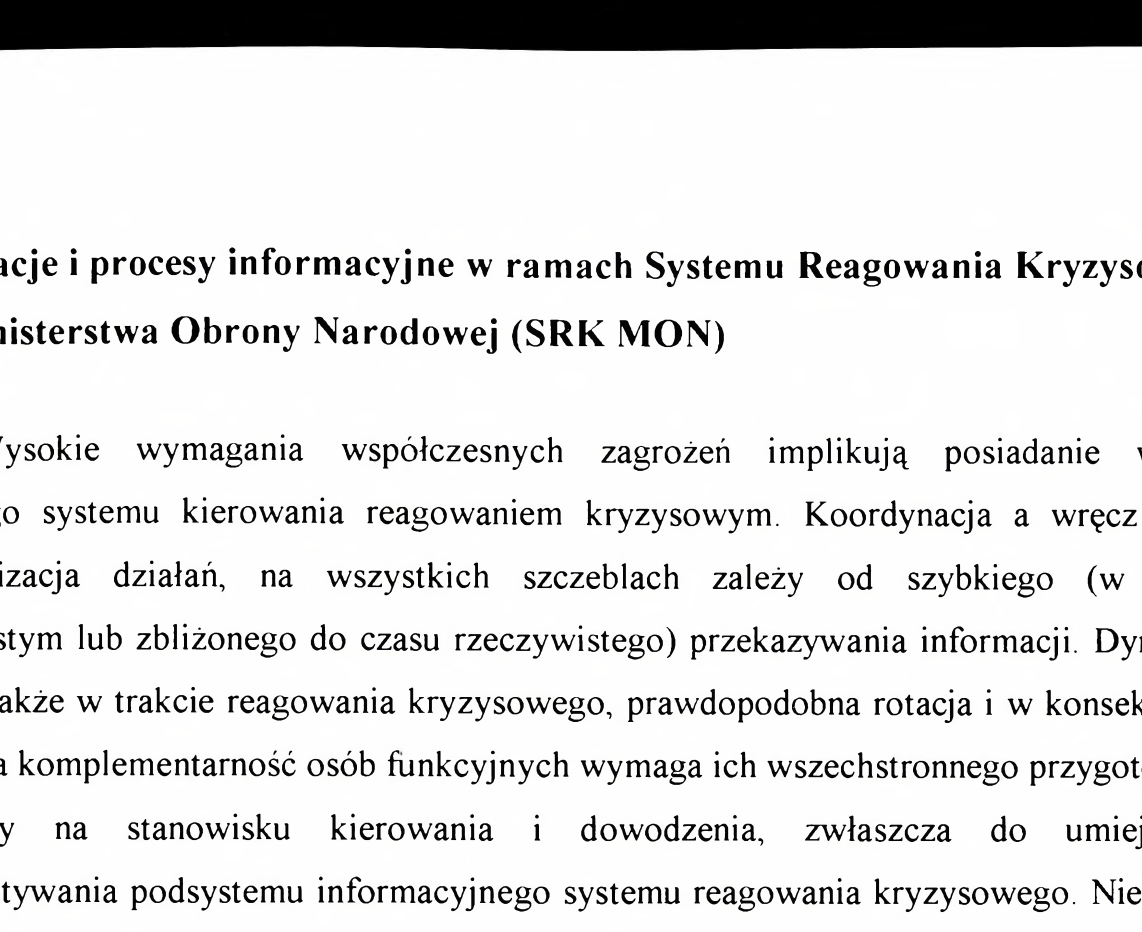
Rodzaje przesyłanych dokumentów oraz więzi deskryptywne przedstawiono na rys. 3.2.3.



Rys. 3.2.3. Więzi współdziałania SRK i SRK MON

3.3. Relacje i procesy informacyjne w ramach Systemu Reagowania Kryzysowego Ministerstwa Obrony Narodowej (SRK MON)

Wysokie wymagania współczesnych zagrożeń implikują posiadanie wysoce sprawnego systemu kierowania reagowaniem kryzysowym. Koordynacja a wręcz nawet synchronizacja działań, na wszystkich szczeblach zależy od szybkiego (w czasie rzeczywistym lub zbliżonego do czasu rzeczywistego) przekazywania informacji. Dynamika działań, także w trakcie reagowania kryzysowego, prawdopodobna rotacja i w konsekwencji wzajemna komplementarność osób funkcyjnych wymaga ich wszechstronnego przygotowania do pracy na stanowisku kierowania i dowodzenia, zwłaszcza do umiejętnego wykorzystywania podsystemu informacyjnego systemu reagowania kryzysowego. Niezbędna jest więc standaryzacja procesów przetwarzania i przekazywania informacji, w tym także standaryzacja postaci (form) przekazywanych informacji (zarówno w postaci dokumentów dowodzenia – przekazywanych w więzi dyrektywnej, jak też dokumentów przekazywanych w więzi deskryptywnej.



Rys.3.3.1. Więzi informacyjne SRK MON

Drugim czynnikiem wymuszającym standaryzację postaci informacji jest stały wzrost jej ilości i szybkości przekazywania. Przekazywanie coraz większych ilości informacji przez techniczne środki łączności o ograniczonych parametrach transmisyjnych jest możliwe, gdy „stałe elementy" informacji będą mogły być pominięte.

Istotna jest także możliwość wykorzystania „standardowych" informacji w procesie informatycznego wspomagania decyzji. Jest to szczególnie istotne przy wymaganej coraz większej wiedzy specjalistycznej i zróżnicowanych potrzebach na informację poszczególnych grup i osób funkcyjnych.

Standaryzacja dokumentów w procesie reagowania kryzysowego jest, więc niezbędnym czynnikiem sprawnego obiegu informacji.

Dokumenty opracowywane w trakcie reagowania kryzysowego w zależności od ich miejsca i roli w procesie wypracowywania decyzji, a także przyjętego kryterium można podzielić na różne grupy lub kategorie. Jednak trudno w tym przypadku przyjąć do klasyfikacji tych dokumentów tylko rodzaj informacji która jest przekazywana. Związane jest to z ogólnym przeznaczeniem dokumentów, gdyż ze względów pragmatyki procesu dowodzenia dokumenty, które w jego trakcie są wypracowywane najczęściej łączą w sobie różne rodzaje informacji. Dlatego, pomimo że ogólnie rzecz biorąc dokumenty przekazywane w więzi dyrektywnej przede wszystkim przekazują informacje imperatywne dla podwładnych, to trudno byłoby zaliczyć te dokument do dokumentów przekazujących tylko tę informację. Z tego też względu do przedstawienia podziału dokumentów wykorzystywanych w trakcie reagowania kryzysowego należałoby powrócić w następnych badaniach.

4. SYSTEM ŁĄCZNOŚCI KRAJU

ppłk dr inż. Zbigniew FIOŁNA

Zapewnienie sprawnego kierowania reagowaniem kryzysowym wymaga istnienia technicznych środków przekazywania informacji pomiędzy poszczególnymi organami reagowania kryzysowego na każdym szczeblu. Analiza sytuacji kryzysowych, które zaistniały w ostatnich latach na obszarze kraju (np. powodzie na Śląsku, w Trójmieście, na Podkarpaciu) jak i kryzysów w innych państwach (konflikty etniczne na Bałkanach, zamachy terrorystyczne we Francji i Hiszpanii, powódź w Czechach) potwierdza praktycznie najistotniejsze czynniki w walce z kryzysem – informację i jej terminową dystrybucję do organów decyzyjnych oraz wykonawczych. Niezbędne jest utrzymywanie łączności pomiędzy ośrodkami centralnymi administracji państwowej, wojewódzkimi, powiatowymi i gminnymi zespołami reagowania kryzysowego (tymi, których bezpośrednio lub pośrednio dotyczą działania antykryzysowe), zespołami kierującymi służbami publicznymi oraz grupami zadaniowymi w terenie objętym kryzysem. Istotnym zatem elementem systemu reagowania kryzysowego jest podsystem łączności.

Jednocześnie należy zauważyć, że normalnie funkcjonujące i spełniające swoje zadania systemy łączności, na obszarze objętym kryzysem są często niszczone przez antagonistyczne strony (Bałkany) lub przez żywioł (Śląsk, Czechy), przy czym wielkość tych zniszczeń lub uszkodzeń jest trudna do przewidzenia i może obejmować nawet większość istotnych dla funkcjonowania systemu łączności obiektów na całym, objętym kryzysem obszarze.

Celowe zatem jest tworzenie i utrzymywanie w ciągłej gotowości (a przynajmniej w sytuacjach zagrożenia kryzysem) odrębnego systemu łączności dla potrzeb reagowania kryzysowego. Jednakże utrzymywanie takiego wyodrębnionego systemu jest nieefektywne z wielu powodów:

- system łączności utrzymywany wyłącznie dla celów reagowania kryzysowego nie służy celom komercyjnym, więc koszty jego utrzymania ponosi wyłącznie państwo;
- brak możliwości wcześniejszego określenia lokalizacji i zasięgu potencjalnego kryzysu wymusza stworzenie systemu ogólnokrajowego a więc kosztownego;

- niekomercyjność systemu powoduje a) brak konkurencji, b) brak dochodów, co oznacza małe motywacje i małe możliwości modernizacji systemu, a więc szybkie jego starzenie (techniczne i technologiczne);
- istnienie takiego systemu może spowodować nieuzasadnione zwiększenie poczucia bezpieczeństwa i „odporności na kryzys";
- w przypadku kryzysu będącego skutkiem konfliktu grup społecznych, terroryzmu itp., taki system będzie jednym z pierwszych obiektów obezwładnianych lub niszczonych (przewrót w Rumunii, konflikt Bałkański), co przy prawdopodobnym jego stanie technicznym (powody wyżej wymienione) może uczynić go bezużytecznym.

Uzasadnione jest zatem (co zostanie przedstawione w rozdziale 5) maksymalne wykorzystanie na potrzeby reagowania kryzysowego komponentów systemu łączności kraju, wspomaganych elementami mobilnych systemów łączności służb publicznych i mobilnego podsystemu łączności utworzonego dla potrzeb reagowania kryzysowego. Wymaga to analizy struktury systemu łączności kraju, jego kompatybilności z systemami łączności służb publicznych i możliwości wyodrębnienia z jego zasobów technicznych i usługowych części niezbędnej, w określonym czasie i obszarze, dla potrzeb reagowania kryzysowego.

4.1. Struktura systemu łączności kraju

W strukturze systemu łączności kraju można wyodrębnić dwa, technicznie odrębne komponenty: system pocztowy i system telekomunikacyjny[1].

4.1.1. System łączności pocztowej

System łączności pocztowej stanowi jeden z podstawowych elementów systemu łączności państwa. Jego głównym zadaniem jest zapewnienie odbioru, dystrybucji i dostarczanie przesyłek pocztowych.

Obecny system pocztowy tworzą dwa zasadnicze komponenty. Są to: sieć usług pocztowych o charakterze powszechnym - reprezentowanym przez Państwowe Przedsiębiorstwo Użyteczności Publicznej „Poczta Polska" oraz sieć usług komercyjnych,

[1] Kolejność wymienienia systemów łączności odzwierciedla ich kolejność „historyczną" a nie możliwości usługowe czy też wielkość obsługiwanego rynku usług łączności.

głównie kurierskich, reprezentowanych przez licencjonowane firmy świadczące usługi kurierskie {Serwisco, DHL i inne).

Analizując przydatność usług systemu pocztowego dla potrzeb kierowania reagowaniem kryzysowym można stwierdzić, że pomimo dużych możliwości wykorzystania tego systemu, celowość korzystania z usług pocztowych (opóźnienia w procesie przekazywania informacji, konieczność fizycznego dotarcia do adresata) jest znikoma (zasadna jest w tych przypadkach, gdy inne systemy nie funkcjonują, ale w takich sytuacjach efektywniejsze będzie wykorzystanie własnych kurierów). Stąd też w dalszych badaniach analiza struktury komponentów systemu pocztowego i ich możliwości usługowych została pominięta.

4.1.2. System telekomunikacyjny kraju

System telekomunikacyjny to urządzenia i linie telekomunikacyjne, zorganizowane według określonych zasad oraz współpracujące ze sobą i służące do nadawania, przenoszenia i odbioru informacji (mowy, dźwięków, znaków pisma, obrazów ruchomych i nieruchomych oraz wszelkich innych postaci) za pomocą sygnałów (elektrycznych, elektromagnetycznych). Przyjmując za kryterium wyodrębnienia elementów z systemu telekomunikacyjnego rodzaj realizowanych zadań – to wówczas podstawowymi elementami systemu telekomunikacyjnego będą:

- elementy podsystemu kierowania – organa kierowania systemem telekomunikacyjnym (zarządzania, sterowania) rozmieszczone w punktach kierowania, posiadające łączność ze wszystkimi elementami systemu i z otoczeniem (środowiskiem).[2] Aktualnie, na szczeblu państwa, najwyższym elementem podsystemu kierowania jest Urząd Regulacji Telekomunikacji i Poczty. Na szczeblu poszczególnych podmiotów telekomunikacyjnych[3] są to zarządy i dyrekcje spółek telekomunikacyjnych (lub równorzędne organy). Występujące niżej w hierarchii elementy podsystemów kierowania są w poszczególnych podmiotach telekomunikacyjnych zróżnicowane;
- elementy podsystemu przekazywania informacji zorganizowane w sieci telekomunikacyjne – zespoły linii teletransmisyjnych, urządzeń telekomutacyjnych

[2] Wyodrębnienie elementów podsystemu kierowania ma istotne znaczenie dla określenia ich zakresu kompetencji i zadań w sytuacjach kryzysowych.
[3] Osób prawnych, które uzyskały z URTiP zezwolenie na działalność telekomunikacyjną lub wykonują taką działalność bez zezwolenia URTiP na mocy ustawy „Prawo Telekomunikacyjne".

(central), urządzeń przetwórczych oraz innych urządzeń – przeznaczonych do świadczenia usług telekomunikacyjnych; a więc ten element (scharakteryzowany poniżej) realizuje cel istnienia systemu;

- elementy podsystemu zasilania – elementy szeroko pojętego zabezpieczenia logistycznego oraz odwodu sił i środków systemu telekomunikacyjnego[4] decydujące o ciągłości i terminowości świadczenia usług telekomunikacyjnych.

Elementy podsystemu przekazywania informacji występujące jako sieci telekomunikacyjne są wielkimi systemami[5] o złożonej strukturze, zmiennej w czasie i przestrzeni, składającej się z wielu elementów wzajemnie od siebie uzależnionych. W praktycznie każdym przypadku sieć telekomunikacyjną należy rozpatrywać jako twór (system) złożony z przestrzennie rozłożonych urządzeń technicznych w konfiguracji sieciowej – tworzących węzły i połączenia między-węzłowe. Każda sieć charakteryzuje się następującymi zasadniczymi cechami systemowymi:

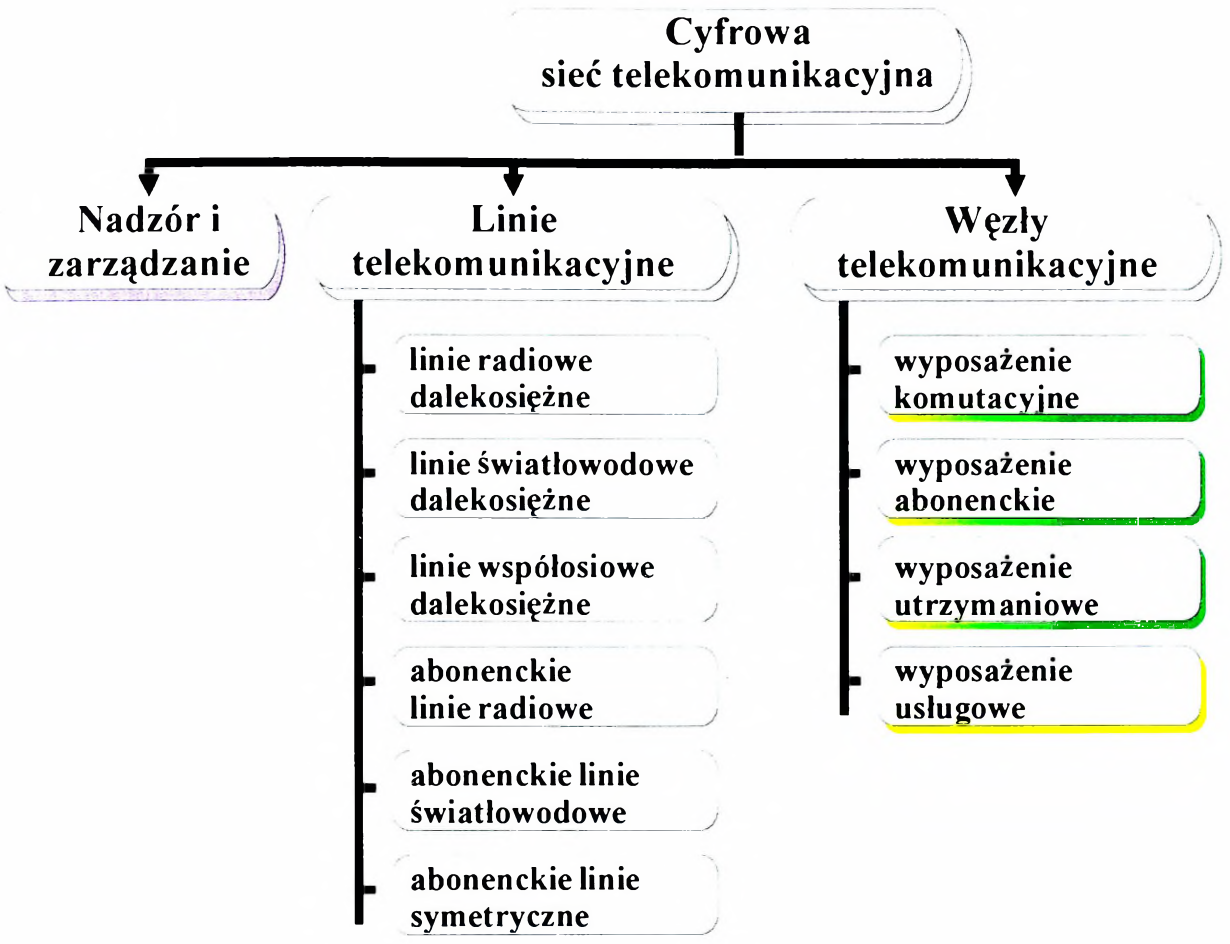
- topologią – strukturą;
- przepustowością – maksymalnym przepływem gałęziowym;
- przepływnością – obciążeniem sieci – chwilową wartością strumienia ruchu telekomunikacyjnego na określonych trasach tych strumieni;
- niezawodnością strukturalną – trwałością, zdolnością sieci do zapewnienia niezakłóconej pracy przy wszystkich (przypadkowych i celowych) oddziałujących czynnikach.

W systemie telekomunikacyjnym Polski można przyjąć, że w obszarze świadczenia usług telekomunikacji porozumiewawczej (dwukierunkowej np.: telefonia), występuje praktycznie (poza niewielkimi rejonami o przestarzałej infrastrukturze) pełna cyfryzacja i integracja techniczna i usługowa sieci. Natomiast w systemach radiokomunikacyjnych (szczególnie radiodyfuzyjnych, np.: radiofonii publicznej) stosowane są zarówno systemy analogowe (różnych generacji technicznych) jak i cyfrowe. Przykładową, ogólną strukturę cyfrowej sieci telekomunikacyjnej przedstawia rys. 4.1.2.1.

---

[4] W systemie telekomunikacyjnym elementy podsystemu zasilania są niekiedy trudne do wyodrębnienia, gdyż np. niektóre elementy odwodu (wyposażenie rezerwowe i elementy nadmiarowe) są zintegrowane z elementami roboczymi systemu.

[5] Są to odrębne lub współdziałające systemy sieci telekomunikacyjnych różniących się np. techniką przesyłania sygnałów, zakresem świadczonych usług telekomunikacyjnych, rodzajem wykorzystywanych sygnałów itp.



Rys.4.1.2.1. Ogólna struktura cyfrowej sieci telekomunikacyjnej

W skład systemu telekomunikacyjnego państwa wchodzą następujące sieci:

- sieci telekomunikacyjne użytku publicznego tj. sieci służące do wykonywania usług telekomunikacyjnych o charakterze powszechnym;
- wewnętrzne sieci telekomunikacyjne tj. sieci założone i używane wyłącznie do zaspokajania własnych potrzeb operatora sieci.

W Polsce działa wiele typów sieci telekomunikacyjnych o charakterze publicznym:

- komutowane sieci telefoniczne PSTN (Public Switched Telephone Network);
- teledacyjne sieci z komutacją kanałów CSPDN (Curcuit Switched Public Data Network);
- teledacyjne sieci z komutacją pakietów PSPDN (Public Switched Packed Data Network);
- radiotelefoniczne sieci komórkowe MT (Mobile Telephony);
- sieci wydzielone o charakterze lokalnym lub prywatnym (PABX, LAN, dyspozytorskie, specjalne).

W krajowej sieci telefonicznej PSTN funkcjonują następujące systemy komutacji (analogowej i cyfrowej):

- system Strowgera (pojedyncze egzemplarze a więc system praktycznie w zaniku);
- system krzyżowy (Pentaconta 1000C, K66, LNI) – także w zaniku;
- system elektroniczny I generacji (E-10A, E-10B) – nie rozbudowywany;
- nowoczesne systemy komutacji cyfrowej;
- Alcatel 1000 S12;
- Lucent Technologies 5ESS-2000;
- Siemens EWSD;
- krajowe: DGT 3450, ACT-6000;
- oraz wiele innych.

Działają one na wszystkich warstwach sieci telekomunikacyjnej, w tym na poziomie łączy międzynarodowych, central międzymiastowych, central okręgowych i zespolonych.

Sieć użytku publicznego - to sieć charakteryzująca się przede wszystkim dużą różnorodnością zainstalowanego w niej sprzętu: od przestarzałych systemów analogowych do systemów cyfrowych, od systemów przewodowych po systemy radiowe itp. Przykładem tego jest ilość rodzajów łączy telekomunikacyjnych, jaką przedstawiono w tabeli 4.1.2.1.

Tabela 4.1.2.1.

Rodzaje łączy telekomunikacyjnych i ich cechy użytkowe

Parametr	Rodzaj łącza	Główne cechy użytkowe
Rodzaj transmisji	analogowe	Przenoszenie ciągłego sygnału analogowego w całym dostępnym paśmie częstotliwości.
	cyfrowe	Transmisja sygnału w postaci cyfrowej. W porównaniu do łącza analogowego znacznie wyższa odporność na zakłócenia.
Sposób realizacji	komutowane	Jest zestawiane przez system komutacyjny wyłącznie na czas trwania rozmowy lub usługi. Kontrolę nad zestawieniem, utrzymaniem i rozłączeniem realizują centrala telefoniczna lub system komutacji. Możliwość transmisji danych.

Sposób realizacji	dzierżawione (trwałe i okresowe)		Linie dzierżawione są najlepszym rozwiązaniem w sytuacji, gdy ruch odbywa się stale, cechują się dużą przepustowością, a każde żądanie transmisji jest obsługiwane bezzwłocznie. Opłacalne tylko przy dużym trafiku (generowanym ruchu). Większa szybkość niż łączy komutowanych, przy niższej stopie błędów - co wynika z omijania pól komutacyjnych w centralach tranzytowych. Trasy i punkty końcowe są ustalane czasowo lub na stałe z wyprzedzeniem realizacji połączeń.
Charakter medium transmisyjnego	kablowe	przewodowe	Powszechnie stosowane medium miedziane znane jako: linia napowietrzna, kabel prosty, skrętka, podwójna skrętka, kabel wielożyłowy, kabel współosiowy. Typowy zakres przenoszenia od 0 do kilkudziesięciu MHz.
		światłowodowe	Oferta najwyższych przepływności binarnych opartych na włóknach optycznych jedno- i wielomodowych. Maksymalna przepływność jednostkowa powyżej kilkudziesięciu Gbit/s·km.
		hybrydowe	Połączenie „miedzianej" i „optycznej" technologii przekazu z przeznaczeniem do realizacji abonenckich usług multimedialnych. Interaktywne i asymetryczne usługi wideofoniczne o przepływności kilku Mbit/s.
	bezprzewodowe	podczerwone	Wykorzystanie promieniowania podczerwonego do tworzenia bezprzewodowych sieci lokalnych w pomieszczeniach budynków i halach fabrycznych. Typowa przepływność do 10 Mbit/s, maks. 50 Mbit/s.
		radiowe naziemne (stałe i ruchome)	Różnorodna oferta komunikacji radiowej opartej na stałych łączach dwupunktowych typu P-P (radiolinie) i wielopunktowych typu P-M, a także łączności rozsiewczej - radiodyfuzji (radiofonia i telewizja, niektóre systemy bezprzewodowej łączności abonenckiej) oraz komórkowej (analogowej i cyfrowej).
		satelitarne	Obsługa szerokopasmowej międzykontynentalnej łączności telefonicznej i telewizyjnej wraz z przekazem danych. Utrzymanie komunikacji na obszarach trudno dostępnych (VSAT), globalnej komunikacji komórkowej o charakterze osobistym oraz komunikacja, nawigacja i lokalizacja pojazdów znajdujących się w ruchu.
Szybkość transmisji	podakustyczne		Telemetryczne i komunikacyjne łącza o szybkości transmisji nie przekraczającej 600 bit/s.
	akustyczne		Analogowe łącza transmisyjne (0,3 - 64 kbit/s)
	wąskopasmowe		Cyfrowe łącza komunikacyjne do maksymalnej szybkości transmisji do 2 Mbit/s.
	szerokopasmowe		Komunikacja z szybkościami transmisji powyżej 2 Mbit/s.

4.2. Sieć telekomunikacyjna użytku publicznego

Sieci telekomunikacyjne stanowią zasadniczą część infrastruktury łączności państwa. Zasadniczą i na razie największą częścią tych sieci jest publiczna sieć telekomunikacyjna świadcząca powszechne usługi dla dowolnych abonentów.[6]

4.2.1. Elementy sieci telekomunikacyjnej użytku publicznego

Linie teletransmisyjne

Sieć linii teletransmisyjnych stanowi najistotniejszy składnik sieci telekomunikacyjnej i obejmuje zbiorowość linii telekomunikacyjnych (teletransmisyjnych) rozwiniętych na obszarze kraju za pomocą wszystkich rodzajów środków teletransmisyjnych.

W warstwie międzymiastowej występują następujące rodzaje linii teletransmisyjnych:

a) połączenia krajowe:

- międzymiastowe i międzycentralowe linie światłowodowe o przepustowościach:
  - 2 Mbit/s (odpowiednik 30 kanałów telefonicznych 64 kbit/s),
  - 34 Mbit/s (480 kanałów telefonicznych),
  - 140 Mbit/s (1920 kanałów telefonicznych),
  - 155 Mbit/s (system SDH - STM1),
  - 622 Mbit/s (system SDH - STM4),
  - 2,5 Gbit/s (system SDH - STM16),
- międzymiastowe i międzycentralowe linie radiowe o przepustowościach: 2, 34, 140 i 155 Mbit/s;
- linie kablowe współosiowe telefonii nośnej TN 300, 960, 1800, 1920, 2700 (pozostały niewielkie ilości relacji – są sukcesywnie wycofywane od 1992r);
- linie radiowe analogowe TN 300, 960, 1800 (praktycznie wycofane).

b) połączenia międzynarodowe:

- linie światłowodowe o przepustowościach: 155, 622 Mbit/s (system SDH do Niemiec, Danii, Rosji, Litwy, Ukrainy, Słowacji i Czech);

---

[6] Ze względu na dominującą rolę w sieci użytku publicznego sieci telekomunikacyjnej TPSA, przedstawiono w niniejszej publikacji jako przykład elementy składowe tej sieci.

- linie światłowodowe o przepustowościach: 1÷ n x 140 Mbit/s (system PDH do Niemiec, Czech, Słowacji, Ukrainy, Białorusi, Litwy i Danii).

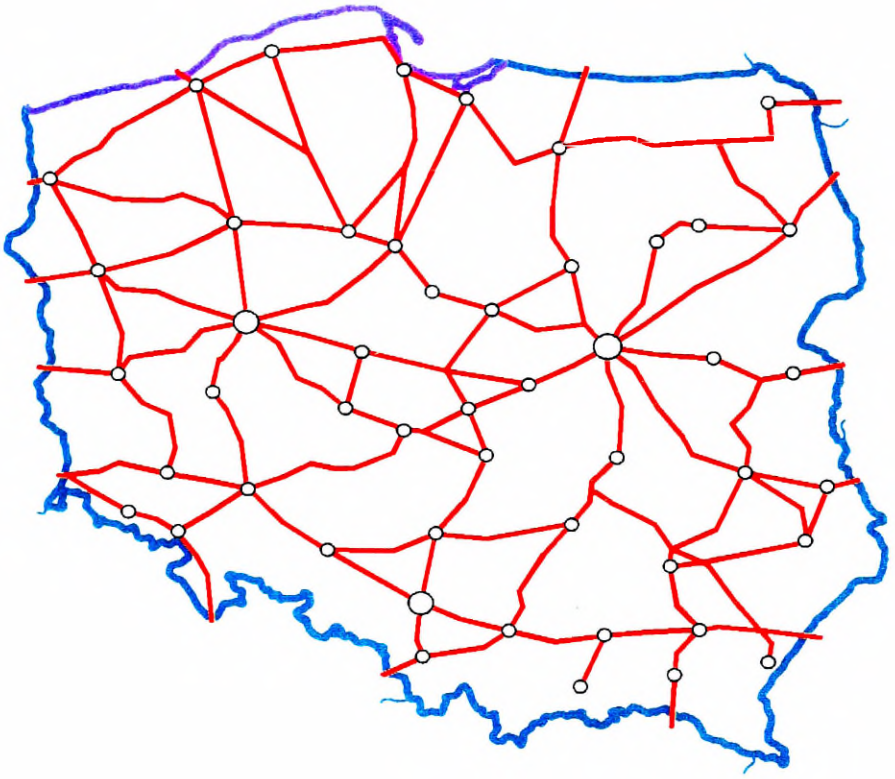
W sieciach strefowych linie międzycentralowe mogą występować jeszcze kablowe linie przewodowe (podziemne lub napowietrzne). Stanowią one kilka procent wszystkich linii strefowych Na liniach tych stosowane są cyfrowe systemy wielokrotne PCM 30/32 (sporadycznie analogowe systemy 12-krotne).

Znaczną część, (kilkanaście procent) linii międzycentralowych (szczególnie krótkich, w obrębie jednego miasta) stanowią jeszcze linie kablowe symetryczne.

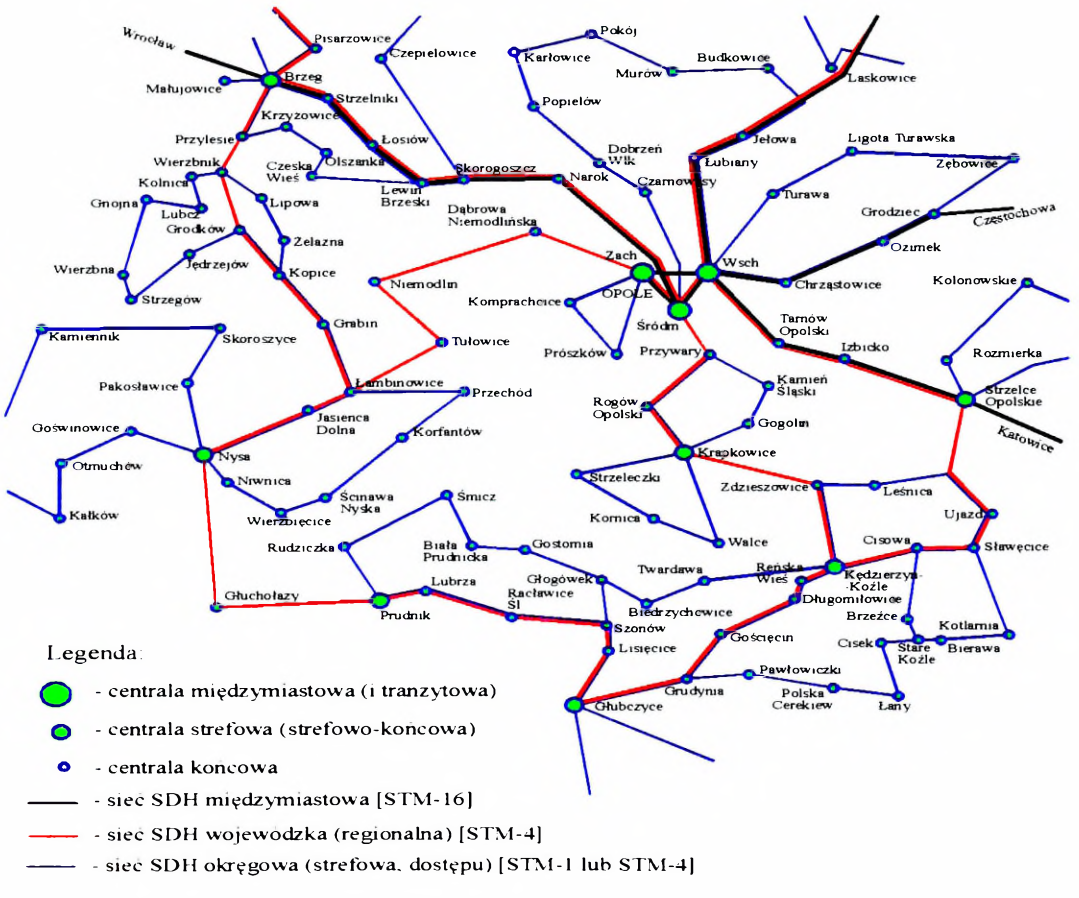
W sieciach miejscowych na terenach miast telefoniczne łącza abonenckie tworzone są jako łącza naturalne (lub łącza ISDN 2B+D) z wykorzystaniem symetrycznych torów kablowych, które stanowią ponad 96% ogólnej liczby torów. Łącza międzycentralowe w tych sieciach realizowane są w około 20% przy użyciu systemów cyfrowych PCM-30/32.

W sieciach telefonicznych na terenach wiejskich w liniach abonenckich znaczną część stanowią obecnie linie radiowe (system DECT).

Na rysunkach 4.2.1.1., 4.2.1.2. i w tabeli 4.2.1.1. pokazano potencjał i strukturę wysokokrotnych linii teletransmisyjnych.



Rys. 4.2.1.1. Sieć wysokokrotnych linii telekomunikacyjnych (wybrane relacje międzymiastowe i międzynarodowe)



Rys. 4.2.1.2. Struktura strefowej sieci transmisyjnej (przykład na części obszaru kraju)

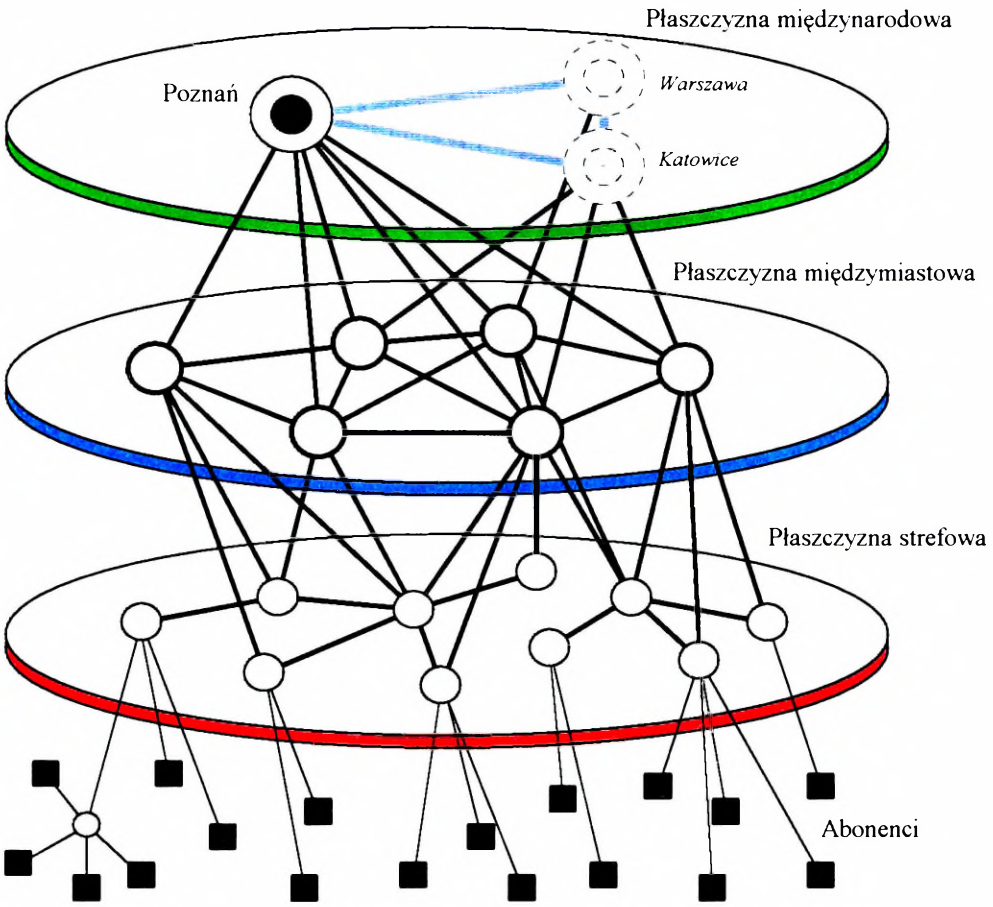
Tabela 4.2.1.1.

Potencjał linii teletransmisyjnych sieci telekomunikacyjnej użytku publicznego (dane orientacyjne)

	Linie sieci miejscowych				
	Kablowe				Radiowe
	symetryczne		optotelekomunikacyjne		
	doziemne	napowietrzne	doziemne	napowietrzne	
w kilometrach	180 000	36 000	5 000	800	4 500
w kilometrotorach	14 000 000	700 000	62 000	9 000	65 000
	Linie sieci wewnątrzstrefowych				
	Kablowe doziemne				
	symetryczne		optotelekomunikacyjne		
w kilometrach	18 000		12 000		
w kilometrotorach	1 100 000		150 000		
	Linie sieci międzymiastowej				
	Kablowe doziemne			Radiowe	
	symetryczne	współosiowe	optotelekomunikacyjne	analogowe	cyfrowe
w kilometrach	2 000	2 500	30 000	łącznie 15 000	
w kilometrotorach	100 000	55 000	600 000	40 000	80 000

Węzły telekomunikacyjne

Drugim komponentem sieci telekomunikacyjnej są węzły telekomunikacyjne (komutacyjne). Umożliwiają one dołączenie abonentów do sieci i korzystanie przez nich z oferowanych przez sieć usług, koncentrację ruchu abonenckiego, zestawianie połączeń lokalnych i dalekosiężnych (międzycentralowych), nadzór i sterowanie siecią. Strukturę warstwową grup węzłów w sieci telekomunikacyjnej przedstawia rysunek 4.2.3.



Rys.4.2.3. Struktura warstwowa sieci telekomunikacyjnej

W zależności od przeznaczenia węzłów w sieci telekomunikacyjnej, można wyróżnić:

- węzły międzynarodowe (w płaszczyźnie międzynarodowej, do której zalicza się centrale międzynarodowe i łącza międzynarodowe),
- węzły międzymiastowe tranzytowe (w płaszczyźnie międzymiastowej, do której zalicza się centrale międzymiastowe i łącza międzymiastowe),
- węzły międzymiastowe końcowe (w płaszczyźnie międzymiastowej),
- węzły strefowe tranzytowe (w płaszczyźnie strefowej),

- węzły strefowe (w płaszczyźnie strefowej),
- węzły miejskie końcowe (w płaszczyźnie strefowej),
- węzły wiejskie końcowe (w płaszczyźnie strefowej).

Poniżej wyróżnianych płaszczyzn mogą występować węzły lokalne (centrale wewnętrzne przedsiębiorstw), dołączone do sieci telekomunikacyjnej podobnie jak abonenckie urządzenia końcowe.

W publicznej sieci telekomunikacyjnej (TP S.A.) znajdują się trzy centrale międzynarodowe (w Warszawie, Poznaniu i Katowicach), około 50 central międzymiastowych, około 230 central strefowych oraz ponad 6900 central końcowych (miejscowe), o pojemności łącznej około 10 000 000 NN - zautomatyzowanych w ponad 99%.

Abonenci

Przedstawiony potencjał publicznej sieci telekomunikacyjnej (TP S.A.) tworzy sieć, której średnia gęstość linii transmisyjnych dalekosiężnych {międzymiastowych i strefowych) wynosi ok. 20 km na 100 km^2 (w zależności od obszaru kraju - tereny zurbanizowane lub pojezierza, wartość ta może się znacznie zmieniać). Są to wyłącznie linie kablowe przewodowe (ok. 50%), światłowodowe (ok. 45%) i radioliniowe (ok. 5%), przy czym udział kabli światłowodowych stale się zwiększa. Sieć linii dalekosiężnych w relacjach pomiędzy miastami wojewódzkimi (i byłymi miastami wojewódzkimi) oraz pomiędzy innymi dużymi miastami ma strukturę wieloboczną (rys.4.2 i 4.3.), przy czym istnieją dla każdej relacji co najmniej 2-3 drogi transmisji umożliwiające utworzenie połączeń. W relacjach: centrala strefowa - centrale miejskie/wiejskie struktura sieci jest w zasadzie gwiaździsta. Transmisyjne linie dalekosiężne są to linie wielowłóknowe umożliwiające realizację wielu torów transmisyjnych w jednej linii (średnio występuje ok. 20 włókien światłowodowych w jednym kablu dalekosiężnym, co może zapewnić dwukierunkową transmisję sygnałów dziesięciu systemów SDH 155Mbit/s).

Średnia gęstość linii miejscowych wynosi ok. 110 km linii na 100 km^2 (łącznie z liniami dalekosiężnymi daje to średnią gęstość ok. 130 km linii transmisyjnych na 100 km^2). Linie miejscowe są także wieloparowe (średnio 50÷100 par dla linii kablowych, 10÷12 włókien dla światłowodów i 20÷30 par dla linii drutowych).

Średnia gęstość węzłów komutacyjnych {central) w sieci TP S.A. wynosi ok. 2,2 centrali na 100 km^2 (od 1,2 do 4,1). Ich rozmieszczenie na obszarze kraju jest prawie równomierne (za wyjątkiem części obszarów górskich i pojezierzy). Taka topologia sieci

telekomunikacyjnej umożliwia wykorzystywanie jej przez abonentów na całym obszarze kraju i jest szczególnie przydatna w przypadkach gwałtownego wzrostu zapotrzebowania na usługi telekomunikacyjne (np.: w sytuacji kryzysowej).

Gęstość sieci telekomunikacyjnej określa się najczęściej poprzez liczbę abonentów sieci przypadających na jednostkę powierzchni lub stosunek liczby abonentów do liczby ludności na danym terenie. Obecnie w publicznej sieci telekomunikacyjnej jest zarejestrowanych ok. 9÷10 milionów abonentów. Są to abonenci prywatni (ok. 80%), abonenci jednostek budżetowych: szkół, szpitali, urzędów (ok. 7%), oraz biznesowi i inni (ok. 13%).

Rozmieszczenie abonentów na obszarze kraju jest nierównomierne i wynika wprost z gęstości zaludnienia, uprzemysłowienia danego regionu i sytuacji makroekonomicznej. W obszarach miejskich znajduje się około 86% ogółu abonentów (na wsi ok. 14%). Stąd też średnia gęstość telefoniczna w miastach wynosi ok. 25÷35 abonentów na 100 mieszkańców, a na wsi ok. 6÷8 abonentów na 100 mieszkańców[7].

Poza urządzeniami abonenckimi, w sieci telekomunikacyjnej występują także aparaty końcowe ogólnodostępne (około 100 000 szt.) oraz centrale abonenckie (PABX), obsługiwane przez sieć na podobnej zasadzie jak abonenci.

Abonenckie urządzenia końcowe, w zależności od wymagań użytkownika i stopnia zaawansowania technicznego obsługującej go centrali może być najprostsze (aparat telefoniczny) lub bardzo rozbudowane usługowo (terminal szerokopasmowego dostępu ISDN).

4.2.2. Struktura usługowo-techniczna sieci telekomunikacyjnej

Sieci telekomunikacyjne stanowią część infrastruktury państwa. Jak już wcześniej zostało stwierdzone, zasadniczą i największą częścią tych sieci jest publiczna sieć telekomunikacyjna, świadcząca powszechne usługi dla dowolnego abonenta. Z wielości i powszechności publicznych sieci telekomunikacyjnych państwa oraz międzynarodowej współpracy sieci publicznej wynika, że podstawowe standardy techniczne i usługowe na sieci telekomunikacyjne są narzucane przez sieć publiczną.

Współczesna sieć telekomunikacyjna składa się z uniwersalnych linii telekomunikacyjnych i cyfrowych central komutacyjnych (łącznic), świadczących wszelkie dostępne usługi. Oznacza to, że te same linie telekomunikacyjne i te same centrale

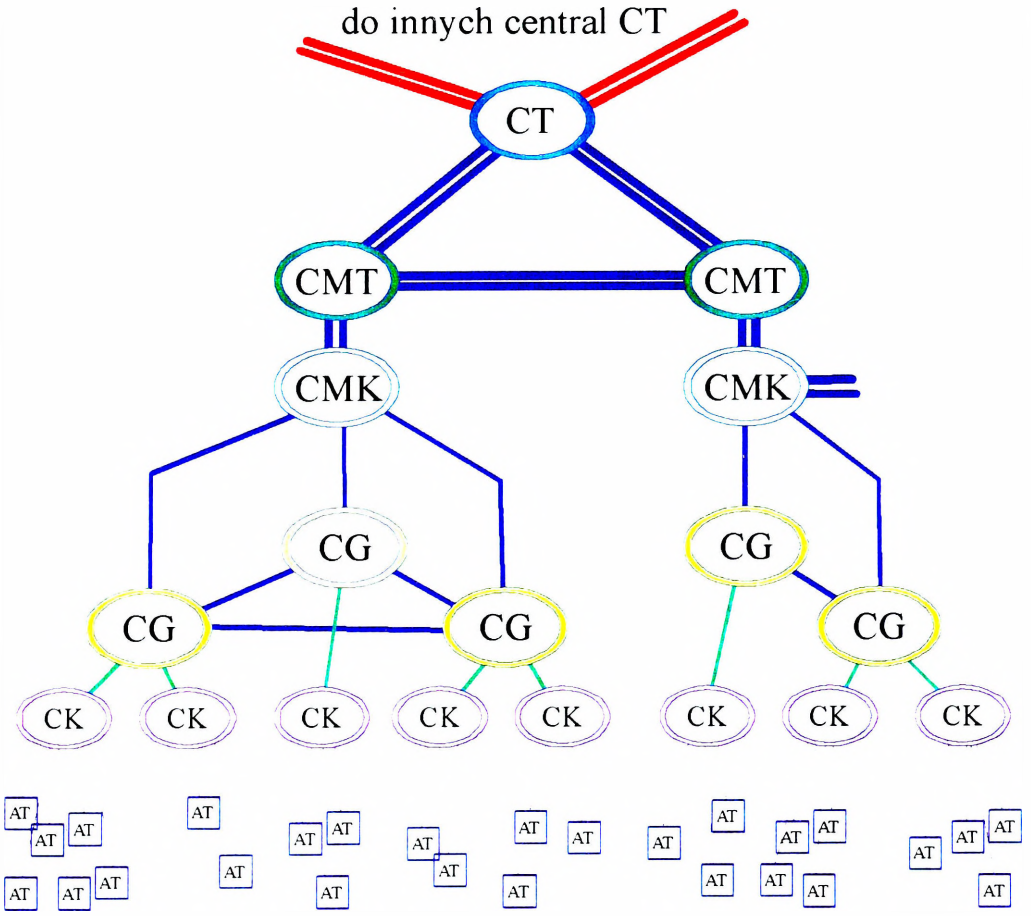
[7] Gęstość ta dotyczy publicznej sieci telefonicznej stacjonarnej (TP S.A.).

wykorzystywane są w dziedzinie telefonii, transmisji danych itp. Związane to jest z zaawansowanym rozwojem sieci telekomunikacyjnych i integracją techniczną i usługową poszczególnych systemów telekomunikacyjnych. Istnieją jednakże wyodrębnione (w sposób fizyczny lub programowy) sieci realizujące pewne, specyficzne grupy usług lub świadczące te usługi tylko wybranym grupom (wyodrębnione sieci dzierżawione). Dlatego poniżej zostały przedstawione części (podsieci), wyodrębnionych w publicznej sieci telekomunikacyjnej.

Telefonia

Podstawowa usługa telekomunikacyjna - telefonia - polega na umożliwieniu wymiany informacji w czasie rzeczywistym w postaci sygnałów akustycznych zawartych w paśmie 0,3÷3,4 kHz. Usługa ta realizowana jest poprzez zestawianie połączeń pomiędzy abonentami w publicznej sieci telefonicznej.

Struktura publicznej sieci telefonicznej PSTN (Public Switched Telephone Network) jest hierarchiczna (rys.4.2.2.1.).



Rys.4.2.2.1. Hierarchiczna struktura sieci telefonicznej

Dalekosiężne kablowe lub radiowe linie transmisyjne między węzłami międzynarodowymi CT, międzymiastowymi centralami tranzytowymi CMT i międzymiastowymi centralami końcowymi CMK przystosowane są do przesyłania sygnałów zwielokrotnionych w systemie PDH lub SDH. Na najwyższym szczeblu hierarchii łącza międzykontynentalne wiążą centrale międzynarodowe CT, łącza międzynarodowe wiążą centrale międzynarodowe CT na terytoriach różnych krajów, a łącza międzymiastowe - centrale międzymiastowe tranzytowe CMT i końcowe CMK różnych stref numeracyjnych.

Łącza między centralami niższej hierarchii w obrębie tej samej miejscowości (strefy numeracyjnej) łączące centrale strefowe tranzytowe (główne) CG i centrale strefowe końcowe CK, tzw. łącza strefowe (międzystrefowe) i międzycentralowe są najczęściej łączami cyfrowymi (przewodowe, radiowe lub światłowodowe).

Na niższych szczeblach hierarchii sieć telefoniczna ma strukturę w zasadzie gwiaździstą. Taką strukturę ma sieć łączy abonenckich wiążących abonentów z centralami końcowymi CK, centralami wewnątrzzakładowymi lub koncentratorami wyniesionymi central (albo centralami satelitowymi). Łącza abonenckie są w przeważającej większości łączami naturalnymi. Każdy abonent (użytkownik sieci) korzysta z odrębnego przewodowego łącza jednotorowego. Część łączy stanowią radiowe łącza cyfrowe w systemie DECT (32kbit/s).

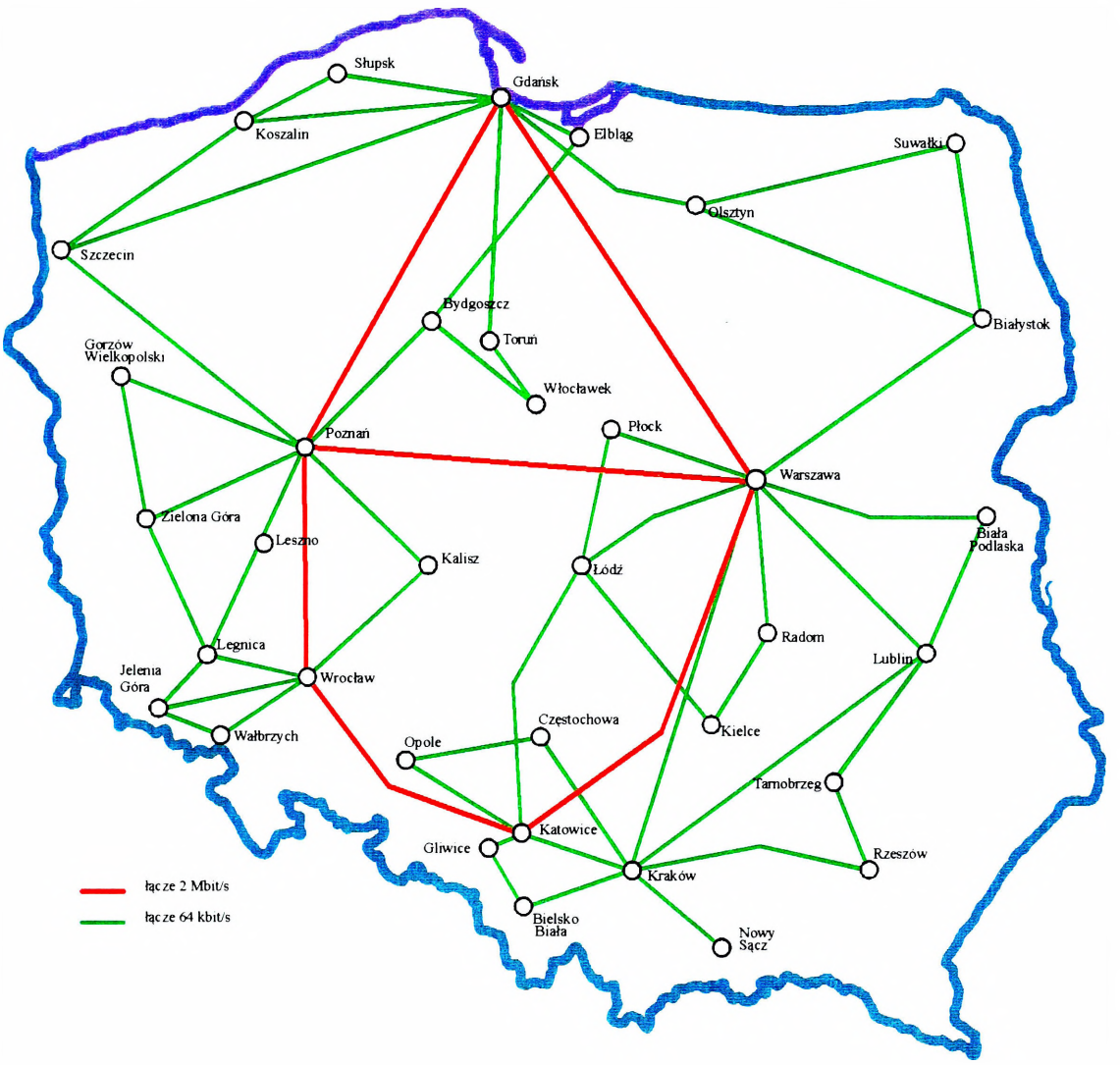
Obecna, powszechna sieć telefoniczna PSTN przekształcana jest w sieć cyfrową z kanałami PCM o przepływności 64 kbit/s dla transmisji sygnałów i komutacji. Cyfryzacja sieci prowadzi do cyfrowej sieci zintegrowanej technicznie IDN, co powoduje zasadnicze zmiany w strukturze hierarchicznej sieci i metodach jej eksploatacji.

Transmisja danych (sieć teleinformatyczna)

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

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

Za pomocą sieci POLPAK-T realizowany jest dostęp do Internetu (TPNET - podłączenie za pomocą łącza dzierżawionego lub dostępu komutowanego). Dostęp komutowany jest oparty na protokole PPP pod ogólnopolskim numerem telefonicznym 0202122 (username: PPP, password: PPP).



Rys.4.2.2.2. Publiczna sieć transmisji danych POLPAK.

Sieć szkieletowa POLPAK-T składa się z 15-tu sieci MAN, co pokrywa równomiernie obszar Polski. Węzły sieci (175 w całym kraju) znajdują się we wszystkich większych miastach, w tym każdym dawnym wojewódzkim. Porty sieci POLPAK-T mogą pracować z prędkością transmisji od 64 do 2048 kbit/s. Oprócz tego każdy węzeł wyposażony jest w porty dla połączeń międzywęzłowych z interfejsem G-703 w liczbie od 4 do 8 sztuk w zależności od ilości połączeń do innych węzłów. W oparciu o sieć POLPAK-T w 49 miastach jest możliwy dostęp PSTN (4500 tys. modemów) do Internetu (protokół PPP). Prędkość transmisji na modemach to 28,8 kbit/s, 33,6 kbit/s i 56 kbit/s.

Sieć TELBANK której operatorem jest_Bankowe Przedsiębiorstwo Telekomunikacyjne „TELBANK" S.A. czyli spółka akcyjna polskich banków działająca na rynku telekomunikacyjnym od września 1992 roku. BPT „TELBANK" S.A. jest operatorem telekomunikacyjnym działającym na obszarze Rzeczypospolitej Polskiej zgodnie z zezwoleniem ministra łączności (aktualne przedłużenie zezwolenia wydał Urząd Regulacji Telekomunikacji i Poczty). Zakres działania BPT obejmuje świadczenie usług telekomunikacyjnych oraz usługi w zakresie zakładania, używania i utrzymania sieci oraz systemów telekomunikacyjnych, a także sprzedaży urządzeń i systemów telekomunikacyjnych. Świadczone przez BPT usługi telekomunikacyjne obejmują: usługi transmisji danych, usługi z wartością dodaną, usługi ISDN, dzierżawę kanałów i urządzeń telekomunikacyjnych, które są oferowane w sieci telekomunikacyjnej użytku publicznego (dla wszystkich zainteresowanych klientów) oraz usługi telefoniczne w wydzielonej sieci telekomunikacyjnej (dla banków i administracji państwowej).

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

Sieć TELBANK obejmuje:

- sieć międzymiastowych kanałów stałych TELBANK-M;
- sieć pakietową TELBANK-P;
- sieć telefoniczną o cechach ISDN TELBANK-T;
- sieć satelitarną TELBANK-VSAT;
- system ruchomej transmisji danych MOBITEX TELBANK-R;
- sieć internetową BPTNet.

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

- cyfrowe kanały transmisyjne - sieć TELBANK-M (w relacjach międzymiastowych);
- sieci miejscowe;

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

Integracja usług telekomunikacyjnych - ISDN

Sieć zintegrowana nosi nazwę sieci cyfrowej z integracją usług i jest oznaczona powszechnie skrótem ISDN (ang. Integrated Services Digital Network). Zasadnicze elementy standardu ISDN zostały opracowane przez CCITT w latach osiemdziesiątych. Opracowane wtedy zalecenia dotyczące ISDN są przykładem nowoczesnej koncepcji współpracy abonenta z publiczną siecią telekomunikacyjną.

Sieć cyfrowa z integracją usług telekomunikacyjnych jest zdefiniowana następująco: *„Główną cechą sieci zintegrowanej jest możliwość świadczenia usług fonicznych i niefonicznych w tej samej sieci. Podstawowym elementem integracji jest realizacja różnych usług w ograniczonym zestawie połączeń i układów sprzęgów służących do wielu celów użytkowych. Sieć zintegrowana umożliwia różnorodność zastosowań na łączach komutowanych i nie komutowanych. Połączenia komutowane mogą być tworzone metodą komutacji łączy i pakietów lub ich kombinacji."*

Zgodnie z koncepcją określoną przez CCITT wielousługowa sieć ISDN jest to sieć rozwinięta z cyfrowej sieci telefonicznej typu IDN, zapewniająca cyfrowe połączenia od terminala do terminala (end - to - end) dla szerokiego zakresu usług. Użytkownicy mają dostęp do usług dzięki zdefiniowaniu ograniczonego zbioru standardowych styków abonenckich (sprzętowych i programowych) pomiędzy terminalami użytkownika i centralą końcową sieci telekomunikacyjnej.

Zintegrowana sieć telekomunikacyjna opiera się na wykorzystaniu jednolitej cyfrowej transmisji i komutacji.

Sieci cyfrowe z integracją usług telekomunikacyjnych pozwalają uzyskać wiele korzyści:

- wielorakość usług za pośrednictwem jednego dostępu abonenckiego;
- równoczesne użytkowanie dwóch łączy (równoważnych dwóm łączom telefonicznym) za pośrednictwem „podstawowego dostępu" (standardowy dostęp abonencki w sieci zintegrowanej - $2B_{64}+D_{16}$ - dwa kanały o przepustowościach 64 kbit/s obsługiwane w trybie komutacji kanałów i jeden kanał l6 kbit/s obsługiwany w trybie komutacji pakietów), co umożliwia zainstalowanie u abonenta do ośmiu terminali lub aparatów telefonicznych;
- łatwość dołączenia central abonenckich za pośrednictwem „dostępu pierwotnogrupowego" (przepustowość 2 Mbit/s - $30B_{64}+D_{64}$, gdzie kanał D ma przepustowość 64 kbit/s).

Zgodnie z zaleceniem Komisji Europejskiej sieć cyfrowa z integracją usług telekomunikacyjnych w Europie realizuje:

1. Telefonię cyfrową wysokiej jakości na łączach o przepływności 64 kbit/s i z dużym zakresem nowych funkcji dla użytkownika:
   - oczekiwanie na rozmowę;
   - wskazywanie abonenta wywołującego;
   - informacja o wysokości opłaty;
   - przekazywanie rozmów;
   - zestawienie połączenia do abonenta zajętego (automatycznie, po zakończeniu poprzedniego połączenia);
   - identyfikacja połączeń złośliwych.
2. Transmisję danych o dużej przepływności 64 kbit/s z możliwością dołączenia komputerów osobistych;

3. Wiele nowoczesnych usług, np:
    - telekopia 64 kbit/s (przekazywanie arkusza A4 w ciągu kilku sekund, 10 razy szybciej niż obecnie używane aparaty telekopiowe III generacji);
    - teleteks 64 kbit/s (100 razy większa szybkość niż aparatu teleksowego);
    - alfageometryczny i alfafotograficzny wideoteks (wysoka jakość obrazu) o przepływności 64 kbit/s (niemal natychmiastowe pojawienie się obrazu na ekranie, 30 razy większa przepływność).

Od 1.04.1998 w publicznej sieci telekomunikacyjnej (TP S.A.) wprowadzone zostało świadczenie usług w ramach sieci ISDN. Możliwości usługowe sieci, w zależności od wyposażenia abonenta, można podzielić na dwie kategorie:

- usługi przenoszenia (bearer services);
- teleusługi (teleservices);
- usługi dodatkowe (supplementary services) - usługi modyfikujące lub uzupełniające usługi podstawowe należące do jednej z dwóch w/w kategorii.

Usługi przenoszenia zapewniają transmisję sygnałów między stykami użytkowników z siecią. Natomiast teleusługi w pełni umożliwiają wymianę informacji między użytkownikami sieci zintegrowanej, obejmują więc również funkcję urządzeń końcowych.

Spośród znormalizowanych już przez CCITT (następnie ITU/T) usług przenoszenia można wymienić np.: usługi:

- z wykorzystaniem kanałów o przepływności 64 kbit/s bez ograniczeń oraz częstotliwością bazową 8 kHz;
- z wykorzystaniem kanałów o przepływności 64 kbit/s oraz przepływnością bazową 8 kHz, do przesyłania sygnałów mowy.

Ta ostatnia usługa różni się od pierwszej tym, że sygnał cyfrowy na styku użytkownik - sieć jest kodowany jednym ze sposobów znormalizowanych międzynarodowo oraz że w sieci można korzystać z technik przetwarzania mowy, takich jak np.: transmisja analogowa, kompresowanie echa itd.

Teleusługi:

- Telefonia - usługi telefoniczne świadczone przez ISDN charakteryzują się wyższą jakością dźwięku (szersze pasmo: 7 kHz i stereofonia).
- Teleteks - jest usługą stanowiącą rozwinięcie teleksu; różni się od teleksu przede wszystkim znacznie większym repertuarem znaków i możliwością odbierania

dokumentów formatu A4 o takiej samej postaci jak dokumenty nadane pod względem treści i formy.

- Telekopia (telefaks) - z telekopii korzysta się już w sieciach telefonicznych, co umożliwia reprodukowanie wszystkich rodzajów materiałów graficznych.
- Wideoteks - umożliwia dostęp do odległych baz danych za pośrednictwem sieci telekomunikacyjnych. Cechy tej usługi są następujące:
  - informacje mają postać alfanumeryczną bądź piktograficzną;
  - informacje są przechowywane w bazie danych;
  - informacje przesyła się między bazą danych a użytkownikiem przez sieci telekomunikacyjne;
  - informacje wizualne są przedstawiane przy użyciu odpowiednio zmodyfikowanego odbiornika telewizyjnego lub innego urządzenia z ekranem;
  - dostępem do usługi steruje bezpośrednio lub pośrednio użytkownik;
  - korzystanie z usługi jest łatwe zarówno dla specjalistów jak i niespecjalistów;
  - jest możliwe tworzenie oraz modyfikowanie informacji zawartych w bazach danych przez użytkowników;
  - jest możliwe zarządzanie bazami danych, czyli tworzenie nowych baz oraz utrzymywanie baz istniejących, jak również tworzenie zamkniętych grup użytkowników.
- Poczta elektroniczna.
- Transmisja danych - sieć ISDN umożliwia przesyłanie danych przy zastosowaniu zarówno komutacji kanałów, jak i pakietów.
- Wideofonia - integracja tej usługi z innymi jest możliwa w szerokopasmowej sieci z integracją usług (z kanałami 155 Mbit/s). Przewiduje się, że wideofonia będzie szczególnie użyteczna w przypadku telekonferencji.
- Telewizja - zastosowanie sieci szerokopasmowej umożliwi dostęp do wielu różnych programów telewizyjnych, także o podwyższonej jakości (HDTV).
- Teleakcje - przesyłanie między użytkownikiem a siecią krótkich wiadomości, wymagających bardzo małych szybkości transmisji.

Ponadto sieć cyfrowa z integracją usług jest tak zaprojektowana, aby było możliwe korzystanie za jej pośrednictwem nie tylko z zaprezentowanych teleusług, lecz również usług, które powstaną dopiero w przyszłości.

Usługi dodatkowe modyfikują lub uzupełniają usługi podstawowe. Przykładami takich usług mogą być: oczekiwanie zgłoszenia, identyfikacja numeru abonenta wywołującego, połączenie konferencyjne, połączenie z zastosowaniem karty kredytowej itp.

Radiokomunikacja

Inny sposób transmisji sygnału - przesyłanie fali elektromagnetycznej w wolnej przestrzeni, wyznacza odrębną część telekomunikacji - radiokomunikację. Podział ten wynika z zastosowania innej techniki transmisyjnej i związanych z tym charakterystyk toru transmisyjnego i sygnału, natomiast aspekty usługowe czy też obszar zastosowania radiokomunikacji są praktycznie porównywalne z klasyczną (tzw. „przewodową") telekomunikacją.

Techniki radiowe są we współczesnych sieciach telekomunikacyjnych wykorzystywane powszechnie. W zależności od cech charakterystycznych systemu telekomunikacyjnego[8] wykorzystuje się różne systemy radiokomunikacyjne. Przyjmując za kryterium stopień skupienia fali, wykorzystuje się systemy:

- torowe: linie radiowe (radiolinie), w tym także linie radiowe satelitarne;
- beztorowe: systemy radiodostępu, telefonii komórkowej, radiofonii i telewizji.
- Dla kryterium kierunku transmisji można wyróżnić systemy:
- porozumiewawcze: systemy radiodostępu, telefonii komórkowej;
- rozsiewcze: systemy przywoławcze, radiofonię i telewizję.

Poszczególne zastosowania systemów radiokomunikacyjnych są przedstawione w kolejnych podrozdziałach.

---

[8] Tu: system telekomunikacyjny określony głównymi cechami elektrycznymi lub konstrukcyjnymi urządzeń. Leksykon naukowo-techniczny WNT 1989, str. 954.

Linie radiowe (radiolinie)

W systemie telekomunikacyjnym kraju linie radiowe są stosowane wszędzie tam, gdzie np.: ze względów technicznych niemożliwe lub niecelowe jest budowanie linii kablowej.

Zastosowanie radiolinii w publicznej sieci telekomunikacyjnej (także w sieciach komercyjnych innych operatorów) można podzielić na:

- naziemne linie radiowe,
- linie radiowe satelitarne.

W naziemnym systemie linii radiowych zastosowanie mają:

1. Analogowe linie radiowe (występują jeszcze jedynie w publicznej sieci telekomunikacyjnej TP S.A., są one sukcesywnie wycofywane z eksploatacji), przeznaczone dla transmisji sygnałów telewizyjnych, radiofonicznych i telefonii nośnej;
2. Cyfrowe linie radiowe (m.in. w publicznej sieci telekomunikacyjnej TP S.A., w sieciach telefonii komórkowej - jako linie transmisyjne pomiędzy stacjami bazowymi, w systemach radiowego dostępu abonenckiego - jako linie transmisyjne do stacji bazowej radiodostępu). Obecnie stosowane cyfrowe linie radiowe pracują z przepustowościami od 2 Mbit/s do 140 Mbit/s (system PDH) oraz 155 Mbit/s i 622 Mbit/s (system SDH).

Dla naziemnych linii radiowych przewidziane dla Polski pasma częstotliwości to: 2,4; 3,5; 5,8; 6; 7; 8; 10; 11; 13; 15; 18; 23; 26; 28; 38; 58 GHz. Cechą charakterystyczną radiolinii jest ograniczenie zasięgu łączności do horyzontu radiowego (widoczności anten) oraz malenie zasięgu (nawet do ok. 800 m) ze wzrostem częstotliwości pracy radiolinii. Łączna liczba linii radiowych naziemnych jest trudna do określenia ze względu na stale rozbudowujące się systemy łączności bezprzewodowej. Obecnie można ją oszacować na ok. 60 000 linii (tylko w TP S.A. ok. 15 000).

W satelitarnych liniach radiowych, pracujących w układzie punkt - punkt, w Polsce pracują 73 stacje radioliniowe:

W systemie:

- INTELSAT - 11 stacji,
- EUTELSAT - 20 stacji,
- KOPERNIKUS - 29 stacji,

- TELE-X - 20 stacji,
- INTELSAT - 3 stacje,
- ORION - 10 stacji.

Radiowe stacjonarne łącza abonenckie

Coraz większa popularność systemów komórkowych i spowodowana nią miniaturyzacja i obniżenie cen podzespołów transmisji radiowej sprawiły, że od początku lat 90-tych obserwowany jest wzrost zainteresowania systemami bezprzewodowych pętli abonenckich, tzn. możliwością podłączania abonentów publicznej sieci telefonicznej do infrastruktury sieci poprzez łącze radiowe. Standardy telefonii bezprzewodowej są jedną z możliwości realizacji systemów bezprzewodowych pętli abonenckich.

Radiowe stacjonarne łącza abonenckie mają zastosowanie w terenach o małej gęstości abonentów (tereny wiejskie), znacznie oddalonych od central komutacyjnych.

Systemy telefonii bezprzewodowej

Systemy telefonii bezprzewodowej pojawiły się w końcu lat siedemdziesiątych. Mogą być one scharakteryzowane jako środek łączności bezprzewodowej o niewielkiej mocy dla użytkownika poruszającego się w zasięgu stacji bazowej. Celem telefonu bezprzewodowego miało być w większości zastąpienie telefonu przewodowego dla abonenta lokalnego. Stacja bazowa, to część systemu telefonii bezprzewodowej dołączona do publicznej sieci telefonicznej i widziana przez nią jako zwykły telefon.

Prace unifikacyjne prowadzone w ramach Unii Europejskiej doprowadziły do ustanowienia europejskiego standardu cyfrowej telefonii bezprzewodowej DECT (Digital European Cordless Telephony}. System ten został zoptymalizowany ze względu na zastosowanie wewnątrz budynków. Stacje bazowe systemu DECT są dołączone poprzez kontroler do wewnętrznych (zakładowych) central telefonicznych. Wśród najistotniejszych wymagań stawianych standardowi były m.in.:

- wysoka jakość przesyłanego sygnału mowy,
- duża pojemność systemu,
- możliwość stosowania procedur służących do identyfikacji użytkowników oraz szyfrowania przesyłanego sygnału mowy,

- mała złożoność systemu, możliwość tworzenia systemów jedno i wielokomórkowych wraz z możliwością przełączania rozmów pomiędzy stacjami bazowymi w trakcie trwającego połączenia.

Standard DECT został stworzony z myślą o zastosowaniu go do usług typu telepoint, realizacji bezprzewodowych central abonenckich oraz bezprzewodowych pętli abonenckich. Światowy sukces standardu GSM stworzył nadzieje na podobnie szerokie zastosowanie standardu DECT. Fakt ten, jak również rozbudowane cechy standardu związane z przesyłaniem sygnałów innych niż sygnały mowy sprawiły, że obecnie skrót DECT rozwijany jest jako: Digital Enhanced Cordless Telecommunications.

System DECT zaprojektowano do pracy w pasmie 1880-1900 MHz. Kanały fizyczne wydzielono zarówno w dziedzinie częstotliwości, jak i czasu. Łączna liczba kanałów fizycznych w standardzie DECT wynosi 120. Sygnały mowy w standardzie DECT są kodowane przy wykorzystaniu modulacji adaptacyjnej ADPCM, z przepływnością 32 kbit/s, co umożliwia osiągnięcie jakości porównywalnej z telefoniczną siecią stałą.

Systemy łączności oparte na standardzie DECT zawierają jedną lub wiele stacji bazowych oraz pewną liczbę terminali. Stacja bazowa w systemie DECT podczas pracy prowadzi w sposób ciągły, w co najmniej jednym kanale nadawanie rozsiewcze informacji systemowych, sygnalizacji oraz sygnałów przywołania. Każda ze stacji ruchomych pracujących w systemie zaraz po włączeniu dostraja się do częstotliwości najlepiej odbieranej stacji bazowej, co zwykle odpowiada stacji bazowej najbliżej położonej i prowadzi ciągły nasłuch radiowy. Pomimo dostrojenia się do najsilniejszej stacji bazowej, terminal równolegle przegląda także całe dostępne pasmo radiowe w poszukiwaniu ewentualnych innych pobliskich stacji bazowych systemu, a jeśli je rozpozna, to porządkuje je w wewnętrznym rejestrze w kolejności według średniej mocy ich sygnału. Po dostrojeniu się do najsilniejszej stacji bazowej terminal w podobny sposób dokonuje wyboru najmniej zakłóconego kanału fizycznego, w obrębie wybranej stacji bazowej.

Standardy telefonii bezprzewodowej są wykorzystywane w prostych systemach użytku domowego, w systemach publicznych typu telepoint, w bezprzewodowych centralach abonenckich PBX oraz jako technologia realizacji bezprzewodowych pętli abonenckich.

Domowe systemy telefonii bezprzewodowej umożliwiają prowadzenia rozmów zwykle na odległość kilkudziesięciu metrów. Typowy system tego rodzaju składa się z jednego przenośnego bezprzewodowego mikrotelefonu oraz stacjonarnej, domowej stacji bazowej podłączonej do gniazdka telefonicznego. Urządzenia tego typu są powszechnie stosowane w sieciach telekomunikacyjnych.

Systemy publiczne typu telepoint

Innym zastosowaniem dla standardów telefonii bezprzewodowej są publiczne systemy typu telepoint. Abonenci korzystający z tej usługi mogą uzyskiwać dostęp do publicznej stałej sieci telefonicznej z przenośnych terminali w obrębie działania stacji bazowych tego systemu, najczęściej umieszczanych w miejscach publicznych, tj. w centrach handlowych, dworcach, lotniskach itd. Abonenci korzystający z usługi typu telepoint nie mogą zazwyczaj odbierać za pomocą terminali przenośnych rozmów przychodzących, mogą je jedynie inicjować. Tak zdefiniowana usługa zwalnia system z konieczności śledzenia pozycji abonenta, przez co złożoność oraz koszt infrastruktury systemu są znacznie niższe w porównaniu np. z infrastrukturą systemów telefonii komórkowej.[9]

Bezprzewodowe centrale abonenckie PBX

Bezprzewodowy zamknięty system łączności przeznaczony do wykorzystania na terenie zakładów pracy, hoteli, szpitali itp. składa się w ogólności z bezprzewodowej centrali abonenckiej WPBX {Wireless Private Branch Exchange), jednej lub kilku stacji bazowych oraz terminali bezprzewodowych. Centrala WPBX jest sterownikiem całego systemu, do którego dołączone są wszystkie stacje bazowe. Każda ze stacji bazowych jest odpowiedzialna za połączenia w obrębie jednej komórki.

Systemy trankingowe

Radiowe systemy trankingowe są rozwiązaniem technicznym znanego od dziesiątków lat problemu zapewnienia łączności radiowej, choćby o dostatecznej tylko jakości, rozproszonym w terenie grupom użytkowników będących pracownikami tego samego przedsiębiorstwa. Chodzi tu najczęściej o duże przedsiębiorstwa wykonujące prace na terenach całych regionów, jak np. służby energetyczne, gazownicze i wodociągowe, policja, straż pożarna i pogotowie ratunkowe, kolejnictwo i transport drogowy. Wiele z tych firm musi liczyć się codziennie z możliwością wystąpienia sytuacji awaryjnych, wymagających szybkiej reakcji i często współdziałania zespołu osób. Inną grupą użytkowników systemu tego typu są firmy, których teren działania jest bardziej zwarty, ale niedogodny dla łączności przewodowej, np. służby obsługi portów, stacji kolejowych i lotnisk, pracownicy firm budowlanych, dużych zakładów pracy, służby ochrony itp.

---

[9] Jest to cenna cecha w przypadku tworzenia systemu radiokomunikacyjnego na potrzeby działań antykryzysowych na ograniczonym obszarze.

Systemy trankingowe charakteryzują się następującymi zaletami:

- dużą pojemnością, przy ustalonej liczbie kanałów;
- wysoką niezawodnością działania;
- możliwością dogodnej realizacji priorytetowania rozmów;
- prywatnością prowadzonych rozmów;
- dostępnością usług trankingowych także dla niewielkich grup użytkowników;
- elastycznością systemu;
- prostotą obsługi.

Rosnące zapotrzebowanie na nowe usługi w systemach trankingowych doprowadziły do opracowania standardu nowoczesnego europejskiego cyfrowego systemu trankingowego pod nazwą TETRA.

Standard TETRA (Trans European Trunked RAdio) został zaprojektowany w sposób, który umożliwia efektywne przesyłanie w kanale radiowym zarówno sygnałów mowy, jak i danych w trybie połączeniowym, a także w trybie pakietowym. Istotnym wymaganiem była także możliwość współpracy systemów eksploatowanych przez różnych operatorów.

W architekturze systemu TETRA można wyróżnić część komutacyjno-sieciową, stacje bazowe i terminale. W części komutacyjno-sieciowej znajdują się centrale główne i lokalne. Centrale lokalne są podporządkowane centralom głównym pełniąc rolę pośrednią pomiędzy koncentratorami wyniesionymi nowoczesnych central elektronicznych w telefonii stałej a sterownikiem stacji bazowych w systemie GSM. W części komutacyjno-sieciowej znajduje się ponadto moduł rejestracji użytkowników oraz centrum eksploatacji i utrzymania sieci. W tej części znajduje się zespół modułów pośredniczących, umożliwiających współpracę systemu z sieciami zewnętrznymi takimi jak: publiczna telefoniczna sieć stała, sieci ISDN, sieci pakietowej transmisji danych itp. Do central lokalnych dołączone są stacje bazowe.

W standardzie TETRA zastosowano, podobnie jak w systemie GSM, mieszany sposób wielodostępu, tj. połączenie wielodostępu częstotliwościowego FDMA i czasowego TDMA. Przydzielone do użytkowania pasmo częstotliwości dzielone jest na kanały o szerokości 25 kHz każdy, a w każdym kanale zdefiniowana jest struktura pozwalająca na utworzenie czterech kanałów rozmównych zwielokrotnionych czasowo. Tak więc efektywna szerokość pasma zajmowanego przez pojedynczy kanał rozmówny wynosi 6,25 kHz.

Standard TETRA definiuje dwa podstawowe tryby pracy systemu:

- Voice plus Data (TETRA VD), służący do transmisji sygnałów mowy oraz danych,

- Packed Optimized Data (TETRA POD), przeznaczony wyłącznie do transmisji danych.

W systemie TETRA dla jego poprawnego działania zastosowano szereg procedur sieciowych, wśród nich m.in.:

- przełączanie kanałów pomiędzy stacjami bazowymi,
- zmianę obszaru lokalizacyjnego przez stację ruchomą,
- migrację terminala do innej sieci TETRA, identyfikację terminali oraz użytkowników,
- rozpoczęcie i kończenie pracy w systemie,
- na żądanie terminala, przerwanie i wznawianie transmisji wiadomości w kanale w „dół".

Standard trankingowy TETRA zaprojektowano m. in. pod kątem potrzeb związanych z działaniem i współdziałaniem krajowych służb publicznych. Szczególny nacisk położono więc na wysoką niezawodność systemu, jego bezpieczeństwo, dostępność specyficznego typu usług, możliwość współdziałania różnych systemów ze sobą.

Systemy trankingowe działają w Polsce od roku 1991, kiedy powstała sieć Radio-Net, której operatorem jest spółka Uni-NET i TP S.A. System ten dysponował w połowie lat 90-tych około 20 stacjami bazowymi zlokalizowanymi w większych miastach Polski. Działają jeszcze dwie sieci w różnych rejonach kraju. Wszystkie te sieci mają nieciągłe pokrycie radiowe i oferują łączność w większych aglomeracjach miejskich i ich bezpośredniej okolicy.

Opinie dotyczące perspektyw rozwoju sieci trankingowych są podzielone. Głównym powodem jest szybkie poszerzanie usług oferowanych przez systemy telefonii komórkowej. Jednakże służby publiczne każdego kraju mają tak specyficzne wymogi, że trudno jest dla ich spełnienia wykorzystywać publiczne systemy telefonii komórkowej. Mimo to, (jak przedstawiono w rozdziale 5.) zmodyfikowane systemy komórkowe mogą stanowić alternatywę lub (co bardziej prawdopodobne) jedynie uzupełnienie dla systemów trankingowych. Wydaje się, więc że system TETRA jest praktycznie standardem w zakresie zastosowań w służbach ratowniczych i systemach reagowania kryzysowego.

Sieci telefonii komórkowej

Telefonia komórkowa jest kolejnym przykładem systemu radiokomunikacyjnego z obiektami ruchomymi. Systemy telefonii komórkowej można scharakteryzować jako systemy zapewniające dwustronną łączność bezprzewodową ze stacjami ruchomymi poruszającymi się nawet z dużą szybkością na dużym obszarze pokrywanym przez system stacji bazowych, który może sięgać nawet poza zakres danego państwa (jak to jest w przypadku Europy i systemu GSM).

W obecnych, cyfrowych systemach drugiej generacji jako cel przyjęto maksymalizację pojemności systemu rozumianą jako liczbę użytkowników na jednostkę pasma oraz liczbę użytkowników w pojedynczej komórce. Z drugiej strony, zapewnienie możliwości łączności z pojazdami poruszającymi się wzdłuż autostrad na obszarach słabo zaludnionych powoduje konieczność zastosowania stacji bazowych o dużym zasięgu i dużej mocy nadawczej.

Uwzględniając oba przeciwstawne czynniki, system telefonii komórkowej charakteryzuje się następującymi cechami:

- stosunkowo dużą mocą nadajników,
- dużą komplikacją telefonu komórkowego, w tym jego procedur przetwarzania sygnałów,
- relatywnie niską jakością połączenia,
- dużą komplikacją sieci związaną z funkcjami przejmowania połączenia przez kolejne stacje bazowe, wielością usług itp.

Systemy telefonii komórkowej drugiej generacji, pomimo różnic występujących między nimi, mają wiele cech wspólnych. Są to:

- mała szybkość sygnałów cyfrowych reprezentujących sygnały mowy (13 kbit/s) - przyczynia się to do zwiększenia pojemności systemu kosztem jakości sygnału mowy;
- stosunkowo duże opóźnienie transmisji, około 200 ms łącznie w obu kierunkach, wynikające z kodowania i dekodowania mowy oraz skomplikowanych algorytmów odbioru i detekcji sygnałów cyfrowych;
- transmisja dupleksowa z wykorzystaniem metody podziału częstotliwości;
- sterowanie poziomem mocy stacji ruchomej w celu zapewnienia jednakowej jakości dostępu telefonom ruchomym różnie oddalonym od stacji bazowej.

Poniżej przedstawiona jest charakterystyka systemów telefonii komórkowej stosowanych w Polsce.

GSM 900 i DCS 1800 (GSM 1800)

W systemie GSM wyróżnia się następujące części funkcjonalne:

I. zespół stacji bazowych (Base Station Subsystem BSS);

II. część komutacyjno-sieciową (Network and Switching Subsystem NSS);

III. stacje ruchome (Mobile Station MS);

IV. zespół eksploatacji i utrzymania (Operation and Maintenance Subsystem OMS).

Z zasady tworzenia systemu radiokomunikacji ruchomej wynika, że podstawowym sposobem organizacji takiego systemu jest struktura komórkowa. Każda komórka posiada jedną stację bazową (Basa Transceiver Station BTS). Zespół stacji bazowych umożliwia dostęp stacjom ruchomym do części stałej systemu GSM i dalej, w miarę potrzeby, do innych systemów telekomunikacyjnych.

Systemy działają w zakresach częstotliwości wokół 900 MHz i 1800 MHz. W tych zakresach częstotliwości fale rozchodzą się w zasadzie za pośrednictwem fali przyziemnej, w zasięgu horyzontu radiowego. Biorąc pod uwagę typowe wysokości anten nadawczych stacji bazowych oraz moce nadajników, maksymalny zasięg promieniowania anten systemów komórkowych wynosi od 30 km do 65 km. Wielkości komórek są wypadkową kilku czynników i nie przekraczają dla systemu GSM - 35 km (najmniejsze wymiary komórek w dużych aglomeracjach, to około 0,8÷1 km).

Organizacja zespołu stacji bazowych jest dwuwarstwowa, co pozwoliło na uproszczenie konstrukcji i obniżenie kosztów urządzeń pracujących na peryferiach systemu, w dużej odległości od central MSC. Zespół stacji bazowych podzielono więc na część sterującą (tzw. sterowniki stacji bazowych - Base Station Controller BSC) i transmisyjną (stacje bazowe BTS). Jeden sterownik BSC zarządza typowo pracą kilku lub kilkudziesięciu stacji bazowych. W bezobsługowych stacjach bazowych pozostawiono jedynie niezbędne wyposażenie nadawczo-odbiorcze odpowiadające analogicznym modułom w stacji ruchomej.

Główne funkcje realizowane w stacjach bazowych, to:

- wykrywanie zgłoszeń (zadania przydzielenia wydzielonego kanału sygnalizacyjnego) stacji ruchomych;
- funkcje związane z przetwarzaniem sygnału w kierunku nadawczym i odbiorczym.

Urządzenia części komutacyjno-sieciowej odpowiadają za podstawowe funkcje komutacyjne systemu, współpracę z innymi sieciami telekomunikacyjnymi i za przechowywanie informacji o zarejestrowanych użytkownikach systemu oraz wszelkich informacji niezbędnych do kontroli uprawnień i śledzenia ruchu abonentów.

Jedyną częścią systemu GSM widzianą przez przeciętnego użytkownika jest zazwyczaj jego stacja ruchoma, zwana potocznie telefonem komórkowym. Istnieje kilka klas stacji ruchomych (tabela 4.2.2.1.), różnią się one między sobą mocą nadajnika, wielkością oraz możliwościami współpracy z urządzeniami transmisji danych. Poza tym różnią się one między sobą funkcjami, zarówno podstawowymi i dodatkowymi, a także parametrami elektrycznymi, w tym przede wszystkim maksymalną mocą wysyłanego sygnału.

Tabela 4.2.2.1.

Klasy stacji ruchomych w systemach GSM 900 i DCS 1800

Klasa	GSM 900		DCS 1800	
	Moc nadajnika	**Typ stacji**	**Moc nadajnika**	**Typ stacji**
1	20 W (43 dBm)	przewoźne i przenośne	1 W (30 dBm)	kieszonkowe
2	8 W (39 dBm)	przewoźne i przenośne	0,25 W (24 dBm)	kieszonkowe
3	5 W (37 dBm)	kieszonkowe	-	-
4	2 W (33 dBm)	kieszonkowe	-	-
5	0,8 W (29 dBm)	kieszonkowe	-	-

Zespół eksploatacji i utrzymania OMS w systemie GSM umożliwia operatorowi wgląd w pracę systemu oraz administrowanie nim. Zarządzanie obejmuje następujące dwie grupy funkcji:

- zarządzanie konfiguracją systemu, np.: tworzenie nowych komórek, określanie obszarów przywołań, administrowanie zasobami radiowymi, zmiany w architekturze sieci;
- administrowanie rejestracją abonentów.

W systemie DCS 1800 (GSM 1800) szerokość pasm częstotliwości dla każdego kierunku transmisji wynosi 75 MHz, co daje trzykrotnie większą liczbę kanałów w porównaniu z systemem GSM 900. Jeśli oprócz tego uwzględnić, że wielkość komórek w systemie DCS 1800 jest znacznie mniejsza niż w systemie GSM 900, wówczas okaże się, że pojemność systemu DCS 1800, mierzona liczbą kanałów rozmównych na jednostkę powierzchni, jest około 10-krotnie wyższa w porównaniu z systemem GSM 900.

Systemy telefonii komórkowej stanowią obecnie znaczny udział rynku telekomunikacyjnego kraju (aktualnie liczba abonentów sieci GSM przekroczyła 5 milionów). W bliskiej perspektywie przewiduje się w Polsce uruchomienie (pierwsze elementy składowe systemu zostały sprowadzone do Polski w kwietniu bieżącego roku) i wprowadzenie do użytku publicznego systemu UMTS (ang. Universal Mobile Telecommunication System). Jest to system umożliwiający globalną dostępność dzięki zastosowaniu zintegrowanych podsystemów: naziemnego i satelitarnego.

System UMTS przewidziany jest do pracy w szerokim zakresie widma: 470÷2900 MHz, podzielonym na podzakresy przeznaczone dla poszczególnych służb radiokomunikacji ruchomej i radiodyfuzji. System UMTS projektowany jest w taki sposób, aby zapewnić kompatybilność z dotychczas wykorzystywanymi systemami oraz możliwość korzystania z infrastruktury i usług dowolnego innego systemu radiokomunikacyjnego.

Z powodu uniwersalności systemu UMTS i współdziałania szeregu jego segmentów sieć systemu ma bardzo różnorodną strukturę. Sieć części radiokomunikacyjnej systemu jest dołączona do segmentu stałego przez centrale tranzytowe (TX). Do nich z kolei dołączone są centrale lokalne (LE), których grupy nadzorowane są przez węzły sterujące (MCN). Poszczególne centrale zarządzają z kolei zespołami sterowników stacji bazowych (BSC) współpracującymi z grupami stacji bazowych (BTS).

Stopień mobilności abonentów sieci lub jej fragmentów (jak to jest w przypadku realizacji podsieci w pędzącym pociągu) jest różny, jednak konstrukcja sieci musi przewidywać szereg możliwych sytuacji związanych z przenoszeniem połączenia zarówno wewnątrz pojedynczych komórek, pomiędzy nimi, jak również pomiędzy centralami i pomiędzy poszczególnymi segmentami sieci (np. między segmentem prywatnym a publicznym oraz pomiędzy segmentem naziemnym i satelitarnym). Problem przenoszenia połączenia jest jednym z trudniejszych i ważniejszych zadań dla dobrze działającej sieci systemu UMTS ze względu na jej komplikację.

Radiodyfuzja

Radiodyfuzja jest rodzajem usługi telekomunikacyjnej, polegającej na dostarczaniu do odbiorców (abonentów) systemu radiokomunikacyjnego sygnału w układzie rozsiewczym, tj.: do wielu odbiorców jednocześnie. Usługa taka ma z zasady charakter jednokierunkowy: centrum nadawcze - duża grupa odbiorców (sygnały w przeciwnym kierunku wykorzystują inne systemy łączności). Dostarczanie sygnału do odbiorców może odbywać się przy pomocy fal radiowych (telewizja, radiofonia) lub sieci kablowych (telewizja kablowa).

Radiofonia i telewizja

Struktura sieci radiofonicznej i telewizyjnej jest podobna: centrum nadawcze - studio radiowe lub telewizyjne - przesyła sygnał w sieci telekomunikacyjnej (liniami radiowymi lub kablowymi) do zespołu radiowych stacji nadawczych. Radiowe stacje nadawcze rozmieszczone na obszarze kraju emitują sygnał, który dociera do abonentów (praktycznie na obszarze całego kraju). W celu uniknięcia wzajemnych zakłóceń, poszczególne stacje nadawcze mają odpowiednio dobrane częstotliwości pracy.

W ogólnopolskich sieciach radiowych i telewizyjnych właścicielem zespołu stacji nadawczych (a także linii transmisyjnych i niektórych centrów nadawczych) jest TP S.A., od której właściciele programów „dzierżawią czas antenowy".

Potencjał sieci radiowych i telewizyjnych przedstawia się następująco:

1. Radio UKF:
   - stacje nadawcze ok. 260
   - nadajniki radiowe ok. 350 o łącznej mocy ok. 1,5 MW
2. Radio KF:
   - stacje nadawcze 6
   - nadajniki radiowe 6 o łącznej mocy ok. 0,6 MW
3. Radio - fale długie:
   - stacje nadawcze 1
   - nadajniki radiowe 1 o mocy ok. 0,5 MW
4. Telewizja:
   - stacje nadawcze ok. 140 , w tym 60 stacji o mocy powyżej 5 kW,
   - nadajniki telewizyjne ok. 210 , w tym 96 nadajników o mocy powyżej 5 kW,
   - stacje przemienników ok. 250,
   - nadajniki telewizyjne ok. 300.

Radiodyfuzja w systemach satelitarnych

Uzupełnieniem systemów rozsiewczych pracujących na obszarze kraju są systemy łączności satelitarnej. W ramach tych systemów wyróżnić należy:

- systemy radiowe i telewizyjne, w których nadawane są programy radiowe i telewizyjne ze stacji nadawczych naziemnych poprzez satelity telekomunikacyjne, które emitują sygnał w kierunku ziemi w postaci wiązki (grupy wiązek) punktowej lub globalnej (szerokiej, obejmującej cały kontynent);
- systemy łączności satelitarnej dużego zasięgu (są to w zasadzie systemy porozumiewawcze, jednak ze względu na szerokość wiązek nadawanych z satelity do korespondentów ruchomych - statków - mają one cechy systemów radiofuzyjnych).

Określenie tych systemów jako satelitarne wynika z przebiegu nadawanych w nich sygnałów linią radiową, w której stacją retransmisyjną jest satelita telekomunikacyjny. Podobnie jak w systemach „naziemnych" źródłem sygnału może być centrum nadawcze - np.: studio telewizyjne (lub w systemach łączności satelitarnej - abonent publicznej sieci telekomunikacyjnej).

W Polsce w systemach tych pracuje kilka naziemnych stacji satelitarnych (w Psarach koło Kielc), obsługujących obszar Oceanu Atlantyckiego, Oceanu Indyjskiego i Europy.
W tabeli 4.2.2.2. przedstawione zostały wybrane systemy łączności satelitarnej.

Tabela 4.2.2.2.

Wybrane systemy łączności satelitarnej

Organizacja	Standard	Satelita	Usługi (obszar)	Szybkość TD (bit/s)	Główne zastosowanie
INMARSAT	A (1982)	MARECS, INMARSAT II	transmisja mowy, teleks, faks, TD	analogowa FM	statki, platformy wiertnicze, terminale przenośne
INMARSAT	B (1993)	MARECS, INMARSAT II	transmisja mowy, teleks, faks, TD	16 k (transmisja mowy)	zastąpienie INMARSAT-A
INMARSAT	C (1991)	MARECS, INMARSAT II	transmisja teleksowa z buforowaniem, TD, określanie pozycji (świat)	600	małe statki (jachty, kutry rybackie etc.), pojazdy ruchome
INMARSAT	M (1992/93)	MARECS, INMARSAT II	transmisja mowy, faks, TD	6,4 k (transmisja mowy) 2,4 k	terminale walizkowe, małe łodzie
INMARSAT	lotniczy (1992)	MARECS, INMARSAT II	transmisja mowy, faks, TD	300 9,6 k	samoloty komercyjne i prywatne
	AERO-C			600	
	AERO-L			600	
	AERO-H			10,5 k/4,8 k/-	
INMARSAT	D (1995)		transmisja sygnałów przywoławczych	brak danych	powiadamianie, zdalne sterowanie
QUALCOMM	Omni Tracs (1989)	GSTAR	dwukierunkowa trans. krótkich informacji, określanie pozycji (Ameryka Płn.)	5-15 k (w dół), 55-165 (w górę)	transport dalekosiężny
ALCATEL QUALCOMM	Eutel Tracs (1991)	EUTELSAT I-II	dwukierunkowa trans. informacji, określanie pozycji (Europa)	5-15 k (w dół), 55-165 (w górę)	transport dalekosiężny

4.3. Wewnętrzne sieci telekomunikacyjne

Poza publicznymi sieciami telekomunikacyjnymi na obszarze kraju występują także sieci świadczące usługi dla zamkniętych grup użytkowników - sieci wewnętrzne (resortowe). Ze względu na ich potencjał można podzielić je na dwie grupy:

1. Sieci autonomiczne, wykorzystujące do obsługi abonentów własne urządzenia transmisyjne i komutacyjne.
2. Sieci nie autonomiczne, współpracujące z sieciami publicznymi i wykorzystujące do obsługi swoich abonentów potencjał innych sieci (np.: linie transmisyjne). Do tej grupy należy m.in. stacjonarny system łączności sił zbrojnych.

W analizie potencjału systemu telekomunikacyjnego kraju istotne znaczenie mają więc te systemy, które nie bazują na zasobach innych systemów. Do takich systemów należą:

- sieć teleinformatyczna PKP - „Kolpak";
- sieci telekomunikacyjne energetyki.

4.3.1. Sieć teleinformatyczna PKP

Polskie Koleje Państwowe są użytkownikiem rozbudowanego systemu telekomunikacyjnego, który jest niezależny od publicznej sieci telekomunikacyjnej. System ten służy służbom utrzymania i eksploatacji, systemom sterowania sygnalizacji, kontroli ruchu kolei itp.

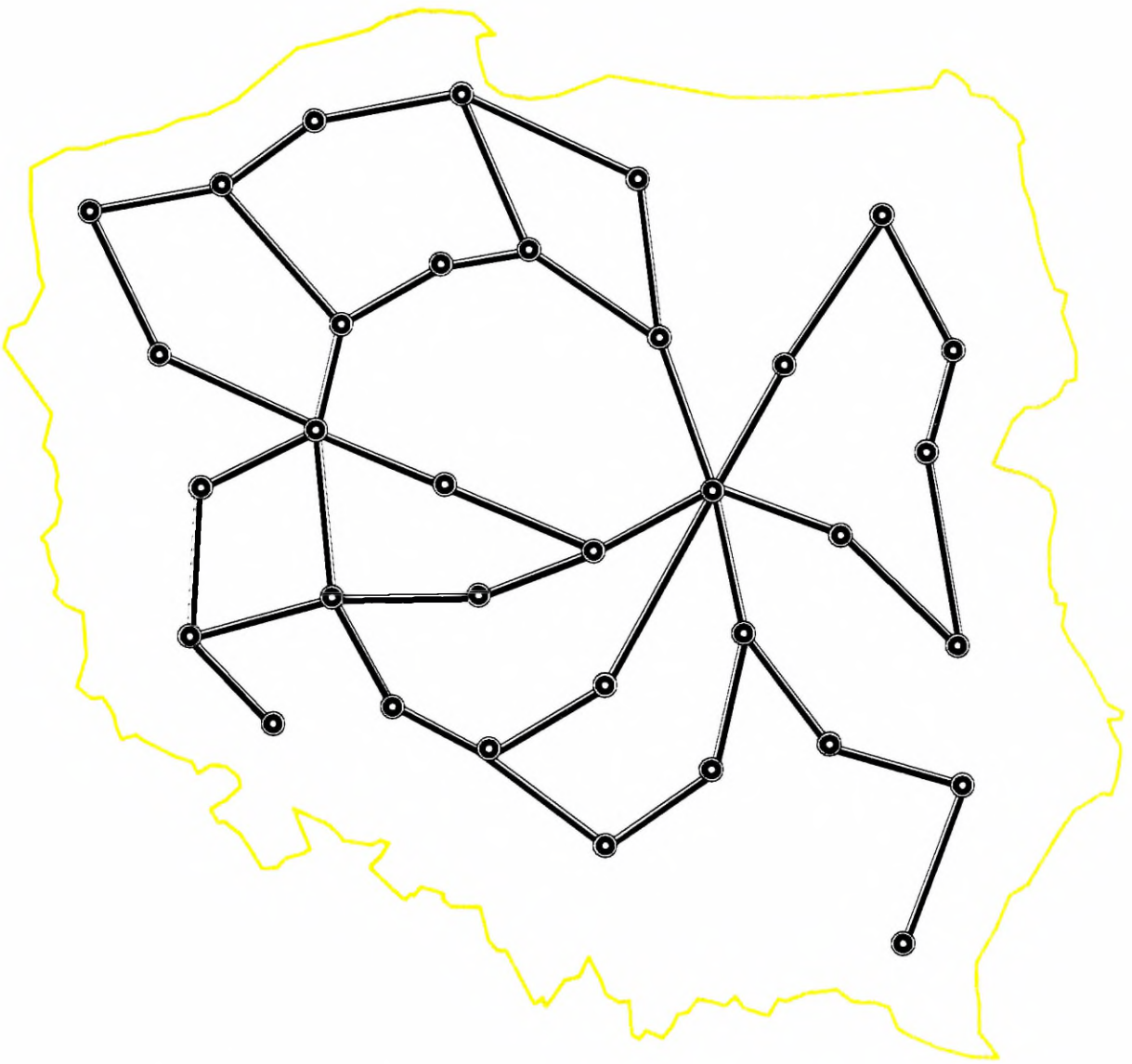
W skład sieci teleinformatycznej PKP "Kolpak" wchodzą:

- 7 węzłów głównych, zainstalowanych w dyrekcji generalnej PKP i w siedzibach dyrekcji okręgowych PKP,
- ok. 60 węzłów regionalnych rozmieszczonych w miejscach koncentracji ruchu,
- ok. 200 węzłów lokalnych,
- około 9600 portów,
- około 30 000 km linii transmisyjnych (przewodowych lub światłowodowych) biegnących wzdłuż tras kolejowych. Są to linie telekomunikacyjne PKP.

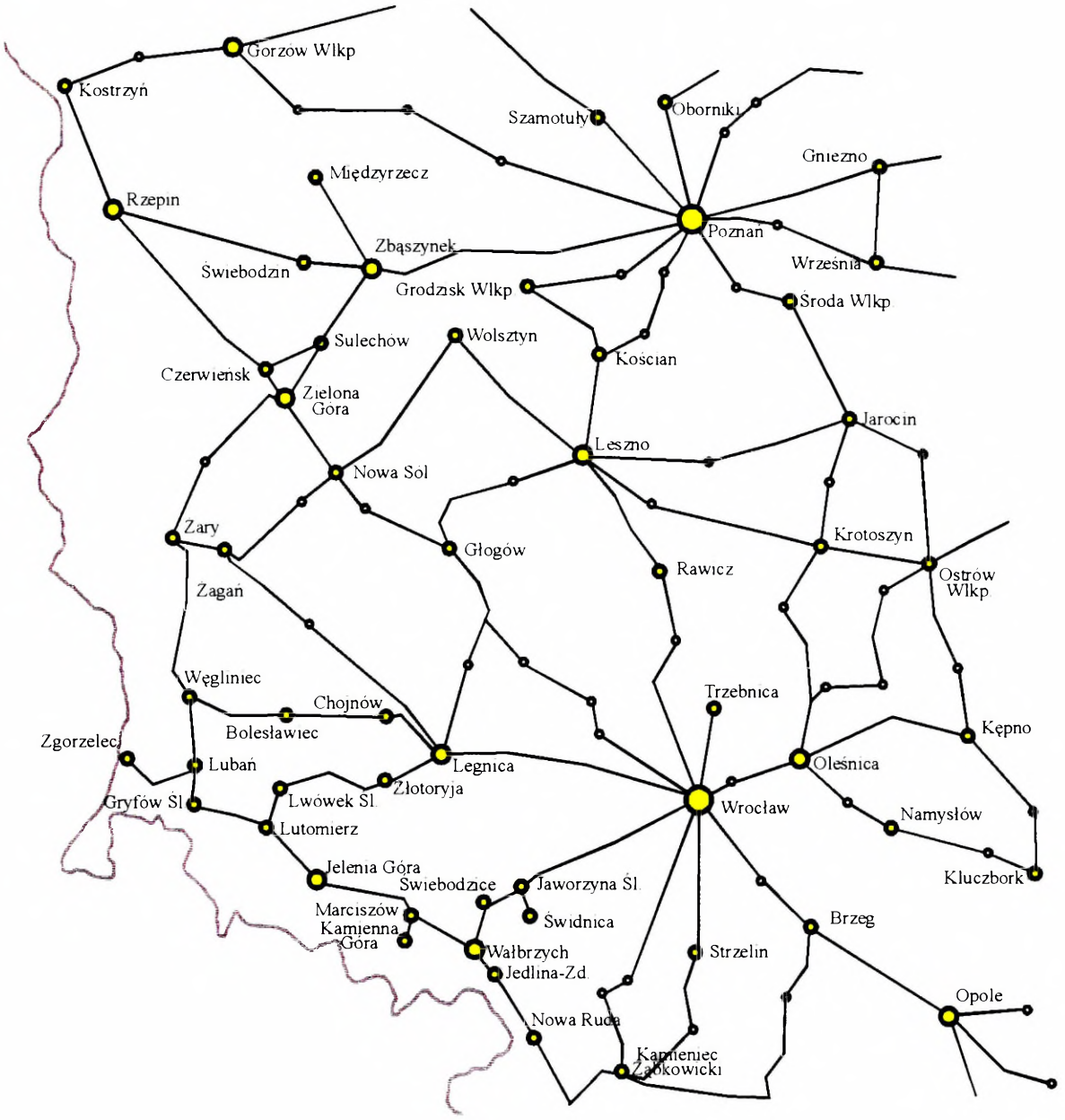
W strukturze sieci przewidziano połączenie ze sobą wszystkich węzłów głównych na zasadzie wieloboku zupełnego (każdy z każdym). Węzły regionalne są w drodze pierwszego wyboru przyłączone bezpośrednio do węzłów głównych lub niekiedy pośrednio poprzez inny węzeł regionalny. Węzły te mają, co najmniej dwie drogi dojścia do węzłów głównych.

Węzły lokalne są łączone w łańcuchy równoległe do przebiegu linii kolejowych (wzdłuż kolejowych szlaków komunikacyjnych), co zapewnia dostęp do wyższych poziomów sieci również, co najmniej dwiema drogami.

Węzły kategorii wyższych niż lokalne zapewniają działanie non - stop. Oznacza to, że w razie uszkodzenia jakiegoś modułu w węźle jego działanie przejmuje automatycznie inny moduł nadmiarowy, bez utraty informacji przekazywanych przez sieć. Węzły te mają budowę modularną umożliwiającą zwiększenie liczby portów odpowiednio do wzrastających potrzeb. Topologię sieci „Kolpak" przedstawiają rysunki 4.3.1.1. i 4.3.1.2.



Rys. 4.3.1.1. Topologia sieci teleinformatycznej „Kolpak" na obszarze kraju



Rys. 4.3.1.2. Topologia sieci teleinformatycznej „Kolpak" – szczegóły (fragment)

Do przekazywania danych między węzłami sieci wykorzystywane są łącza o przepustowościach 64 kbit/s, 2 Mbit/s i (kilka) o wyższych przepustowościach.

Zasadą działania sieci „Kolpak" jest komutacja pakietów. Do portów sieci można przyłączyć urządzenia działające w trybie synchronicznym i asynchronicznym, a przyłącza mogą być zarówno trwałe, jak i komutowane. Sieć umożliwia świadczenie dowolnych usług teleinformatycznych przez całą dobę z każdego miejsca, które ma dostęp do publicznej sieci telefonicznej, teleksowej lub portu sieci „Kolpak".

4.3.2. Sieci telekomunikacyjne Energetyki

Światłowodowa sieć telekomunikacyjna energetyki

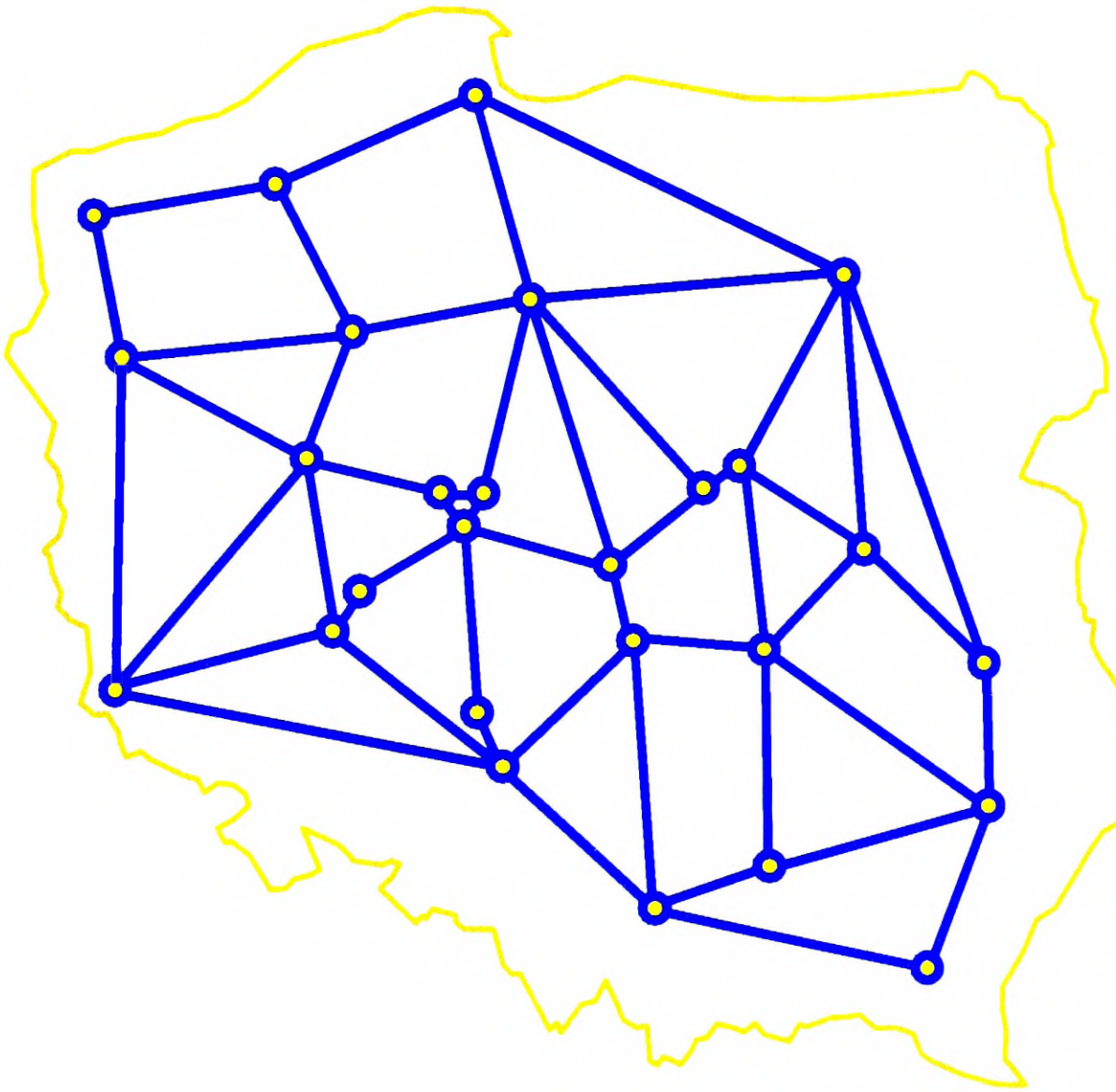
Polskie Sieci Energetyczne i zakłady energetyczne dysponują, praktycznie niezależną od sieci użytku publicznego, siecią telekomunikacyjną, której operatorem jest spółka z o.o. Telekomunikacja Energetyczna „Tel-energo".

Przeznaczeniem sieci jest przede wszystkim zapewnienie bezpiecznego sterowania systemem elektroenergetycznym i świadczenie usług telekomunikacyjnych dla potrzeb jednostek organizacyjnych energetyki zawodowej. Jest ona nowoczesną cyfrową siecią zintegrowaną pracującą w 100%, jako jedyna w sieć w kraju, w standardzie SDH. W skład sieci „Tel-energo" wchodzą:

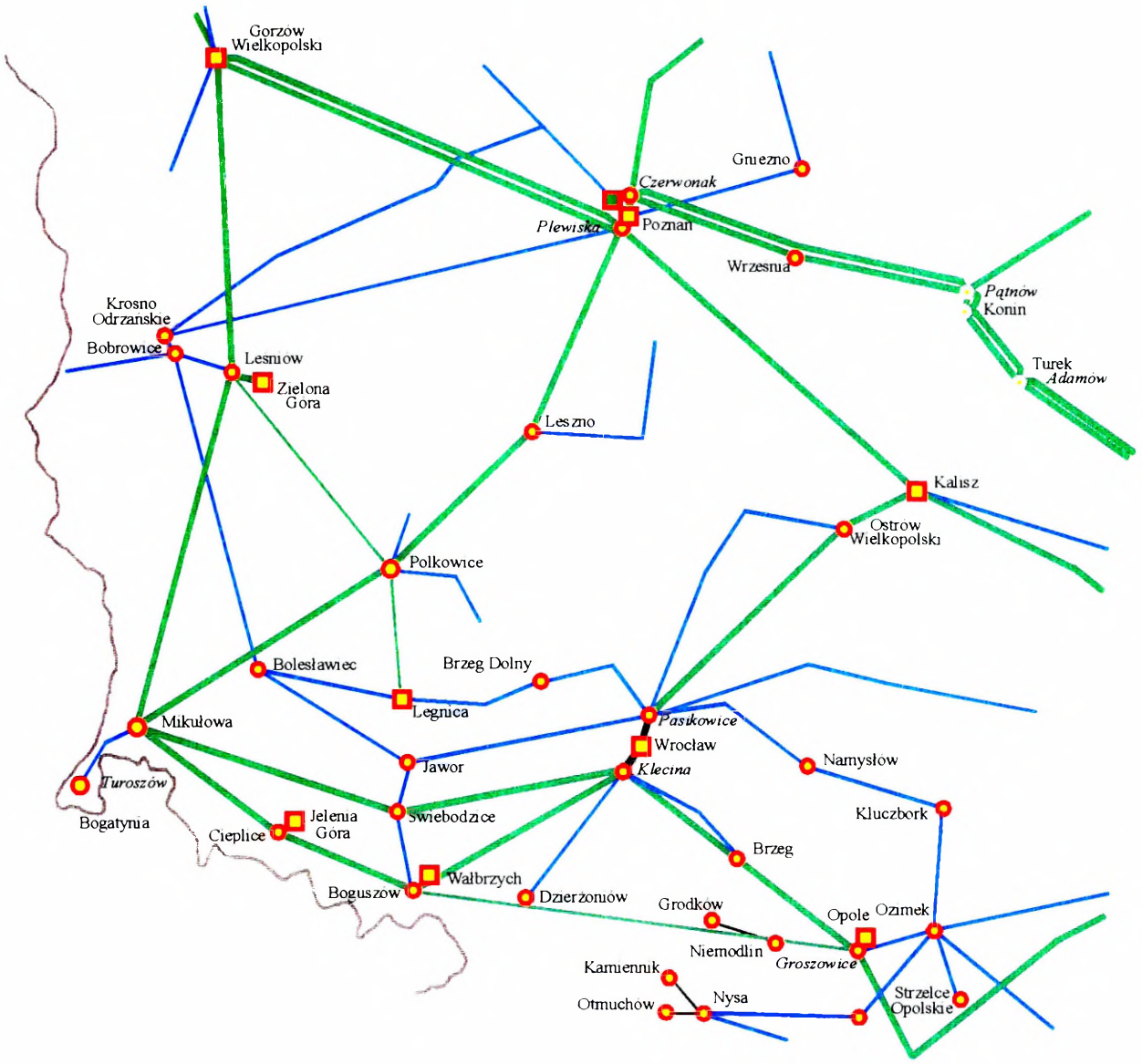
- ok. 40 węzłów komutacyjnych, zainstalowanych w oddziałach eksploatacji sieci przesyłowej i zakładach energetycznych,
- ok. 130 węzłów teletransmisyjnych, zainstalowanych w stacjach energetycznych,
- węzły transmisyjne (kilkaset) w elektrowniach o mocy powyżej 50 MW, węzłach sieci 400 i 220 kV, ważniejszych stacjach 110/15 kV,
- kable optotelekomunikacyjne napowietrzne (różnej technologii: w przewodach energetycznych, zerowych, odgromowych i samonośnych) w liniach przesyłowych wysokich napięć (ok. 6500 km),
- kable optotelekomunikacyjne napowietrzne (różnej technologii) w liniach przesyłowych wysokich i średnich napięć (w sieciach regionalnych zakładów energetycznych - kilkanaście tys. km),
- kable optotelekomunikacyjne podziemne własności „Tel-energo" (kilkaset km),
- trakty cyfrowe dzierżawione z TP S.A. (niewielkie ilości dzierżawione do czasu zakończenia budowy własnych linii energetyki).

W sieci przewidziano połączenie ze sobą wszystkich węzłów w struktury pierścieniowe zapewniające istnienie rezerwowych dróg transmisyjnych. 7 takich pierścieni tworzy sieć bazową energetyki. W sieci bazowej energetyki w każdym pierścieniu zastosowano urządzenia o przepustowości 622 Mbit/s (przepustowość równoważna 252 traktom 2 Mbit/s lub 7560 kanałom 64 kbit/s).

Sieć bazowa uzupełniona jest traktami światłowodowymi lub przewodowymi o przepustowościach 622 lub 155 Mbit/s (tzw. sieci szkieletowej). Do sieci bazowej, poprzez stacje telekomunikacyjne znajdujące się w jej strukturze, włączone są sieci regionalne zakładów energetycznych. Sieci regionalne budowane są z wykorzystaniem kabli światłowodowych na liniach energetycznych niższych napięć (110 i 15 kV) w technologii SDH z przepustowością 155 Mbit/s. Łącznie w sieci bazowej i w sieciach regionalnych na obszarze kraju zbudowanych jest około 50 000 km linii telekomunikacyjnych. Topologię sieci „Tel-energo" przedstawiają rysunki 4.3.2.1. i 4.3.2.2.



Rys. 4.3.2.1. Telekomunikacyjna sieć światłowodowa energetyki



Rys. 4.3.2.2. Telekomunikacyjna sieć światłowodowa energetyki

(fragment sieci szkieletowej)

Przy budowie sieci „Tel-energo" zastosowano kable światłowodowe o profilu minimum 12 włókien, co umożliwia, poprzez zastosowanie dodatkowych urządzeń w stacjach teletransmisyjnych, znaczne zwiększenie możliwości transmisyjnych sieci bez konieczności budowy nowych linii.

Zastosowanie kabli światłowodowych umożliwiło zwiększenie odległości międzyregeneratorowych do około 60÷100 km, dzięki czemu większość łączy w sieci posiada regeneratory wyłącznie w stacjach końcowych (w węzłach sieci). Jednakże umożliwia to włączenie się do sieci wyłącznie w węzłach sieci lub w punktach abonenckich.

Sieć „Tel-energo" dzięki posiadaniu własnych linii transmisyjnych i własnych urządzeń komutacyjnych jest, podobnie jak sieć „Kolpak", siecią całkowicie niezależną od publicznej sieci telekomunikacyjnej.

Sieć energetyki z zasady jest siecią resortową. Jej połączenia z siecią publiczną TP S.A. zrealizowane zostały w punktach KDM i ODM[10].

Sieć intranetowa energetyki

W energetyce występuje zapotrzebowanie na odrębne sieci intranetowe, których organizatorami i administratorami będą poszczególne przedsiębiorstwa energetyki, co nie oznacza konieczności tworzenia odrębnych sieci komputerowych.

Obszary działalności w energetyce, w których celowe jest zastosowanie intranetu, to:

- rynek energii elektrycznej, który będzie wymagał systemu obsługi giełdy docierającego do wszystkich zainteresowanych jednostek energetycznych na terenie całego kraju;
- funkcjonowanie agencji regulacji rynku energii elektrycznej;
- funkcjonowanie Polskich Sieci Elektroenergetycznych oraz Pionu Dyspozycji Mocy ze względu na rozproszony charakter PSE S.A. i konieczność bieżącej współpracy z jednostkami energetycznymi;
- zastosowanie intranetu do informacji procesów organizacyjnych;
- funkcjonowanie spółek dystrybucyjnych i powiązanych z nimi przedsiębiorstw;
- usprawnienie prac projektowych, procesów uzgodnień prowadzonych przez projektantów, wykonawców i użytkowników;
- tworzenie elektronicznych giełd towarów i usług świadczonych na rzecz jednostek energetycznych; kształcenie ustawiczne i szkolenie na odległość; tworzenie baz danych o zasięgu krajowym i integracja z nimi istniejących baz lokalnych zarówno relacyjnych, jak i multimedialnych;
- usprawnienie komunikacji między pracownikami energetyki oraz wewnętrzna publikacja informacji.

Budowana sieć korporacyjna będzie podstawą do tworzenia sieci intranetowych o różnym zasięgu. Zasięg informacji w intranecie będzie określony na trzech nie wykluczających się płaszczyznach zgodnie ze strukturą geograficzną sieci, zgodnie z hierarchią dostępu oraz definiowany dla pojedynczego użytkownika.

Wykorzystanie

[10] Krajowa (Okręgowa) Dyspozycja Mocy.

Wykorzystanie telekomunikacyjnej sieci energetyki na potrzeby elektroenergetyki i firm z nią związanych nastąpi poprzez usługi zintegrowane w sieci komutowanej o zasięgu ogólnokrajowym. Sieć wykorzystywana jest także do transmisji sygnałów automatyki zabezpieczającej (Teleprotection), transmisji danych czasu rzeczywistego dla dyspozycyjnych systemów nadzoru, sterowania i optymalizacji EMS/SCADA (Energy Management System/Supervisory Control and Data Acquisition), transmisji danych o średnich i dużych prędkościach transmisji na potrzeby informatycznych systemów zarządzania eksploatacyjnego i administracyjnego MIS (Management Information System), transmisji danych na potrzeby rozliczeń obrotu energią elektryczną.

Istnienie sieci umożliwi wprowadzenie usługi wideo, a w tym wideokonferencji pomiędzy ośrodkami zarządzania eksploatacyjnego i administracyjnego w relacjach międzymiastowych oraz zdalny nadzór wideo nad obiektami energetycznymi.

Na podstawie zezwolenia Ministra Łączności NR Z-078(1)96 oraz Decyzji Nr T-316 TEL-ENERGO S.A. operator telekomunikacyjny energetyki świadczy klientom zewnętrznym usługi:

- dzierżawy cyfrowych łączy o przepustowości:
- 64 kbit/s i ich wielokrotności,
- 2 Mbit/s i ich wielokrotności,
- 34 Mbit/s,
- 155 Mbit/s,
- dzierżawy „ciemnych włókien".

Sieć radiotelefoniczna energetyki

Drugim operatorem sieci telekomunikacyjnych energetyki w zakresie radiokomunikacji ruchomej lądowej (rrl) jest Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej (PTPiREE). Zarządza ono siecią radiotelefoniczną energetyki.

Sieć radiotelefoniczna energetyki obejmuje zbiór radiotelefonów bazowych umieszczonych w zakładach energetycznych, elektrowniach, rozdzielniach mocy i ważniejszych stacjach energetycznych oraz zmienny zbiór urządzeń abonenckich u abonentów ruchomych. Sieć radiotelefoniczna energetyki pracuje w systemie trakingowym w paśmie 450 MHz i obejmuje swoim zasięgiem prawie cały obszar kraju. Abonenci radiotelefoniczni energetyki mogą uzyskać połączenie na ok. 90% powierzchni Polski. Dostęp abonentów ruchomych do sieci „Tel-energo" zapewniony jest poprzez urządzenia stacji bazowych.

W powyższym rozdziale na podstawie wyników przeprowadzonych badań przedstawiony został potencjał sieci telekomunikacyjnych funkcjonujących na obszarze kraju, a mogących świadczyć usługi telekomunikacyjne na potrzeby reagowania kryzysowego. Scharakteryzowane zostały sieci o zasięgu krajowym i dużych możliwościach usługowych. Celowo pominięte zostały te sieci (i operatorzy usług telekomunikacyjnych), które większość swoich zasobów (szczególnie zasobów transmisyjnych) dzierżawią z innych, opisanych powyżej, sieci.

5. PODSYSTEM ŁĄCZNOŚCI W SYSTEMIE KIEROWANIA REAGOWANIEM KRYZYSOWYM

ppłk dr inż. Zbigniew FIOŁNA

Duże znaczenie dla efektywnej realizacji zadań służb ratownictwa i zarządzania kryzysowego ma struktura, baza technologiczna i zasady organizacyjne systemu telekomunikacyjnego, stanowiącego podłoże transportowe wszelkiego typu informacji. Struktura i procedury działania systemu telekomunikacyjnego dedykowanego dla potrzeb obsługi sytuacji kryzysowych, wspomagania działań ratowniczych i zarządzania kryzysowego jest ściśle związana z zadaniami i organizacją służb ratownictwa i zarządzania kryzysowego, oraz jest zależna od obowiązujących uregulowań prawnych.

Technologie telekomunikacyjne z uwagi na swoje właściwości użytkowe i ograniczenia aplikacyjne umożliwiają pełniejsze, bądź tylko zadawalające, wspomaganie funkcji i zadań realizowanych przez służby ratownicze i zarządzania kryzysowego.

Systemy wspomagania zarządzania kryzysowego w zależności od przeznaczenia, zakresu funkcjonowania i czasu działania muszą być zasilane informacyjnie z różnych źródeł i przekazywać wypracowane decyzje oraz inne istotne informacje do podległych służb, współpracujących organów kierowania i nadrzędnych instytucji państwowych. Informacje dedykowane dla systemu oraz informacje przekazywane od niego do otoczenia mają różną postać (rozmowa telefoniczna, plik tekstowy ASCII, dokument sformalizowany, strumień wideo, itp.) i objętość (kilka bajtów, MB) oraz wymagają różnego sposobu obsługi (obsługa w czasie rzeczywistym, obsługa nie uwarunkowana czasowo, itp.) i zapewnienia różnych stopni bezpieczeństwa, itp.

Dla systemu telekomunikacyjnego oznacza to:

- konieczność bezstratnej obsługi strumieni ruchu o różnym charakterze i różnym natężeniu;
- dużą zdolność adaptacyjną do zmiennych w czasie i przestrzeni warunków (większość użytkowników jest mobilna, nieznany jest czas, miejsce, zasięg, zakres wystąpienia sytuacji kryzysowej);
- dużą żywotność;
- wysoką niezawodność i gotowość działania.

System telekomunikacyjny mogący sprostać tak poważnym wymaganiom powinien być efektywnie zarządzany, co pozwoli na ciągłe monitorowanie stanu zdatności zasobów, wykrywanie uszkodzeń, predykcję i eliminowanie przeciążeń, dynamiczną alokację zasobów systemu do zadań.

Dostępne dzisiaj technologie telekomunikacyjne zapewniają możliwość stworzenia optymalnej z punktu widzenia systemu wspomagania zarządzania kryzysowego platformy transportowej. Wymaga to jednak zapoznania się z ich charakterystyką techniczno-użytkową, a zwłaszcza zdania sobie sprawy z ograniczeń ich zastosowania.

5.1. Obowiązki operatora telekomunikacyjnego związane z reagowaniem i zarządzaniem kryzysowym

W systemie prawnym Rzeczpospolitej Polskiej obowiązują następujące akty prawne, mające określony wpływ na organizację i działanie podsystemu telekomunikacyjnego dla potrzeb zarządzania kryzysowego:

1) Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2002 r. Nr 21, poz. 205, Nr 74, poz. 676, Nr 81, poz. 732, Nr 113, poz. 984 i 985, Nr 156, poz. 1301, Nr 166, poz. 1363, Nr 199, poz. 1673, Nr 200, poz. 1679, 1687 i 1689).
2) Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (Dz.U.91.88.400 z późn. zm.).
3) Ustawa z dnia 5 czerwca 1998 r. o administracji rządowej w województwie (Dz. U. z 2001 r. Nr 80, poz.872 i Nr 128, poz. 1407, z 2002 r. Nr 37, poz. 329, Nr 41, poz. 365, Nr 62, poz. 558, Nr 89, poz. 804 i Nr 200, poz. 1688, z 2003 r. Nr 52, poz. 450).
4) Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800).
5) Ustawa z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. Nr 122, poz. 1320 i Nr 188, poz. 1571).
6) Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. Nr 62, poz. 558).
7) Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz. U. Nr 113, poz. 850).
8) Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. Nr 156, poz. 1301).

9) Ustawa z dnia 22 listopada 2002 r. o wyrównywaniu strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela (Dz. U. Nr 233, poz. 1955 r.).
10) Rozporządzenie Rady Ministrów z dnia 28 września 1993 r. w sprawie powszechnej samoobrony ludności (Dz. U. 91, poz. 421).
11) Rozporządzenie Rady Ministrów z dnia 28 września 1993 r. w sprawie obrony cywilnej (Dz. U. Nr 93, poz. 429).
12) Rozporządzenie Ministra Łączności z dnia 7 czerwca 2001 r. w sprawie szczegółowego trybu sporządzania przez operatorów publicznych planu działań w sytuacjach szczególnych zagrożeń oraz jego aktualizacji. (Dz. U. Nr 66, poz. 667).
13) Rozporządzenie Rady Ministrów z dnia 5 lutego 2002 r. w sprawie świadczeń na rzecz obrony (Dz. U. Nr 18, poz.168).
14) Rozporządzenie Rady Ministrów z dnia 21 maja 2002 r. w sprawie militaryzacji jednostek organizacyjnych wykonujących zadania na rzecz obronności lub bezpieczeństwa państwa (Dz. U. Nr 78, poz. 707).
15) Rozporządzenie Rady Ministrów z dnia 25 czerwca 2002 r. w sprawie szczegółowego zakresu działania Szefa Obrony Cywilnej Kraju, szefów obrony cywilnej województw, powiatów i gmin (Dz. U. Nr 96, poz. 850).
16) Rozporządzenie Rady Ministrów z dnia 3 grudnia 2002 r. w sprawie sposobu tworzenia gminnego zespołu reagowania, powiatowego i wojewódzkiego zespołu reagowania kryzysowego oraz Rządowego Zespołu Koordynacji Kryzysowej i ich funkcjonowania (Dz. U. Nr 215, poz. 1818).

Szczegółowo zobowiązania operatorów telekomunikacyjnych i podmiotów świadczących usługi telekomunikacyjne związane z reagowaniem i zarządzaniem kryzysowym uregulowano w następujących aktach prawnych:

1) Ustawa z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne" (Dz.U. z 2004 r. Nr 171, poz. 1800).
2) Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. Nr 62, poz. 558).
3) Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz. U. Nr 113, poz. 850).
4) Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. Nr 156, poz. 1301).

5) Rozporządzenie Ministra Łączności z dnia 7 czerwca 2001 r. w sprawie szczegółowego trybu sporządzania przez operatorów publicznych planu działań w sytuacjach szczególnych zagrożeń oraz jego aktualizacji. (Dz. U. Nr 66, poz. 667).

Poniżej przytoczono w dosłownym brzmieniu te części ww. aktów prawnych, które nakładają na operatorów telekomunikacyjnych i podmioty świadczące usługi telekomunikacyjne zobowiązania w zakresie reagowania i zarządzania kryzysowego.

Z Ustawy z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne" (Dz.U. z 2004 r. Nr 171, poz. 1800), która weszła w życie dnia 03 września 2004 r., wynika, że określa ona min. prawa i obowiązki przedsiębiorców telekomunikacyjnych oraz ich zadania i obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji.

Oznacza to, że jest to podstawowy akt prawny regulujący działania w dziedzinie telekomunikacji oraz określający obowiązki, zobowiązania podmiotów działających na rynku telekomunikacyjnym w zakresie udostępniania zasobów w czasie kryzysu i związane z tym należności.

W obowiązującej Ustawie z dnia 16 lipca 2004 r. „Prawo telekomunikacyjne" (Dz.U.Nr 171 poz. 1800) wynika min., że jej celem było stworzenie warunków dla ochrony interesu państwa w zakresie obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Wobec dużych niejasności i braku delegacji wykonawczych dostrzeżonych w czasie funkcjonowania jej poprzedniczki z 2000 r., ustawodawca w nowej ustawie kwestiom powinnościom operatorów telekomunikacyjnych związanych z bezpieczeństwem poświęcił DZIAŁ VIII „ Obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego".

W artykule 176 niniejszej ustawy określono zakres działań operatorów telekomunikacyjnych związanych z projektowaniem i planowaniem infrastruktury sieci telekomunikacyjnych, uwzględniających potrzeby w obszarze bezpieczeństwa publicznego i obronności państwa, w szczególności stwierdzono, że:

1. Przedsiębiorcy telekomunikacyjni, w celu zapewnienia ciągłości świadczenia usług telekomunikacyjnych, są obowiązani uwzględniać przy planowaniu, budowie, rozbudowie, eksploatacji lub łączeniu sieci telekomunikacyjnych możliwość wystąpienia sytuacji szczególnych zagrożeń, a w szczególności wprowadzenia stanu nadzwyczajnego.

2. Przedsiębiorcy telekomunikacyjni, z zastrzeżeniem ust. 4 pkt 2, są obowiązani posiadać aktualny plan działań w sytuacjach szczególnych zagrożeń, zwany dalej "planem", dotyczący w szczególności:

a) wzajemnej współpracy przedsiębiorców telekomunikacyjnych;

b) współpracy przedsiębiorców telekomunikacyjnych z organami koordynującymi działania ratownicze, służbami ustawowo powołanymi do niesienia pomocy oraz podmiotami, o których mowa w art. 177 ust. 1;

c) współpracy przedsiębiorców telekomunikacyjnych z zagranicznymi operatorami telekomunikacyjnymi, a w szczególności państw sąsiadujących;

d) przygotowania wskazanych elementów sieci telekomunikacyjnych dla zapewnienia telekomunikacji na potrzeby systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa;

e) zabezpieczania publicznych sieci telekomunikacyjnych i urządzeń telekomunikacyjnych przed zakłóceniami, skutkami katastrof i klęsk żywiołowych oraz nieuprawnionym dostępem;

f) zachowania ciągłości świadczenia usług telekomunikacyjnych, zwłaszcza dla służb ustawowo powołanych do niesienia pomocy;

g) zapewnienia połączeń telekomunikacyjnych na zasadach preferencyjnych dla podmiotów, o których mowa w art. 177 ust. 1, według określonych priorytetów;

h) sposobu wykonywania przez przedsiębiorców telekomunikacyjnych i osoby eksploatujące urządzenia telekomunikacyjne świadczeń rzeczowych przewidzianych w ustawie;

i) ewidencji i gromadzenia rezerw.

3. Prezes Urzędu Regulacji Telekomunikacji i Poczty może, w drodze decyzji, nakazać przedsiębiorcy telekomunikacyjnemu uzupełnienie planu lub dostosowanie stanu faktycznego do stanu zgodnego z planem.

4. Minister właściwy do spraw łączności, w drodze rozporządzenia:

a) określi tryb sporządzania, aktualizacji oraz zawartość planu,

b) może określić rodzaje przedsiębiorców telekomunikacyjnych nie podlegających obowiązkowi sporządzania planu - mając na uwadze zakres świadczonych usług telekomunikacyjnych, a także wymagania, o których mowa w ust. 2.

W artykule 177 określono zakres działań operatorów telekomunikacyjnych realizowanych w sytuacjach szczególnych zagrożeń, związanych z udostępnianiem infrastruktury sieci telekomunikacyjnej dla potrzeb instytucji i służb państwa, uczestniczących w reagowaniu i zarządzaniu kryzysowym.

W szczególności określono, że:

1. W sytuacjach szczególnych zagrożeń przedsiębiorcy telekomunikacyjni podejmują niezwłocznie działania określone w planie, utrzymując lub odtwarzając świadczenie usług telekomunikacyjnych, przede wszystkim organom koordynującym działania ratownicze i służbom ustawowo powołanym do niesienia pomocy oraz innym podmiotom realizującym zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, a w następnej kolejności pozostałym użytkownikom.
2. Minister właściwy do spraw wewnętrznych, w porozumieniu z Ministrem Obrony Narodowej i ministrem właściwym do spraw łączności po zasięgnięciu opinii Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Agencji Wywiadu, określi, w drodze rozporządzenia, kategorie użytkowników oraz priorytety, a także tryb i zasady ustalania kolejności odtwarzania świadczenia usług telekomunikacyjnych, mając na uwadze rodzaje możliwych zagrożeń oraz działań niezbędnych do przeciwdziałania ich skutkom.
3. Przedsiębiorcy telekomunikacyjni są obowiązani do nieodpłatnego udostępniania urządzeń telekomunikacyjnych niezbędnych do przeprowadzenia akcji ratowniczej innym przedsiębiorcom telekomunikacyjnym, użytkownikom oraz organom, służbom i podmiotom, uczestniczącym w reagowaniu i zarządzaniu kryzysowym, z zachowaniem zasady minimalizowania negatywnych skutków takiego udostępniania urządzeń dla ciągłości świadczenia usług i dla działalności gospodarczej przedsiębiorcy telekomunikacyjnego.
4. Przepisy ustępów 1-3 stosuje się także wobec osób używających radiowe urządzenia nadawcze lub nadawczo-odbiorcze, wykorzystywane w służbach radiokomunikacyjnych.
5. Przepisy ustępów 1-4 stosuje się odpowiednio podczas działań ratunkowych lub łagodzenia skutków katastrof o zasięgu międzynarodowym, co najmniej w zakresie ustalonym umowami międzynarodowymi, których Rzeczpospolita Polska jest stroną.

W artykule 178 i 179 określono obowiązki, jakie mogą zostać nałożone na operatora telekomunikacyjnego w sytuacji szczególnego zagrożenia oraz wskazano podmioty na rzecz, których poszczególne działania powinny być świadczone, zasady i tryb ich realizacji.

W artykule 178 określono, że:

1. W sytuacji wystąpienia szczególnego zagrożenia Prezes Urzędu Regulacji Telekomunikacji i Poczty może, w drodze decyzji, nałożyć na przedsiębiorców telekomunikacyjnych obowiązki dotyczące:
   a) utrzymania ciągłości świadczenia usług telekomunikacyjnych, w tym realizacji połączeń telekomunikacyjnych na zasadach preferencyjnych;
   b) ograniczenia niektórych, publicznie dostępnych usług telekomunikacyjnych;
   c) ograniczenia zakresu lub obszaru eksploatacji sieci telekomunikacyjnych i urządzeń telekomunikacyjnych, używania urządzeń radiowych, z wyłączeniem urządzeń używanych przez podmioty, takie jak:
      - komórki organizacyjne i jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane oraz organy i jednostki organizacyjne nadzorowane lub podległe ministrowi właściwemu do spraw wewnętrznych,
      - organy i jednostki organizacyjne podległe ministrowi właściwemu do spraw wewnętrznych,
      - jednostki sił zbrojnych obcych państw oraz jednostki organizacyjne innych zagranicznych organów państwowych, przebywające czasowo na terytorium Rzeczypospolitej Polskiej na podstawie umów, których Rzeczpospolita Polska jest stroną,
      - jednostki organizacyjne Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu,
      - jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych,
      - przedstawicielstwa dyplomatyczne, urzędy konsularne, zagraniczne misje specjalne oraz przedstawicielstwa organizacji międzynarodowych, korzystające
        z przywilejów i immunitetów na podstawie ustaw, umów i zwyczajów międzynarodowych, mające swe siedziby na terytorium Rzeczypospolitej Polskiej,
      - jednostki organizacyjne Służby Więziennej,

- komórki organizacyjne przeprowadzające czynności wywiadu skarbowego, które wchodzą w skład jednostek organizacyjnych kontroli skarbowe nadzorowanych lub podległych ministrowi właściwemu do spraw finansów publicznych,

d) nakazu nieodpłatnego świadczenia, w określonym zakresie, publicznie dostępnych usług telefonicznych z aparatów publicznych - kierując się rozmiarem zagrożenia i potrzebą ograniczenia jego skutków, z zachowaniem zasady minimalizowania negatywnych skutków nałożonych obowiązków dla ciągłości świadczenia usług i dla działalności gospodarczej przedsiębiorcy telekomunikacyjnego. Decyzji nadaje się rygor natychmiastowej wykonalności.

2. Decyzja Prezesa Urzędu Regulacji Telekomunikacji i Poczty nakładająca na przedsiębiorców telekomunikacyjnych ograniczenia, o których mowa w ust. 1, wydawana jest z urzędu lub na wniosek prokuratora, Komendanta Głównego Policji, komendanta wojewódzkiego Policji, Komendanta Głównego Straży Granicznej, Komendanta Głównego Żandarmerii Wojskowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, Szefa Wojskowych Służb Informacyjnych lub Szefa Biura Ochrony Rządu.
3. W sytuacji wystąpienia szczególnego zagrożenia organy, o których mowa w ust. 2, mogą podjąć decyzję o zastosowaniu urządzeń uniemożliwiających wykonywanie na określonym obszarze połączeń telefonicznych za pośrednictwem ruchomej publicznej sieci telefonicznej, informując Prezesa Urzędu Regulacji Telekomunikacji i Poczty o podjętych działaniach.

W artykule 179 określono, że:

1. Przedsiębiorcy telekomunikacyjni są obowiązani do wykonywania zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w zakresie i na warunkach określonych w niniejszej ustawie i w przepisach odrębnych.
2. Przedsiębiorca telekomunikacyjny jest obowiązany do wykonywania zadań i obowiązków w zakresie przygotowania i utrzymywania wskazanych elementów sieci telekomunikacyjnych dla zapewnienia telekomunikacji na potrzeby systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa realizowanych na zasadach określonych w planach, decyzjach lub umowach zawartych między przedsiębiorcami telekomunikacyjnymi a uprawnionymi podmiotami.

3. Zadania i obowiązki, o których mowa w ustępie 1, dotyczą zapewnienia na koszt przedsiębiorcy telekomunikacyjnego:
   a) w szczególności technicznych i organizacyjnych warunków jednoczesnego i wzajemnie niezależnego:
      - dostępu do wskazywanych treści przekazów telekomunikacyjnych i posiadanych przez przedsiębiorcę telekomunikacyjnego danych, dotyczących użytkownika, danych związanych ze świadczoną usługą telekomunikacyjną,
      - utrwalania treści i danych, o których mowa w lit. a - przez uprawnione jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, uprawnione organy i jednostki organizacyjne nadzorowane lub podległe ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw finansów publicznych oraz Szefowi Agencji Bezpieczeństwa Wewnętrznego i Szefowi Agencji Wywiadu;
   b) utrwalania treści i danych, o których mowa w pkt 1 lit. a, na rzecz sądu lub prokuratora.
4. Dostęp, o którym mowa w ust. 3, może być realizowany także za pomocą interfejsów, na zasadach określonych w porozumieniach zawartych przez uprawnione podmioty z przedsiębiorcami telekomunikacyjnymi za zgodą: Ministra Sprawiedliwości, Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw finansów publicznych, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu, zgodnie z ich właściwością. Porozumienie może określać także współudział stron w kosztach zastosowania interfejsów.
5. Przedsiębiorca telekomunikacyjny zapewnia wykonanie zadań i obowiązków, o których mowa w ust. 3, począwszy od dnia rozpoczęcia działalności telekomunikacyjnej.
6. Prezes Urzędu Regulacji Telekomunikacji i Poczty w szczególnie uzasadnionych przypadkach może, na wniosek zainteresowanego przedsiębiorcy telekomunikacyjnego, odroczyć termin wykonywania zadań i obowiązków, o których mowa w ust. 3.
7. Przedsiębiorca telekomunikacyjny, który wykonuje działalność telekomunikacyjną za pośrednictwem sieci telekomunikacyjnej innego przedsiębiorcy telekomunikacyjnego, może zlecić temu przedsiębiorcy wykonywanie zadań i obowiązków, o których mowa w ust. 3. Zlecenie wykonywania zadań i obowiązków nie zwalnia zlecającego z odpowiedzialności za ich właściwą realizację.

8. Przedsiębiorca telekomunikacyjny jest obowiązany do wskazania Prezesowi Urzędu Regulacji Telekomunikacji i Poczty w terminie 60 dni od dnia wejścia w życie ustawy lub z dniem rozpoczęcia świadczenia usług telekomunikacyjnych:
   a) jednostki organizacyjnej lub osoby mającej siedzibę lub miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej, spełniającej wymagania określone odrębnymi przepisami, uprawnionej do reprezentowania przedsiębiorcy w sprawach związanych z wykonywaniem zadań i obowiązków, o których mowa w ust. 3;
   b) przedsiębiorcy telekomunikacyjnego, który będzie w jego imieniu realizował zadania i obowiązki, o których mowa w ust. 3.
9. Przedsiębiorca telekomunikacyjny świadczący publicznie dostępne usługi telekomunikacyjne jest obowiązany prowadzić elektroniczny wykaz abonentów, użytkowników lub zakończeń sieci, uwzględniając w nim dane uzyskiwane przy zawarciu umowy.
10. Prezes Urzędu Regulacji Telekomunikacji i Poczty przekazuje niezwłocznie informacje, o których mowa w ust. 8, Ministrowi Sprawiedliwości, Ministrowi Obrony Narodowej, ministrowi właściwemu do spraw wewnętrznych, ministrowi właściwemu do spraw finansów publicznych oraz Szefowi Agencji Bezpieczeństwa Wewnętrznego i Szefowi Agencji Wywiadu.
11. Przedsiębiorca telekomunikacyjny jest obowiązany do zapewnienia wykonywania zadań i obowiązków, o których mowa w ust. 3, z chwilą rozpoczęcia świadczenia nowej usługi telekomunikacyjnej.

W artykule 180 Ustawy „Prawo telekomunikacyjne" określono działania restrykcyjne operatora telekomunikacyjnego w stosunku do posiadanych zasobów, w szczególności:

1. Przedsiębiorca telekomunikacyjny jest obowiązany do niezwłocznego blokowania połączeń telekomunikacyjnych lub przekazów informacji, na żądanie uprawnionych podmiotów, jeżeli połączenia te mogą zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu albo do umożliwienia dokonania takiej blokady przez te podmioty.
2. Operator ruchomej publicznej sieci telefonicznej jest obowiązany do:
   a) uniemożliwienia użytkowania w jego sieci skradzionych telekomunikacyjnych urządzeń końcowych;

b) przekazywania informacji identyfikujących skradzione telekomunikacyjne urządzenia końcowe innym operatorom ruchomych publicznych sieci telefonicznych w celu realizacji przez nich czynności, o których mowa w pkt 1.

3. Czynności, o których mowa w ust. 2, dokonywane są przez operatora w terminie 1 dnia roboczego od dnia przedstawienia przez abonenta poświadczenia zgłoszenia kradzieży telekomunikacyjnego urządzenia końcowego, numeru identyfikacyjnego tego urządzenia i dowodu jego nabycia lub innych danych jednoznacznie identyfikujących właściciela tego urządzenia. W przypadku uzyskania informacji identyfikujących skradzione urządzenia od innego operatora, termin 1 dnia roboczego liczy się od tej daty.

Ponadto w Rozdziale 2 „Dostęp telekomunikacyjny" Ustawy „Prawo telekomunikacyjne, w artykule. 78 ustawodawca określił zasady udostępniania numeru alarmowego „112" i innych numerów alarmowych. Zostało to sformułowane w następujący sposób:

Operator publicznej sieci telefonicznej jest obowiązany, na każde żądanie służb ustawowo powołanych do niesienia pomocy, udostępniać, w miarę możliwości technicznych, w czasie rzeczywistym informacje dotyczące lokalizacji zakończenia sieci, z którego zostało wykonane połączenie do numeru alarmowego "112" oraz innych numerów alarmowych, umożliwiające niezwłoczne podjęcie interwencji.

Ponadto w dziale IV „Gospodarowanie numeracją", w artykule 129 ww. ustawy stwierdzono, że ustala się numer "112" jako wspólny numer alarmowy dla wszystkich służb ustawowo powołanych do niesienia pomocy.

Innym istotnym aspektem regulacji w Ustawie „Prawo telekomunikacyjne" jest zapewnienie warunków technicznych funkcjonowania instytucji i służb realizujących zadania z zakresu reagowania i zarządzania kryzysowego, obronności i porządku publicznego. Tym kwestiom poświęcone zostały artykuły:112, 123 z działu IV „Gospodarowanie częstotliwościami i numeracją" oraz artykuły 137 z działu VI „Infrastruktura, urządzenia telekomunikacyjne i urządzenia radiowe".

W artykule 112 określono, że plany zagospodarowania częstotliwości oraz ich zmiany uwzględniają w szczególności spełnianie wymagań dotyczących obronności i bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

W artykule 123. określono, że:

1. Rezerwacja częstotliwości może zostać zmieniona lub cofnięta, w drodze decyzji organu właściwego do jej dokonania, w przypadku min. wystąpienia okoliczności prowadzących do zagrożenia obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego;
2. W okresie ważności rezerwacji częstotliwości można odmówić wydania lub cofnąć pozwolenie radiowe na używanie urządzenia radiowego wykorzystującego częstotliwości objęte rezerwacją z tytułu wystąpienia m.in. zagrożenia obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego;
3. Odmowa udzielenia rezerwacji częstotliwości, jej zmiana lub cofnięcie w przypadku, zagrożenia obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, a także odmowa wydania pozwolenia radiowego lub jego cofnięcie z powodu tych okoliczności, następuje po zasięgnięciu opinii lub na wniosek Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu, w zakresie ich właściwości.

Artykuł 137 stanowi, że:

1. Operatorzy są obowiązani przekazywać Prezesowi Urzędu Regulacji Telekomunikacji i Poczty oraz udostępniać zainteresowanym podmiotom specyfikacje techniczne stosowanych zakończeń sieci, interfejsów radiowych i ich zmiany zanim usługi telekomunikacyjne, które mają być świadczone przez te zakończenia sieci lub interfejsy radiowe staną się dostępne dla użytkowników.
2. Specyfikacje techniczne, o których mowa w ust. 1, powinny być na tyle szczegółowe, aby umożliwiały zaprojektowanie telekomunikacyjnych urządzeń końcowych zdolnych do wykorzystywania wszystkich usług świadczonych przez dane zakończenie sieci lub interfejs radiowy i zawierać w szczególności informacje pozwalające producentom przeprowadzanie odpowiednich testów umożliwiających stwierdzenie czy telekomunikacyjne urządzenie końcowe spełnia odnoszące się do niego zasadnicze wymagania.

Aktami prawnymi regulującymi podstawowe zagadnienia związane z funkcjonowaniem państwa, podmiotów gospodarczych i obywateli w sytuacjach nadzwyczajnych są wspomniane wcześniej ustawy: „O stanie klęski żywiołowej", „O stanie wyjątkowym" oraz

„O stanie wojennym i kompetencjach Naczelnego Wodza Sił Zbrojnych RP". W nich zawarte są również uregulowania prawne nakładające obowiązki na operatorów telekomunikacyjnych.

Z Ustawy z dnia 18 kwietnia 2002 r. „O stanie klęski żywiołowej" Dziennik Ustaw Nr 62 Poz.558 wynikają poniżej określone postanowienia istotne dla funkcjonowania operatora telekomunikacyjnego.

W rozdziale 3 określającym zakres ograniczeń wolności i praw człowieka i obywatela stwierdzono w artykule 25:

1. Dla zapewnienia łączności na potrzeby działań ratowniczych mogą być wprowadzone ograniczenia w wykonywaniu pocztowych usług o charakterze powszechnym lub usług kurierskich.
2. Ograniczenia w pracy urządzeń radiowych nadawczych lub nadawczo-odbiorczych oraz w wykonywaniu usług telekomunikacyjnych określają odrębne przepisy.
3. Minister właściwy do spraw łączności może, w drodze rozporządzenia, wprowadzić ograniczenia, o których mowa w ust.1,oraz określić zakres tych ograniczeń

   z uwzględnieniem konieczności zapewnienia warunków pozwalających na sprawne zapobieganie lub zwalczanie skutków klęski żywiołowej przy jednoczesnym zminimalizowaniu uciążliwości wynikłych dla osób i podmiotów korzystających z pocztowych usług o charakterze powszechnym lub usług kurierskich.

W rozdziale 4 ustawodawca określił zakres i wysokość sankcji karnych za nie przestrzeganie przez operatorów postanowień zawartych w ustawie.

W artykule 27 stwierdzono:

Kto w czasie stanu klęski żywiołowej:

19) wbrew obowiązkowi określonemu w art.25 nie stosuje się do wprowadzonych ograniczeń w pracy urządzeń radiowych nadawczych lub nadawczo-odbiorczych, w wykonywaniu usług telekomunikacyjnych, pocztowych usług o charakterze powszechnym lub usług kurierskich, podlega karze aresztu albo grzywny.

Z ustawy „O stanie wyjątkowym" z dnia 21 czerwca 2002 r. Dziennik Ustaw 113 poz. 984 i 985 wynikają poniżej określone postanowienia istotne dla funkcjonowania operatora telekomunikacyjnego.

W rozdziale 3 określającym zakres ograniczeń wolności i praw człowieka i obywatela stwierdzono:

w artykule 20, że w czasie stanu wyjątkowego może być wprowadzona:

3) kontrola treści korespondencji telekomunikacyjnej i rozmów telefonicznych lub sygnałów przesyłanych w sieciach telekomunikacyjnych,
4) emisja sygnałów uniemożliwiających nadawanie lub odbiór przekazów radiowych, telewizyjnych lub dokonywanych przez urządzenia i sieci telekomunikacyjne, których treść może zwiększyć zagrożenie konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego.

w artykule 21, że w czasie stanu wyjątkowego mogą być wprowadzone ograniczenia wolności i praw człowieka i obywatela w zakresie:

2) wolności działalności gospodarczej, poprzez nakazanie okresowego zaniechania prowadzenia działalności gospodarczej określonego rodzaju albo ustanowienie obowiązku uzyskania zezwolenia na rozpoczęcie działalności gospodarczej określonego rodzaju,
6) funkcjonowania systemów łączności oraz działalności telekomunikacyjnej i pocztowej, poprzez nakazanie wyłączenia urządzeń łączności lub zawieszenia świadczenia usług na określony czas, a także poprzez nakazanie niezwłocznego złożenia do depozytu właściwego organu administracji rządowej radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych oraz ustalenie innego sposobu ich zabezpieczenia przed wykorzystaniem w sposób zagrażający konstytucyjnemu porządkowi państwa, bezpieczeństwu obywateli albo porządkowi publicznemu.

W rozdziale 4 ustawodawca określił zakres i wysokość sankcji karnych za nie przestrzeganie przez operatorów postanowień zawartych w ustawie.

w artykule 23 stwierdzono: kto w czasie stanu wyjątkowego:

16) wbrew obowiązkowi określonemu w art. 21. pkt 6. nie stosuje się do nakazu wyłączenia na czas określony urządzeń łączności lub zawieszenia świadczenia usług, albo nakazu niezwłocznego złożenia do depozytu radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych lub innego sposobu ich zabezpieczenia - podlega karze aresztu albo grzywny.

Z ustawy „O stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej" z dnia 29 sierpnia 2002 r. (Dz. U. Nr 156, poz. 1301) wynikają poniżej określone postanowienia istotne dla funkcjonowania operatora telekomunikacyjnego.

W rozdziale 2 określającym zasady działania organów władzy publicznej stwierdzono:
w artykule 12, że: Minister Obrony Narodowej w czasie stanu wojennego w szczególności:

3) przedstawia właściwym organom potrzeby w zakresie świadczeń organów państwowych i jednostek samorządu terytorialnego, przedsiębiorców i innych jednostek organizacyjnych oraz osób fizycznych, na rzecz Sił Zbrojnych i obrony państwa;
6) współdziała z ministrem właściwym do spraw wewnętrznych w zakresie świadczeń, o których mowa w pkt 3.

w artykule 13, że: W czasie stanu wojennego wojewoda kieruje realizacją zadań obronnych i obroną cywilną na terenie województwa. Wojewoda w czasie stanu wojennego w szczególności:

2) wprowadza, w zakresie nienależącym do właściwości innych organów, ograniczenia wolności i praw człowieka i obywatela oraz łagodzi i uchyla te ograniczenia;
3) występuje z wnioskami do właściwych organów o wprowadzenie ograniczeń wolności i praw człowieka i obywatela, jak również o ich złagodzenie lub uchylenie;
5) koordynuje i kontroluje działalność organów władzy publicznej, przedsiębiorców oraz innych jednostek organizacyjnych działających na obszarze województwa;

W zakresie działań, o których mowa w ust. 2, wojewodzie są podporządkowane wszystkie jednostki organizacyjne administracji rządowej i samorządowej działające na obszarze województwa oraz inne siły i środki wydzielone do jego dyspozycji i skierowane do wykonywania zadań związanych z obroną państwa i województwa, a także związanych z obroną cywilną.

W rozdziale 4 określającym zakres ograniczeń wolności i praw człowieka i obywatela stwierdzono:
w artykule 18, że:

1. Na obszarze, na którym został wprowadzony stan wojenny, ograniczeniom wolności i praw człowieka i obywatela podlegają wszystkie osoby fizyczne zamieszkałe lub przebywające tam chociażby czasowo, a także ograniczenia te stosuje się odpowiednio wobec osób prawnych i jednostek organizacyjnych

nieposiadających osobowości prawnej mających siedzibę lub prowadzących działalność na obszarze objętym stanem wojennym.

w artykule 20:

2. W czasie stanu wojennego w przypadku osób, których działalność zagraża bezpieczeństwu lub obronności państwa, można dokonać przeszukania tych osób lub przeszukania ich mieszkania, a także zajęcia przedmiotów wykorzystywanych do prowadzenia tej działalności.
3. Przepis ust. 1 stosuje się odpowiednio do przeszukania innych pomieszczeń, pojazdów, statków powietrznych oraz jednostek pływających, należących do osób, o których mowa w ust. 1.
4. Rada Ministrów określi, w drodze rozporządzenia, organy właściwe do stosowania ograniczeń wolności i praw człowieka i obywatela, o których mowa w ust. 1 i 2, a także tryb postępowania w tych sprawach, mając na względzie potrzeby obronne Rzeczypospolitej Polskiej oraz poszanowanie godności osób, o których mowa w ust. 1.

w artykule 21:

1. W czasie stanu wojennego może być wprowadzona:
   3) kontrola treści korespondencji telekomunikacyjnej i rozmów telefonicznych lub sygnałów przesyłanych w sieciach telekomunikacyjnych;
   4) emisja sygnałów uniemożliwiających nadawanie lub odbiór przekazów radiowych, telewizyjnych lub dokonywanych poprzez urządzenia i sieci telekomunikacyjne, których treść może zwiększyć zagrożenie bezpieczeństwa lub obronności państwa.
2. Funkcję organów cenzury i kontroli pełnią właściwi wojewodowie, którzy mogą nakazać organom administracji publicznej działającym na obszarze województwa wykonywanie czynności technicznych niezbędnych do prowadzenia cenzury lub kontroli.
3. Organy cenzury i kontroli są uprawnione do zatrzymywania w całości lub w części publikacji, przesyłek pocztowych i kurierskich oraz korespondencji telekomunikacyjnej, a także do przerywania rozmów telefonicznych i transmisji sygnałów przesyłanych w sieciach telekomunikacyjnych, jeżeli ich zawartość lub treść może zwiększyć zagrożenie bezpieczeństwa lub obronności państwa.
4. Zatrzymane publikacje, przesyłki lub korespondencję telekomunikacyjną doręcza się adresatom po zniesieniu stanu wojennego, z zastrzeżeniem ust. 5.

5. Zatrzymane publikacje, przesyłki pocztowe i kurierskie oraz korespondencję telekomunikacyjną, których treść lub zawartość pochodzi z przestępstwa, była przeznaczona do popełnienia przestępstwa albo została objęta zakazem posiadania, organ cenzury i kontroli przekazuje niezwłocznie, a najpóźniej bezpośrednio po zniesieniu stanu wojennego, organom właściwym do prowadzenia postępowania karnego lub orzeczenia przepadku rzeczy.

w artykule 24:

1. W czasie stanu wojennego mogą być wprowadzone ograniczenia wolności i praw człowieka i obywatela w zakresie:
   5) funkcjonowania systemów łączności oraz działalności telekomunikacyjnej i pocztowej, poprzez nakazanie wyłączenia urządzeń łączności lub zawieszenia świadczenia usług, na czas określony, a także poprzez nakazanie niezwłocznego złożenia do depozytu właściwego organu administracji rządowej radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych lub ustalenie innego sposobu ich zabezpieczenia przed wykorzystaniem w sposób zagrażający bezpieczeństwu lub obronności państwa;
2. Określone w ust. 1 ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniu, o którym mowa w art. 3 ust. 1) wprowadza się i stosuje w drodze rozporządzeń wydawanych przez:
   4) ministra właściwego do spraw łączności, działającego w porozumieniu z ministrem właściwym do spraw wewnętrznych, Ministrem Obrony Narodowej i ministrem właściwym do spraw finansów publicznych oraz po zasięgnięciu opinii Prezesa Narodowego Banku Polskiego w odniesieniu do bankowych systemów telekomunikacyjnych - w przypadku ograniczeń określonych w ust. 1 pkt 5.

w artykule 25:

1. W czasie stanu wojennego można:
   1) nakładać na przedsiębiorców dodatkowe zadania, których realizacja jest niezbędna dla bezpieczeństwa lub obronności państwa oraz zapewnienia zaopatrzenia ludności;
   2) wprowadzić zarząd komisaryczny, o którym mowa w odrębnych przepisach, dla przedsiębiorców, w tym z udziałem kapitału zagranicznego, jeżeli przedmiotem ich działalności jest wytwarzanie wyrobów lub świadczenie usług o szczególnym znaczeniu dla bezpieczeństwa lub obronności państwa;

5) wprowadzić zajęcie nieruchomości niezbędnych dla Sił Zbrojnych lub obrony państwa.

W rozdziale 5 ustawodawca określił zakres i wysokość sankcji karnych za nie przestrzeganie przez operatorów postanowień zawartych w ustawie.
w artykule 33 stwierdzono:

Kto w czasie stanu wojennego:

12) wbrew obowiązkowi określonemu w art. 24 ust. 1 pkt 5 nie stosuje się do nakazu wyłączenia na czas określony urządzeń łączności lub zawieszenia usług albo nakazu niezwłocznego złożenia do depozytu radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych lub innego sposobu ich zabezpieczenia;

- podlega karze aresztu albo grzywny.

Istotnym dla publicznych operatorów telekomunikacyjnych aktem wykonawczym nakładającym szereg obowiązków związanych ze sporządzaniem planu działań w sytuacjach szczególnych zagrożeń oraz jego aktualizacji jest **rozporządzenie Ministra Łączności z dnia 7 czerwca 2001 r. (Dz. U. Nr 66, poz. 667).**

Wynikają z niej poniżej określone postanowienia.

§ 2. **Plan** sporządza się na wypadek wystąpienia szczególnych zagrożeń, w szczególności wprowadzenia stanu wojennego, stanu wyjątkowego lub stanu klęski żywiołowej.

§ 3. 1. **Plan** sporządza się po dokonaniu:

1) identyfikacji i analizy potencjalnych, szczególnych zagrożeń na obszarze prowadzenia działalności telekomunikacyjnej przez operatora,
2) oceny wpływu szczególnych zagrożeń na infrastrukturę telekomunikacyjną, eksploatację sieci telekomunikacyjnej oraz zdolność świadczenia lub udostępniania usług telekomunikacyjnych,
3) analizy potrzeb oraz warunków i sposobów świadczenia lub udostępniania usług telekomunikacyjnych podmiotom, o których mowa w art. 65 ust. 1 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne, zwanym dalej "właściwymi organami i służbami".

2. Identyfikacji danych o szczególnych zagrożeniach dokonuje się w porozumieniu z właściwym terytorialnie, określonym odrębnymi przepisami, organem odpowiedzialnym za obronę cywilną i zarządzanie kryzysowe.

3. Operator jest obowiązany do dokonywania, co najmniej raz w roku, weryfikacji danych o szczególnych zagrożeniach.

4. Określenia potrzeb, warunków i sposobów, o których mowa w ust. 1 pkt 3, dokonuje się w porozumieniu z właściwymi organami i służbami.

§ 4. 1. Operator sporządza plan rejonowy, z zastrzeżeniem ust. 2, odrębnie dla części lub całości każdego województwa, na którego obszarze prowadzi działalność telekomunikacyjną.

2. Operator sieci publicznej przeznaczonej do rozprowadzania lub rozpowszechniania programów radiofonicznych lub telewizyjnych, której infrastruktura oraz wszystkie zakończenia są zlokalizowane w całości na obszarze jednej gminy lub powiatu, sporządza plan lokalny dla całości obszaru, na którym prowadzi działalność telekomunikacyjną.

3. Operator prowadzący działalność telekomunikacyjną na obszarze przekraczającym granice administracyjne jednego województwa oraz świadczący usługi międzystrefowe lub międzynarodowe sporządza również plan ogólny dla całego obszaru tej działalności.

§ 5. 1. **Plan ogólny** sporządza się w uzgodnieniu z:

1) właściwymi organami i służbami, wskazanymi przez Prezesa Urzędu Regulacji Telekomunikacji i Poczty,

2) Prezesem Urzędu Regulacji Telekomunikacji i Poczty w zakresie:

a) struktur organizacyjnych i kompetencji personelu i służb eksploatacyjnych operatora, obowiązujących w sytuacjach szczególnych zagrożeń,

b) procedur działania i środków wdrażanych w sytuacjach szczególnych zagrożeń dla zabezpieczenia funkcjonowania własnych urządzeń i sieci telekomunikacyjnej,

c) wielkości, struktury rozmieszczenia, zasad uruchamiania i użycia technicznych rezerw operatora, przeznaczonych do realizacji planu,

d) procedur współpracy z innymi operatorami,

3) ministrem właściwym do spraw łączności, za pośrednictwem Prezesa Urzędu Regulacji Telekomunikacji i Poczty, w zakresie:

a) sposobów i środków realizacji oraz warunków świadczenia pomocy w zakresie telekomunikacji w ramach wypełniania zobowiązań wynikających z umów międzynarodowych, których Rzeczpospolita Polska jest stroną,

b) sposobów i środków realizacji zadań oraz wypełniania zobowiązań wynikających z członkostwa Rzeczypospolitej Polskiej w strukturach NATO.

2. **Plan rejonowy** sporządza się w uzgodnieniu z:

1) organami administracji rządowej szczebla wojewódzkiego, odpowiednio do obszaru prowadzenia działalności telekomunikacyjnej przez operatora,

2) Prezesem Urzędu Regulacji Telekomunikacji i Poczty w zakresie określonym w ust. 1 pkt 2.

3. **Plan lokalny** sporządza się w uzgodnieniu z właściwym terytorialnie organem administracji publicznej, odpowiednio do obszaru prowadzenia działalności telekomunikacyjnej.

4. Uzgodnienia, o których mowa w ust. 1 pkt 1, ust. 2 pkt 1 oraz ust. 3, dotyczą w szczególności:

1) warunków i sposobów świadczenia lub udostępniania usług telekomunikacyjnych, z uwzględnieniem niezbędnego zakresu i priorytetów ich utrzymania oraz odtwarzania,

2) procedur współpracy, form współdziałania, sposobów wzajemnego przekazywania informacji oraz powiadamiania o konieczności podjęcia lub zaprzestania działań określonych w planie.

§ 6. Po dokonaniu uzgodnień operator przesyła:

1) po jednym egzemplarzu planu, o którym mowa w § 4 ust. 3, do ministra właściwego do spraw łączności, za pośrednictwem Prezesa Urzędu Regulacji Telekomunikacji i Poczty, i Prezesa Urzędu Regulacji Telekomunikacji i Poczty,

2) jeden egzemplarz planu, o którym mowa w § 4 ust. 1 i 2, do Prezesa Urzędu Regulacji Telekomunikacji i Poczty.

§ 7. 1. Plan podlega aktualizacji okresowej - nie rzadziej niż raz na 3 lata, w trybie określonym w § 3-6.

2. Plan podlega aktualizacji w przypadku wystąpienia okoliczności wpływających na jego zawartość, a w szczególności:

1) w przypadku zmian w infrastrukturze telekomunikacyjnej oraz zakresie świadczonych lub udostępnianych przez operatora usług telekomunikacyjnych, wpływających na zmianę sposobu i formę realizacji planu,

2) na wniosek właściwych organów i służb, uzasadniony zmianami warunków, sposobów i procedur określonych w § 5 ust. 4,
3) w przypadku wykonywania obowiązków wynikających z decyzji ministra właściwego do spraw łączności, wydanej w trybie art. 66 ustawy - Prawo telekomunikacyjne.

5.2. Zadania i funkcje podsystemu telekomunikacyjnego dla potrzeb zarządzania kryzysowego

Podsystemem telekomunikacyjnym działającym dla potrzeb reagowania kryzysowego będziemy nazywali zbiór elementów funkcjonalnych wydzielanych z zasobów systemu telekomunikacyjnego państwa, powiązanych ze sobą w sposób umożliwiający świadczenie usług telekomunikacyjnych o wymaganej jakości na rzecz sił i środków reagowania kryzysowego oraz zarządzania nimi. Podsystem ten, w zależności od typu sytuacji kryzysowej i jej lokalizacji, będzie być wydzielany z zasobów publicznych systemów telekomunikacyjnych lub będzie organizowany w oparciu o urządzenia telekomunikacyjne stanowiące wyposażenie ewidencyjne sił i służb reagowania kryzysowego.

Z uwagi na nieokreśloność i brak obiektywnych danych dotyczących organizacji systemów telekomunikacyjnych dla potrzeb zarządzania kryzysowego nie jest możliwe określenie jego docelowej struktury organizacyjno – funkcjonalnej.

W tym celu należałoby dokonać modelowania różnych struktur organizacyjnych systemów telekomunikacyjnych wykorzystywanych w innych państwach dla potrzeb zarządzania reagowaniem kryzysowym i uwzględniając specyfikę systemu reagowania kryzysowego w Polsce, na drodze syntezy, określić rozwiązania najbardziej zbliżone do polskich realiów.

Na obecnym etapie realizowanych prac celowe jest określenie wymagań i zadań stawianych podsystemowi telekomunikacyjnemu wydzielanemu dla potrzeb zarządzania kryzysowego.

Zakres zadań stawianych podsystemowi telekomunikacyjnemu działającemu dla potrzeb zarządzania kryzysowego oraz intensywność ich realizacji zależy od szczebla i obszaru, na jakim elementy podsystemu będą eksploatowane.

Uogólniając można stwierdzić, że obejmują one:

- przyjmowanie i archiwizowanie wszystkich zgłoszeń dotyczących zdarzeń;
- przekazywanie danych do zarządzania zasobami;

- przekazywanie informacji służących do zarządzania dostępnymi służbami dyspozytorskimi;
- powiadamianie osób funkcyjnych z różnych służb i przekazywanie informacji na zasadzie rozsiewczej (relacja jeden do wielu) do ludności o przewidywanych zagrożeniach;
- przekazywanie sygnałów sterujących (telematyka) systemami syren alarmowych;
- przekazywanie informacji i komunikatów alarmowych dla członków obrony cywilnej i innych formacji uczestniczących w zwalczaniu kryzysu;
- przekazywanie informacji koordynujących i kierowania dla różnych rodzajów służb;
- umożliwienie współpracy służbom wykorzystującym różnego rodzaju sprzęt komunikacyjny (różni dostawcy – producenci, różne systemy) – funkcja integratora komunikacyjnego;
- przekazywanie danych związanych ze ściąganiem do miejsca przeznaczenia dodatkowego sprzętu ratunkowego/specjalistycznego, będącego własnością różnych służb i podmiotów prawnych;
- przekazywanie informacji z systemów monitoringu;
- lokalizację położenia obiektów w terenie;
- przekazywanie krótkich, zakodowanych, wiadomości sformalizowanych i sformatowanych (droga: radiowa, przewodowa);
- sterowanie pracą urządzeń peryferyjnych systemu zamontowanych w pojazdach, stanowiących wyposażenie patroli (grup reagowania kryzysowego, oddziałów interwencyjnych);
- sterowanie sygnalizacją świetlną;
- monitorowanie transportu np. toksycznych i niebezpiecznych substancji.

Podsystem telekomunikacyjny działający dla potrzeb zarządzania kryzysowego powinien umożliwiać obsługę następujących funkcji:

- medium transmisyjnego, transportowego i integracyjnego dla informacji pochodzących z różnych (technologicznie, geograficznie - zainstalowanych w innych lokalizacjach) baz danych, przechowujących dane o terenie, infrastrukturze, możliwościach służb ratowniczych, dostępnych zasobach oraz przewidywanych prognozach i scenariuszach rozwoju sytuacji kryzysowej oraz zarządzania nią;

- alarmowego powiadamiania osób funkcyjnych odpowiednich służb (indywidualnego, grupowego, według rekonfigurowanych mechanizmów selektywnego doboru) oraz ludności poprzez techniczne środki alarmowe (automatyczne, półautomatyczne, ręczne), działające w układzie punkt-punkt, punkt – wielopunkt;
- powiadamiania ludności za pośrednictwem wszelkich dostępnych typów środków masowego przekazu (rozgłośnie radiowe, telewizyjne, poczta elektroniczna, komunikaty SMS z systemów łączności komórkowej, komunikaty w systemach przywoławczych, komunikaty wysyłane z serwerów SMS centrum do serwerów SMS operatorów komórkowych, komunikaty w sieciach telewizji kablowej, itp.);
- kierowania i dowodzenia służbami za pomocą usług fonicznych, transmisji danych i usług zintegrowanych w systemie: automatycznym i półautomatycznym, w układzie hierarchicznym, grupowym i w strukturach współdziałania;
- informacyjnego zasilania procesu podejmowania decyzji (np. w zakresie dostarczania danych do: oceny zasięgu zdarzenia, jego powiązania z innymi czynnikami kryzysogennymi oraz jego następstw, oceny sytuacji hydrometeorologicznej, oceny sytuacji radiologicznej, symulacji możliwego przebiegu zdarzenia, chronologicznego prowadzenia dziennika zdarzeń);
- wsparcia szkolenia i ćwiczeń sił i środków reagowania kryzysowego, w tym zasilania informacyjnego komputerowych systemów symulacji działań reagowania kryzysowego.

Podsystem telekomunikacyjny działający dla potrzeb zarządzania kryzysowego powinien udostępniać użytkownikom następujące usługi telekomunikacyjne:

- transmisja mowy (jawna i utajniona) z możliwością przełączania z pracy analogowej na cyfrową i odwrotnie w zależności od konfiguracji konkretnego systemu;
- transmisja danych (jawna i utajniona): krótkie informacje – rozkazy, polecenia, długie informacje- sprawozdania, wymiana informacji geograficznych, obrazów, transfer plików;
- transmisja multimedialna;
- zdalny dostęp do sieci komputerowych;
- zdalny dostęp do baz danych;
- usługi poczty elektronicznej;
- usługi transferu plików;

- usługi WWW;
- usługi telematyczne: telesterowania i teleakcji;
- obsługa telekonferencji i wideokonferencji;
- przekazywanie obrazów nieruchomych i ruchomych;
- usługi dostosowane do profilu użytkownika (z zakresu usług dodanych).

Podsystem telekomunikacyjny działający na rzecz zarządzania kryzysowego powinien charakteryzować się na wieloprofilowe, personalizowane usługi bezpieczeństwa,

5.3. Charakterystyka współczesnych systemów łączności wykorzystawanych przez służby ratownictwa i zarządzania kryzysowego

Konieczność zapewnienia ciągłości działania oraz wykorzystania i integracji w ramach systemów wspomagania zarządzania kryzysowego urządzeń i systemów telekomunikacyjnych różnych generacji nakłada wymóg współpracy systemów projektowanych z istniejącymi, a co za tym idzie – konieczność wykorzystania takich metod wymiany informacji, które zapewnią właściwe zasilanie informacyjne (niezawodne, bezpieczne).

Systemy telekomunikacyjne działające na rzecz systemów wspomagania zarządzania kryzysowego powinny, oprócz wymagań ogólnosystemowych (niezawodność, bezpieczeństwo, żywotność, gotowość, wymagania środowiskowe), spełniać następujące wymagania:

- skalowalność, czyli możliwość rozbudowy o kolejne elementy sprzętowe oraz elementy oprogramowania realizujące nowe funkcje;
- otwartość, rozumianą jako integrację różnych – znanych i nieznanych lub trudnych do przewidzenia w trakcie projektowania – platform sprzętowych i programowych, technik i technologii;
- łatwość konfiguracji;
- łatwość podniesienia systemu po wyłączeniu lub awarii;
- możliwość szybkiej reorganizacji systemu lub odtworzenia systemu w innym miejscu;
- otwartość na udostępnianie i pozyskiwanie danych z innych systemów, pierwotnie nie przewidzianych do współpracy.

Z uwagi na organizację służb ratownictwa i zarządzania kryzysowego, a zwłaszcza na fakt znacznej mobilności użytkowników podstawowymi technologiami telekomunikacyjnymi wykorzystywanymi w tego typu systemach będą technologie radiowe.

Nie oznacza to, że technologie przewodowe nie będą wykorzystywane w ramach centrum wspomagania zarządzania kryzysowego. Mają one zastosowanie do obsługi transmisji informacji pomiędzy stanowiskami poszczególnych użytkowników systemów (stacjonarnych), a bazą danych systemu oraz bramą (ang. gateway) systemu stacjonarnego, a systemem ruchomym.

Zagadnieniem samym w sobie jest organizacja łączności telefonicznej centrum wspomagania zarządzania kryzysowego.

Zaletami systemów łączności radiowej w zabezpieczeniu potrzeb komunikacyjnych organów ratownictwa i zarządzania kryzysowego są:

- szybki czas instalacji;
- łatwość konfiguracji i rekonfiguracji;
- możliwość komunikacji na otwartym terenie.

Zastosowanie systemów łączności radiowej w zarządzaniu kryzysowym jest uzasadnione następującymi czynnikami:

- możliwością wyposażenia użytkownika w terminal umożliwiający kontakt drogą radiową;
- potrzebą radiowego, bezpiecznego dostępu do zasobów;
- potrzebą bezpieczeństwa realizacji połączeń i przesyłania danych;
- lokalizacją obiektów i zarządzaniem zasobami w terenie.

Jako korzystne cechy bezprzewodowych systemów radiowych zalicza się przede wszystkim:

- mobilność dająca możliwość komunikacji w ruchu, zarówno z ruchomym użytkownikiem, jak i elementami systemu;
- krótki czas przygotowania do działania;
- duże możliwości użytkowe, przejawiające się:
    - działaniem w relacjach punkt – punkt, punkt – wielopunkt, wielopunkt – wielopunkt;
    - działaniem w simpleksie, semidupleksie i dupleksie;
    - implementacją szerokiego zestawu usług systemowych i abonenckich;

- możliwość rozszerzenia istniejących sieci telefonicznych, teletransmisyjnych prowadzonych w linii prostej do miejsca przeznaczenia;
- możliwość szybkiego stworzenia nowej kompletnej sieci telekomunikacyjnej niezależnie od sieci już istniejących;
- uniknięcie prac ziemnych;
- mniejsze narażenie na uszkodzenia przypadkowe lub celowe, co za tym idzie niższe koszty eksploatacji;
- możliwość tworzenia sieci prywatnych oraz podsieci dla grup zadaniowych;
- dużą podatność na zmiany konfiguracji sieci telekomunikacyjnej;
- wysoka niezawodność i żywotność;
- duża efektywność wykorzystania przydzielonego pasma częstotliwości;
- wbudowane mechanizmy kontroli bezpieczeństwa (autoryzacja, uwierzytelnianie, szyfrowanie połączeń);

Systemy łączności radiowej organów ratownictwa i zarządzania kryzysowego powinny spełniać następujące wymagania:

- realizować przekaz informacji w postaci cyfrowej;
- posiadać możliwość utajniania sygnałów;
- umożliwiać integrację różnych dziedzin łączności;
- obsługiwać przekaz informacji w czasie rzeczywistym;
- posiadać możliwość współpracy z systemami już istniejącymi;
- posiadać odpowiednio dużą pojemność;
- oferować usługi wysokiej jakości;
- posiadać efektywne algorytmy obsługi ruchu;
- umożliwiać korzystanie z jednego zintegrowanego urządzenia (terminala) osobistego;
- oferować zakres usług dostosowany do potrzeb abonenta;
- uniemożliwiać śledzenie przez osoby niepowołane poruszającego się abonenta;
- stosować rozwiązania umożliwiające staranną ochronę informacji poprzez identyfikowanie, uwierzytelnienie itp.
- posiadać możliwość szybkiej instalacji i rozszerzenia wyposażenia w ramach potrzeb.

5.3.1. Systemy łączności satelitarnej

Systemy satelitarne są cennym uzupełnieniem naziemnych systemów łączności, a czasami jedynym możliwym do wykorzystania. Obecnie spośród 5000 stacji satelitarnych, około 180 to satelity telekomunikacyjne.

Satelity są umieszczone grupami lub pojedynczo na:

- orbitach geostacjonarnych (satelity geostacjonarne) GEO *(np. Geostationary Earth Orbit)* na wysokości 35-38 tys. km nad równikiem. Są one wykorzystywane do realizacji dalekosiężnych usług telekomunikacyjnych, a szczególnie połączeń pomiędzy ruchomymi obiektami na lądzie i morzu.
- orbitach niskich (satelity niskoorbitowe) LEO *(np. Low Earth Orbit)* na wysokości (500 – 1500) km;
- orbitach średnich (satelity średnioorbitowe) MEO *(np.Medium Earth Orbit)* na wysokości (5000 – 12000) km.

Systemy satelitarne można podzielić na:

- globalne, działające na obszarze całej kuli ziemskiej (np. Globstar, ICO, Elipso, Odyssey, INMARSAT :A, B, C, M, P, INTELSAT, VSAT);
- lokalne, działające na wyodrębnionym obszarze (np. EUTELSAT, Euteltracs, OmniTracs, AceS, Thuraya).

Dla potrzeb służb ratownictwa i zarządzania kryzysowego obydwa typy systemów mogą być potencjalnie przydatne, zależy to od rozmiaru systemów oraz zasięgu sytuacji kryzysowej.

Cechy systemów satelitarnych, ważne dla służb ratownictwa i zarządzania kryzysowego to:

- możliwość jednolitego udostępniania zaawansowanych usług telekomunikacyjnych użytkownikom rozlokowanym na obszarach trudnodostępnych oraz pozbawionych infrastruktury telekomunikacyjnej (wskutek katastrofy, działań wojennych, kryzysów polityczno-ekonomicznych);
- możliwość świadczenia różnych usług, w tym cechujących się zmiennym zapotrzebowaniem na przepustowość wykorzystywanych łączy teletransmisyjnych;
- wysoka elastyczność konfiguracyjna oraz umożliwiają dostosowanie usług do aktualnych potrzeb użytkowników;

- duża łatwość realizacji usług w trybach: P-P (ang. Point-Point), P-M-P (ang. Point-Multipoint-Point), M-M (ang. Multipoint-Multipoint), co oznacza wysoce ekonomiczne wykorzystanie zasobów sprzętowych;
- możliwość perspektywicznego wykorzystania sieci satelitarnych do realizacji nowych, niezdefiniowanych jeszcze usług i udogodnień;
- możliwość dołączania nowych użytkowników bez budowy łączy fizycznych.

Systemy satelitarne są szczególnie cenione do obsługi telekomunikacyjnej służb ratownictwa i zarządzania kryzysowego, gdyż:

- łącza satelitarne mogą stanowić gotową do natychmiastowego użycia rezerwę wykorzystywaną w stanach przeciążenia, katastrof lub niespodziewanych uszkodzeń zasobów naziemnych;
- charakteryzuje je elastyczność wykorzystania i małe wymagania na terenową infrastrukturę telekomunikacyjną (elementy systemu są autonomiczne);
- cechuje je wysoka niezawodność, żywotność i gotowość;
- gwarantują wierność i pewność transmisji danych;
- zapewniają duże bezpieczeństwo informacyjne.

Wadą systemów satelitarnych są stosunkowo duże opóźnienia sięgające (200 – 250ms). Nie jest to wada dyskwalifikująca ich zastosowanie dla potrzeb służb ratownictwa i zarządzania kryzysowego, dla których cenne są pewność transmisji, wysoka gotowość, niezawodność i żywotność systemu oraz możliwości jego elastycznego wykorzystania (w zależności od dynamicznie zmiennej sytuacji).

Do potencjalnych zastosowań systemów satelitarnych w obszarze ratownictwa i zarządzania kryzysowego można zaliczyć ich wykorzystanie do następujących działań:

- kierowania, zarządzania i dowodzenia akcjami ratowniczymi obszarze zasięgu lokalnym i globalnym;
- monitorowania i kierowania ruchem pojazdów;
- monitorowania i zarządzania dystrybucją materiałów niebezpiecznych;
- koordynacji i kierowania akcjami bojowymi, wymuszającymi i utrzymującymi pokój;
- zarządzania gospodarką wodną - przewidywanie stanu pogody (opadów);
- zbierania i dystrybucji danych sejsmicznych;
- monitorowania i wczesnego ostrzegania przed klęskami żywiołowymi;
- kontroli i zarządzania ruchem lotniczym;

- ratownictwa morskiego i lotniczego;
- określania położenia obiektów.

Do usług telekomunikacyjnych realizowanych przez systemy satelitarne na rzecz służb ratownictwa i zarządzania kryzysowego należy zaliczyć:

- transmisję danych szeroko i wąskopasmowa;
- transmisję strumieni ruchu telefonicznego;
- obsługę multimediów w czasie rzeczywistym;
- obsługę tele i wideokonferencji o wysokiej jakości przekazu w sieciach zamkniętych.

Z punktu widzenia dostępności, relatywnie niskich kosztów terminali oraz możliwości elastycznego tworzenia infrastruktury naziemnej w zależności od potrzeb, czasu i warunków terenowych szczególne znaczenie dla służb ratownictwa i zarządzania kryzysowego mają systemy **VSAT** *(ang. Very Small Aperture Terminal*). VSAT to sieci satelitarne z terminalami wyposażonymi w anteny o średnicy nie przekraczającej 3 m. Wymiennie z nazwą – sieci VSAT używa się nazwy – sieci z małymi terminalami (microterminal).

Do cech charakterystycznych systemów VSAT, wyróżniających je od innych systemów satelitarnych, a przydatnych dla ratownictwa i zarządzania kryzysowego należy zaliczyć:

- prostotę instalacji, terminal może być umieszczony bezpośrednio u użytkownika;
- łatwość rekonfiguracji, możliwość elastycznego poszerzenia zakresu oferowanych usług;
- niezależność parametrów transmisji od odległości (duży zasięg oddziaływania systemu);
- niski koszt terminali i eksploatacji (niezależność tych kosztów od geograficznej lokalizacji);
- wykorzystanie zaawansowanych technologii (w tym również programowych), co umożliwia stosunkowo prostą integrację z systemami zarządzania kryzysowego (elastyczność definicji i konfiguracji interfejsu sieciowego);
- łatwość rozwoju systemu w sensie ilościowym (liczba stacji i przepustowość), przestrzennym i innowacyjnym;
- łatwość współpracy z innymi sieciami (w tym z sieciami cyfrowymi z integracją usług telekomunikacyjnych) i łatwość zastępowania dotychczasowych systemów telekomunikacyjnych;

- wielousługowość i wieloprotokołowość, możliwość przystosowania cech systemu do specyfiki konkretnej sieci i wymagań różnorodnych terminali;
- szybką wymianę informacji, dużą niezawodność systemową (stopa elementowa błędów poniżej 10^{-7} w 99,5% czasu - wskaźnik ten jest lepszy od analogicznego wskaźnika w sieciach naziemnych w wielu krajach),
- automatyzację kontroli stanu sieci;
- scentralizowane zarządzanie systemem;
- logiczną separację sieci;
- możliwość fizycznej separacji sieci.

5.3.2. Radiowe systemy trankingowe

Radiowe systemy trankingowe *(ang. Trunked Radio Systems)* są rozwiązaniem technicznym zapewniającym nawiązanie połączenia z użytkownikami rozproszonymi w terenie. W systemach tych wykorzystywana jest *technika trankingu*. Polega ona na automatycznym i dynamicznym przydziale wspólnego zbioru kanałów radiowych znacznie większej liczbie użytkowników.

Założono, że ustalona, niewielka liczba kanałów może być użytkowana przez znacznie większą liczbę użytkowników, jeśli tylko ich żądania przydziału kanału napływają przypadkowo w czasie i niezależnie od siebie. Wówczas prawdopodobieństwo przydziału kanału przez większą liczbę użytkowników w tym samym, niedużym przedziale średniego czasu trwania połączenia, jest pomijalnie małe.

Przydział kanału łączności następuje na żądanie użytkownika, z pewnego zbioru wolnych kanałów, będących w dyspozycji systemu trankingowego. Po przekazaniu informacji następuje zwolnienie kanału i może być on wykorzystany przez innego użytkownika.

Systemy trankingowe wykorzystywane są przez różne służby np. policję, pogotowie ratunkowe, służby ochrony, staż pożarną, firmy taksówkowe, służby graniczne, służby celne, służby lotniskowe.

Obok pewnej liczby stacji ruchomych w systemie pracuje kilka terminali stałych, obsługiwanych przez dyspozytorów mających uprawnienia do wydawania poleceń. Większość rozmów odbywa się pomiędzy abonentami i dyspozytorem, abonenci też mogą porozumiewać się ze sobą.

Systemy trankingowe charakteryzują się:

- dużą pojemnością, przy ustalonej liczbie kanałów - w systemach trankingowych uzyskuje się dzięki temu wysoką efektywność wykorzystania kanałów pasma transmisyjnego, co pozwala na obsługę pewnej liczby użytkowników przez znacznie mniejsza liczbę kanałów oraz daje możliwość redukcji kosztów połączeń – wykorzystuje się do tego optymalizację wykorzystania przydzielonego pasma częstotliwości;
- wysoką niezawodnością działania - w systemach trankingowych awaria pojedynczego kanału powoduje najwyżej spadek jakości oferowanych usług, co objawia się min. wydłużonym czasem oczekiwania na przydział kanału;
- możliwością dogodnej realizacji priorytetowania rozmów - w przypadku utworzenia wspólnej kolejki abonentów żądających obsługi, o kolejności może decydować, oprócz kolejności zgłoszeń także priorytet żądania;
- prywatnością prowadzonych rozmów - w trakcie trwania rozmowy żaden inny użytkownik systemu nie może przełączyć się na zajęty przez kogoś kanał i zakłócać bądź podsłuchiwać zestawionego wcześniej połączenia;
- dostępnością usług trankingowych, także dla małych grup użytkowników, generujących mały ruch - użytkownik taki może korzystać z publicznych systemów trankingowych;
- dużą efektywnością systemu;
- prostotą obsługi związaną z brakiem konieczności ręcznego przeszukiwania kanałów częstotliwościowych.

Standard TETRA

Standard TETRA *(ang. TErriestral Trunked Radio, początkowo Trans European Trunked Radio)* jest cyfrowym standardem łączności rankingowej, nad którym pierwotne prace rozpoczął na początku lat 90 ETSI *(ang. European Telecommunications Standard Institute).*

Standard TETRA zaprojektowano tak, aby umożliwiał przesyłanie w kanale radiowym zarówno sygnałów mowy, jak i danych w trybie komutacji łączy, a także w trybie komutacji pakietów.

Oficjalnie dokumenty ETSI dotyczące bezpośrednio systemu TETRA są zawarte w normach serii ETS 300 – 392, 393, 394, 395, 396; 301, serii ETR 086, 120,265, 292, 293, 294,295, 300, 346 i innych.

TETRA jest cyfrowym systemem łączności radiowej przeznaczonym do przesyłania głosu i danych w sieci o strukturze komórkowej. Istotną cechą transmisji radiowej w systemie TETRA jest skojarzenie zasady systemu trankingowego, polegającej na dynamicznym, wg potrzeb abonentów, przydzielaniu i wykorzystywaniu dostępnych radiowych kanałów transmisyjnych. Sposób ten umożliwia wykorzystanie jednego kanału radiowego o szerokości 25 kHz do obsługi w tym samym czasie czterech różnych połączeń głosowych, jednoczesne przesyłanie głosu i danych, i na skutek tego charakteryzuje się dużą efektywnością wykorzystania widma częstotliwości radiowych.

W standardzie TETRA zastosowano mieszany sposób wielodostępu tzn. TDMA/FDMA *(ang. Time Division Multiple Access/Frequency Division Multiple Access)*. Transmisja w kanale radiowym realizowana jest z wykorzystaniem cyfrowej modulacji π/4 DQPSK.

Jakość transmisji mowy jest porównywalna do jakości uzyskiwanej w telefonii publicznej. Sumaryczna przepływność danych w pojedynczym kanale częstotliwościowym wynosi 19,2 kbit/s, a po zastosowaniu kodowania protekcyjnego 36 kbit/s. Dostęp do kanału radiowego realizowany jest przy pomocy algorytmu ALOHA.

Zasięg zakładany przez standard wynosi do 60 km od stacji bazowej. Systemy w standardzie TETRA pracują w paśmie (380-400) MHz za zgodą i porozumieniem z NATO.

Ważniejsze parametry standardu:

- modulacja: π/4 DQPSK;
- odstęp między sąsiednimi nośnymi: 25 kHz;
- liczba kanałów na nośnej: 4;
- zwielokrotnienie dostępu: FDMA/TDMA;
- przepływność danych na nośnej: 19,2 kbit/s;
- przepływność danych po kodowaniu protekcyjnym: 36 kbit/s;
- szybkość modulacji: 18 kbod;
- algorytm dostępu do kanału transmisyjnego: ALOHA;
- czas zestawienia połączenia: 300 ms;
- czas przejścia terminala z obszaru działania jednej stacji bazowej do drugiej: poniżej 1s;
- klasy mocy terminali ruchomych 1, 3 oraz 4 W;
- zasięg stacji bazowej: 60 km;

- maksymalna prędkość przemieszczającego się terminala: 200 km/h.

TETRA oferuje dwa podstawowe tryby pracy systemu:

- TETRA VD (*ang. TETRA Voice + Data)*, służący do transmisji sygnału mowy oraz danych;
- TETRA POD *(ang. TETRA Packet Optimized Data*), przeznaczony wyłącznie do transmisji danych.

TETRA oferuje bardzo szeroki wachlarz usług, począwszy od transmisji sygnałów mowy w różnych wariantach, poprzez transmisję danych, do klasycznych usług dodatkowych np. przekazywanie rozmów, czy blokowanie połączeń. Standard oferuje szereg usług nietypowych np. monitorowanie rozmów, czy rozbudowane możliwości nadawania priorytetów. Poniżej wymieniono ważniejsze usługi zdefiniowane w standardzie TETRA, szczególnie przydatne na potrzeby zarządzania kryzysowego:

- transmisja sygnałów mowy, półdupleksowa lub dupleksowa, z możliwością szyfrowania do abonentów grupowych lub indywidualnych;
- transmisja danych w trybie połączeniowym z możliwością szyfrowania na różnych poziomach zabezpieczeń przed błędami z przepływnością (9,6 - 28,8) kbit/s do abonentów grupowych lub indywidualnych;
- pakietowa transmisja danych z potwierdzeniem;
- przekazywanie rozmów, bezwarunkowe oraz warunkowe w przypadku zajętości wołanego terminala, braku odpowiedzi lub też jego wyjścia poza zasięg działania systemu;
- blokowanie przychodzących lub wychodzących rozmów od i do określonych grup odbiorców, informowanie abonenta o rozmowach przychodzących w trakcie trwania innego połączenia;
- definiowanie numerów skróconych;
- dynamiczne tworzenie grup abonentów, a także zestawianie połączeń konferencyjnych;
- priorytetowanie dostępu do zasobów systemu, w tym do kanałów radiowych, bezwarunkowe lub w zależności od aktualnego natężenia ruchu;
- autoryzacja zestawianych połączeń przez centrum nadzoru;
- dyskretne słuchanie przez operatorów centrum dyspozytorskiego – monitorowanie rozmów prowadzonych przez innych użytkowników;

- możliwość zestawiania warunkowych połączeń np. tylko wtedy gdy abonent wywoływany znajdzie się na wskazanym obszarze;
- oferowanie usługi poczta głosowa.

EDACS

Jest systemem trankingowym umożliwiającym cyfrową transmisję danych oraz cyfrową lub analogową transmisję sygnałów mowy w kanale radiowym. System został zaprojektowany dla specyficznych zastosowań, w których szczególnie ważna jest m.in.:

- niezawodność działania podczas pracy w niesprzyjających warunkach np. w czasie klęsk żywiołowych, w warunkach nie w pełni zdatnej własnej infrastruktury telekomunikacyjnej;
- zapewnienie łączności na rozległym obszarze np. całego kraju;
- hierarchiczna struktura łączności dająca się dopasować do struktury przedsiębiorstwa;
- poufność przekazywanych informacji.

System znajduje zastosowanie jako system łączności radiowej w takich służbach jak:

- policja,
- straż pożarna,
- ochrona portów lotniczych.

System EDACS dostępny jest w wersji szerokopasmowej oraz wąskopasmowej. W wersji szerokopasmowej dostęp pomiędzy sąsiednimi kanałami częstotliwościowymi wynosi 255 kHz lub 30 kHz, a w wersji wąskopasmowej kanały mają szerokość 12,5 kHz. W wersji szerokopasmowej system EDACS pracować może tylko w paśmie (896-941) MHz, a wersji wąskopasmowej na pasmach (136-174) MHz, (403-515) MHz i (806-870) MHz.
System umożliwia trzy rodzaje transmisji:

- transmisję analogowego sygnału mowy – transmitowany zarówno w wersji szeroko- jak i wąskopasmowej;
- transmisję cyfrowego sygnału mowy – w wersji szerokopasmowej odbywa się z przepływnością 9600 bit/s;
- cyfrową transmisję danych - w wersji szerokopasmowej odbywa się z przepływnością 9600 bit/s, w wersji wąskopasmowej z przepływnością 4800 bit/s.

Kodowany sygnał mowy jest dodatkowo szyfrowany przy użyciu jednego z algorytmów kryptograficznych. W zależności od konfiguracji, system umożliwia zestawienie połączeń pomiędzy terminalami oraz połączeń dyspozytorskich pomiędzy terminalem lub terminalami radiowymi i konsolą dyspozytorską.

Możliwe są cztery rodzaje połączeń:

- połączenia grupowe – są usługą typową dla systemów trankingowych. Połączenia grupowe są dostępne we wszystkich trzech rodzajach transmisji przy analogowej i cyfrowej transmisji mowy oraz przy cyfrowej transmisji danych.
- połączenie grupowe alarmowe – dostępne przy naciśnięciu odpowiedniego przycisku w terminalu. W przypadku połączenia alarmowego stosuje się przydział kanału radiowego na cały czas trwania połączenia.
- połączenia indywidualne – pozwala na prowadzenie rozmowy między dwoma abonentami, która nie jest słyszalna przez innych użytkowników systemu. Połączenia takie dostępne są dla analogowej i cyfrowej transmisji mowy oraz dla cyfrowej transmisji danych;
- połączenia systemowe – może być realizowane przez operatora systemu zaopatrzonego w specjalny terminal z odpowiednimi uprawnieniami. Operator może nawiązać natychmiastową łączność ze wszystkimi użytkownikami w systemie. Wygenerowanie takiego połączenia w systemie wywołuje zerwanie wszystkich realizowanych połączeń i zestawienie pojedynczego kanału do wszystkich użytkowników w systemie.

EDACS jest systemem o bardzo prostej architekturze. Z założenia jest on zaprojektowany do pracy w warunkach nietypowych jak np. klęski żywiołowe. Umożliwia pokrycie bardzo dużych obszarów. Architektura systemu zapewnia pracę, w razie awarii np. celowych działań niszczycielskich. System posiada możliwość samokonfiguracji w razie awarii jakiegoś elementu.

Umożliwia pracę w trybie przesyłania sygnałów mowy jak również w trybie transmisji danych. Transmisja w systemie EDACS jest szyfrowana, co uniemożliwia podsłuch wiadomości. EDACS umożliwia tworzenie grup użytkowników, do których wysyłane są wiadomości oraz umożliwia połączenia indywidualne, posiada możliwość połączeń alarmowych w grupach.

5.3.3. Bezprzewodowe sieci LAN

Technologie bezprzewodowych sieci lokalnych WLAN *(ang. Wireless Local Area Network)* umożliwiają tworzenie infrastruktury lokalnej sieci komputerowej bez konieczności wykorzystania okablowania strukturalnego, zainstalowanego w konkretnych pomieszczeniach. Uniezależnia to organizatora i przyszłych użytkowników sieci LAN od danej lokalizacji, co jest szczególnie cenne w przypadku prowadzenia ruchomego i aktywnego trybu działania związanego:

- z częstą zmianą miejsc pracy;
- z dynamicznym doborem użytkowników (zespołów) do realizacji różnych przedsięwzięć;
- z doraźną (zależną od sytuacji, miejsca, czasu i osób) organizacją działań zespołów.

Takie scenariusze pracy są częste w przypadku służb ratownictwa i zarządzania kryzysowego, a zwłaszcza organów sztabowych (decyzyjnych) tych służb, gdyż:

- są to ciała kolegialne, w ich skład wchodzą przedstawiciele różnych służb i branż;
- działają wówczas, gdy zachodzi taka potrzeba (pojawia się sytuacja kryzysowa);
- organizują swoje działania w różnych miejscach:
  - różne pomieszczenia różnych centrów zarządzania kryzysowego (szczeble hierarchii);
  - stanowisk dowodzenia, kierowania, koordynacji (branże);
  - praca w „terenie";
- organizują swoje działania w różnym składzie osobowym.

W trakcie pracy organów kierowniczych ratownictwa i zarządzania kryzysowego zachodzi potrzeba elektronicznej wymiany danych pomiędzy komputerami (laptopami) osób biorących udział w spotkaniach, naradach (itp.). Bardzo użyteczne są w tym przypadku technologie WLAN:

- bazujące na zaleceniach IEEE *(ang. International Electronic and Electric Engineering Institute)*: - 802.11;
- opracowane przez ETSI *(ang. European Telecommunications Standard Institute)* – HiPeRLAN;
- rozwiązania firmowe: Blue Tooth i IrDA.

Z punktu widzenia zastosowania technologii WLAN dla potrzeb ratownictwa i zarządzania kryzysowego istotne jest, aby:

- na podstawie analizy oczekiwań poszczególnych szczebli zarządzania kryzysowego określić kiedy, gdzie i w jakim zakresie będzie można zastosować technologię WLAN;
- na podstawie analizy techniczno-użytkowej poszczególnych rozwiązań WLAN, przy uwzględnieniu kryterium ekonomicznego, dokonać wyboru jednej technologii, która byłaby implementowana w służbach ratownictwa i zarządzania kryzysowego;
- przy wyborze technologii WLAN uwzględnić możliwości integracji z istniejącymi komputerowymi systemami wspomagania zarządzania kryzysowego.

5.3.4. System Mobitex

MOBITEX Jest cyfrowym systemem łączności służącym do dwukierunkowej pakietowej transmisji danych pomiędzy terminalami ruchomymi a terminalami stacjonarnymi (np. komputerami lub urządzeniami pomiarowymi) podłączonymi do sieci stałej systemu Mobitex. Umożliwia on zorganizowanie publicznej lub dedykowanej bezprzewodowej sieci WAN.

W systemie Mobitex mogą pracować abonenci ruchomi i stacjonarni dołączeni do sieci poprzez terminale radiowe oraz abonenci stacjonarni, wykorzystujący połączenia z prędkością do 256 kbit/s. do węzła lokalnego sieci (tzw. *Fixed Terminale*) poprzez łącza dzierżawione, inne sieci np. VSAT, lub sieć pakietową X.25.

Jest to system oparty na architekturze komórkowej. Teren objęty zasięgiem systemu podzielony jest na komórki, a każda z nich obsługiwana jest przez jedną stację bazową. Mobitex umożliwia transmisje danych z przepływnością do 8 kbit/s, w paśmie 80, 160, 450, 900 MHz.

Podstawową cechą sieci Mobitex jest transport pakietów możliwie najkrótszą drogą, zapewnienie krótkiego czasu odpowiedzi i minimalizacja ruchu w sieci szkieletowej. Innymi słowy komunikacja pomiędzy dwoma użytkownikami tej samej komórki zamyka się w obszarze jednej stacji bazowej.

Ważną w omawianych zastosowaniach funkcją systemu Mobitex jest funkcja ***zapamiętaj i przekaż*** *(ang.store-and-forward)*, która pozwala na efektywną optymalizację dostępu do kanału radiowego wielu użytkowników tak, że ilość komutowanych pakietów w jednostce czasu w jednym kanale radiowym w systemie Mobitex wielokrotnie przewyższa

systemy głosowe. Dodatkowo w przypadku, gdy czasowo nie jest możliwe dostarczenie wiadomości do odbiorcy, może ona być przechowywana w pocztowej skrzynce sieciowej do momentu pojawienia się odbiorcy w sieci. Po zalogowaniu się użytkownika w sieci wszystkie oczekujące na niego przesyłki automatycznie są mu udostępniane.

Szerokość kanału radiowego wynosi 12,5 kHz ograniczona jedynie dostępnym pasmem radiowym. Transmisja w kanale radiowym realizowana jest z modulacją GMSK.
W celu zapewnienia wysokiej jakości transmisji stosuje się kodowanie zabezpieczające przed błędami, przeplot oraz retransmisję źle odebranych bloków. Kod zabezpieczający umożliwia korekcję błędów pojedynczych jak i niektórych błędów podwójnych, a także „paczek błędów".

Sposób dostępu do kanału radiowego w systemie Mobitex wykorzystuje protokół ALOHA. Praca terminali odbywa się w trybie półdupleksowym, oznacza to, że w danym momencie terminale albo nadają albo odbierają wiadomość. Wiadomościom wysłanym przez terminal system nadaje priorytety, najwyższy priorytet przydzielany jest wiadomościom alarmowym. W przypadku dużego ruch stacje bazowe pozwalają nadawać tylko tym terminalom, które mają do przesłania wiadomość o najwyższym priorytecie.

Do usług systemu Mobitex przydatnych dla służb ratownictwa i zarządzania kryzysowego należy zaliczyć:

- bezpieczną transmisja danych z wykorzystaniem priorytetów;
- bezpołączeniowy tryb pracy;
- tworzenie i obsługa grup użytkowników i zamkniętych grup użytkowników;
- dwukierunkowy paging;
- obsługę zdalny dostęp do baz danych;
- wysyłanie informacji do tzw. ***skrzynki pocztowej*** – *funkcja store-and-forward*;
- funkcję roamingu;
- możliwość przesyłania wiadomości statusowych;
- możliwość przesyłania wiadomości alarmowych – posiadających najwyższy priorytet;
- możliwość transmisji rozsiewczej od jednego użytkownika do grupy (grup) użytkowników;
- możliwość transmisji sygnałów możliwość czasie rzeczywistym;
- możliwość transmisji sygnałów mowy – jest to nietypowy sposób wykorzystania systemu (system dedykowany do pakietowej transmisji danych), nieefektywnie

zajmuje zasoby systemu (kanał zawłaszczony dla użytkowników prowadzących rozmowę);

System Mobitex jest bardzo użyteczny przy tworzeniu infrastruktury telekomunikacyjnej służb ratownictwa i zarządzania kryzysowego w zakresie jaki jest związany z transmisją **danych pakietowych** pomiędzy centrum zarządzania kryzysowego, a elementami wykonawczymi (patrole, grupy interwencyjne, sensory, itp.).

System ten nie posiada mechanizmów integracji danych (głos, dane, multimedia) w związku, z czym nie jest systemem uniwersalnym (tak jak Tetra czy Edacs), wymaga własnej infrastruktury, co w przypadku tworzenia zintegrowanego systemu łączności dla służb ratownictwa i zarządzania kryzysowego stawia go na gorszej (aspekt ekonomiczny: koszt – efekt) pozycji w porównaniu z systemami trankingowymi, systemami komórkowymi, komunikacji osobistej oraz systemami tworzonymi w oparciu o koncepcję „Mobile IP".

5.3.5. Systemy telefonii komórkowej

Z punktu widzenia zastosowania systemu GSM/DCS dla służb ratownictwa i zarządzania kryzysowego należy uwzględnić następujące jego cechy:

- zapewnienie ciągłości komunikacji w obrębie krajów europejskich,
- zapewnienie łączności dla użytkownika mobilnego wraz z możliwością realizacji połączeń z abonentami publicznej sieci telefonicznej i sieci wydzielonych (prywatnych);
- integrację sygnału mowy i danych w kanale komunikacyjnym;
- pełną identyfikację uprawnień abonenta, łącznie z jego kodem prywatnym PIN (*Personal Identification Number*) oraz za pomocą karty identyfikacyjnej SIM (*Subscriber Identity Module*);
- zarządzanie terminalami, siecią, usługami, co umożliwia tworzenie profili użytkowników;
- ochronę informacji obejmującą:
  - identyfikację tożsamości użytkownika;
  - uwierzytelnienie abonenta w sieci i zapewnienie poufności przesyłanych informacji w sieci (szyfrowanie);
- wysoką wierność transmisji bez możliwości podsłuchu;
- efektywne wykorzystanie pasma częstotliwości;

- konfigurowanie sieci bez ograniczeń w miarę wzrostu gęstości abonentów lub zwiększenia ruchu;
- zapewnienie połączeń i usług z istniejącymi sieciami;
- dość dużą pojemność;
- łatwość rozbudowy;
- szeroką gamę usług:
    - transmisja mowy;
    - przesyłanie SMS;
    - synchroniczny dostęp do sieci pakietowej;
    - pakietowa transmisja danych w kanale radiowym;
    - transmisja danych z wysoką przepustowością
    - wyświetlanie numeru abonenta wywołującego i blokowanie numeru abonenta wywołującego;
    - kolejkowanie rozmów;
    - zawieszanie połączenia;
    - połączenie konferencyjne;
    - zamknięte grupy użytkowników;
- dodatkowe łącze transmisji danych (E-GSM);
- możliwość definiowania zestawów usług dla różnych kategorii użytkowników;
- możliwość współpracy z prywatnymi sieciami telekomunikacyjnymi;
- zaawansowane usługi dla połączeń głosowych, w tym:
    - rozsiewcza transmisja głosu;
    - wywołania grupowe;
    - priorytetowanie połączeń;

Spośród szeregu potencjalnych zastosowań systemów GSM/DCS dla służb ratownictwa i zarządzania kryzysowego w najbliższej perspektywie następujące mogą okazać się najbardziej przydatne i będą w pierwszej kolejności implementowane w systemach łączności wspomagających zarządzanie sytuacjami kryzysowymi:

- obsługa zgłoszeń o zaistniałych sytuacjach (najczęściej połączenia telefoniczne);
- usługi powiadamiania i alarmowania służb ratunkowych i zarządzania kryzysowego za pomocą:
    - indywidualnie i grupowo rozsyłanych SMS;
    - automatycznie realizowane połączenia foniczne indywidualne i grupowe (z wykorzystaniem generatorów zapowiedzi słownych, itp.)

- przesyłanie nieruchomych obrazów, plików ASCII, sformalizowanych dokumentów, itp. za pomocą:
  - transmisji danych z wysoką przepustowością w trybie z komutacją łączy (HSCSD) (ang. Hight Speed Circuit Switched Data);
  - pakietowej transmisja danych w kanale radiowym GPRS (ang. General Packet Radio *Services)*;
- obsługa sieci transportowej transmisji danych w systemach GPS;
- zarządzanie i kierowanie jednostkami ruchomymi (monitorowanie położenia);
- usługi bezprzewodowego dostępu do baz danych;
- tworzenie wydzielonych prywatnych sieci GSM dla służb ratownictwa;
- tworzenie tymczasowych sieci GSM na obszarach dotkniętych katastrofą (klęski żywiołowe);
- lokalizacja położenia poszczególnych członków grup interwencyjnych (strażaków, policjantów, ratowników medycznych. itp.).

Mimo zalet systemów GSM/DCS i dużych możliwości ich zastosowania w obszarze zarządzania kryzysowego należy zwrócić uwagę na ograniczenia, takie jak:

- brak możliwości pracy w trybie bezpośrednim (użytkownik z użytkownikiem bez pośrednictwa infrastruktury sieci komórkowej);
- silne zorientowanie na komercyjne świadczenie usług, co w przypadku braku uregulowań prawnych dotyczących zasad funkcjonowania operatorów telekomunikacyjnych w sytuacjach kryzysowych może niekorzystnie wpływać na świadczenie usług o dużej gotowości dla służb ratowniczych;
- czas zestawiania połączenia (> 0,3 s), w przypadku połączenia do grupy jest odpowiednio dłuższy;
- odrzucenie wywołania w przypadku zajętości sieci;
- brak możliwości ustalenia priorytetów;
- ograniczoną liczbę uczestników grupy (grup).

W wielu przypadkach korzystanie z sieci telefonii komórkowej:

- jest efektywnym sposobem zbierania i rozdziału informacji o zdarzeniach, wypadkach, katastrofach (telefon alarmowy nr 112);
- umożliwia komunikację pomiędzy różnymi służbami (osobami) w ramach systemu ratownictwa i zarządzania kryzysowego;
- pozwala doraźnie zabezpieczyć łączność dla służb ratowniczych w miejscu katastrofy.

W związku z tym, może stanowić cenne uzupełnienie docelowego systemu łączności dla służb ratownictwa i zarządzania kryzysowego.

5.3.6. Systemy telefonii bezprzewodowej

Telefonia bezprzewodowa pozwala na realizację połączeń pomiędzy przenośnym telefonem bezprzewodowym a stacją ruchomą podłączoną do PSTN (lub PBX). Z założenia zasięg telefonów bezprzewodowych jest ograniczony do kilkuset metrów, gdy abonent porusza się z niewielką prędkością.

Do liczących się standardów telefonii bezprzewodowej można zaliczyć:

- CT *(ang. Cordless Telephony);*
- DECT *(ang. Digital Enhanced Cordless Telephony).*

Powszechne zastosowanie w krajach europejskich znalazł DECT. Do głównych cech standardu DECT, które decydują o jego przydatności w systemach dostępu radiowego wykorzystywanych przez służby ratownictwa i zarządzania kryzysowego należy zaliczyć:

- wysoką jakość przesyłanego sygnału mowy;
- dużą pojemność systemu;
- możliwość stosowania procedur identyfikacji i uwierzytelniania użytkownika oraz szyfrowania przekazywanych informacji;
- możliwość tworzenia systemów jedno - i wielokomórkowych;
- łatwość w implementowaniu funkcji przełączania kanałów (handover);
- możliwość przesyłania danych;
- możliwość współpracy z innymi sieciami telekomunikacyjnymi;
- cyfrową kompresję głosu i danych w interfejsie radiowym;
- kodowany interfejs radiowy;
- obsługę faksów grupy III i IV;
- elastyczność w dostosowaniu do zmiennego obciążenia transmisyjnego;
- dynamiczne przypisywanie kanałów DCA (ang. Dynamic Channel Allocation);
- łatwość w tworzeniu rozległych i pojemnych struktur pikokomórkowych;
- oferowane usługi:
- usługi podstawowe:
    - realizacja połączeń telefonicznych;
    - transmisja danych;

- transmisja faksowa;

- usługi dodatkowe:
  - szyfrowanie przesyłanych informacji;
  - przesyłanie wiadomości tekstowych;
  - funkcje przywoławcze;
  - połączenia alarmowe;
  - przenoszenie połączeń;
  - blokowanie połączeń;
  - dostęp do sieci pakietowej;
  - kolejkowanie rozmów;
  - zawieszanie połączenia;
  - wywołanie grupowe;
  - przesyłanie informacji taryfikacyjnej;
  - połączenia konferencyjne;
  - wyświetlanie numeru abonenta wywołującego;
  - dyskretna sygnalizacja wywołania;
  - obsługa DTMF;
  - możliwość wykorzystania terminala przez wielu użytkowników;
  - możliwość zawieszenia pracy terminala przez OMC.

Systemy oparte o DECT znajdują zastosowanie:

- do obsługi telefonów bezprzewodowych (residential) – jako bezprzewodowy interfejs pozwalający na łączność w obrębie komórki;
- do obsługi ruchu pieszego wykorzystując zespół stacji bazowych rozmieszczonych w miejscach publicznych oraz terminala bezprzewodowego;
- w bezprzewodowych, abonenckich centralach telefonicznych (WPBX);
- do obsługi bezprzewodowego dostępu do lokalnych sieci komputerowych (LAN) – z wykorzystaniem usługi typu telepoint. Sieć zorganizowana w oparciu o DECT nie zapewnia dużej szybkości transmisji, ale zapewnia poufność przekazywanych informacji;
- do obsługi dostępu do sieci publicznej PSTN i ISDN poprzez centrale radiowe WPBX wraz z możliwością korzystania ze wszystkich usług jakie oferują sieć publiczna i ISDN;

- jako rozszerzenie systemów komórkowych GSM/DECT (czyli w systemach hierarchicznych) i jako radiowe sieci dostępowe;
- jako sieć transportowa transmisji danych w systemach GPS.

DECT może znaleźć zastosowanie w służbach ratownictwa i zarządzania kryzysowego z uwagi na większość swoich cech, gdyż:

- może być szkieletem telekomunikacyjnym dla wydzielonego ośrodka zarządzania kryzysowego, działającego na ograniczonym obszarze oraz zapewniać współpracę z już istniejącymi systemami telekomunikacyjnymi;
- może stanowić podstawę do sieci telekomunikacyjnej budowanej doraźnie (ad hoc) w miejscu wystąpienia sytuacji kryzysowej (katastrofy) celem zapewnienia obsługi służb ratowniczych;
- charakteryzuje się dużą elastycznością.

5.3.7. Systemy przywoławcze

W zaleceniach CCIR (ang. Centre for Communication Interface Research) zdefiniowano system przywoławczy jako jednokierunkowy, rozsiewczy system radiokomunikacji służący do przesyłania sygnału alarmu i krótkich informacji numerycznych lub alfanumerycznych z wyłączeniem transmisji sygnałów rozmównych.

System przywoławczy zapewnia niezawodny jednokierunkowy przekaz informacji do abonentów sieci wyposażonych w odbiorniki przywoławcze, co w przypadku służb ratownictwa i zarządzania kryzysowego umożliwia przesyłanie do osób funkcyjnych (dowódcy, kierownictwo, koordynatorzy), członków grup interwencyjnych (lekarze, ratownicy, strażacy, policjanci, itp.), osób szczególnie ważnych (eksperci, specjaliści branżowi, itp.) informacji, takich jak:

- wezwania (tekst);
- alarmy i komunikaty o zdarzeniach (tekst);
- krótkie informacje tekstowe;
- powiadomienia o wprowadzeniu stanu gotowości z wykorzystaniem ustalonych sygnałów dźwiękowych;
- automatyczne przekazywaniem sygnałów powiadamiania (dźwięk, tekst sformalizowany) z urządzeń nadzorujących bezpieczeństwo obiektów lub systemów;

Możliwe jest również przekazywanie sygnałów sterujących (telesterowanie) z centrum dyspozytorskiego do sensorów monitorowania (np. poziom wód, wstrząsy sejsmiczne, czujników ruchu, itp.) oraz sygnałów pomiarowych (telemetria) od urządzeń pomiarowych do centrum dyspozytorskiego (centrum zarządzania) lub do poszczególnych użytkowników.
Aktualnie opracowano następujące standardy systemów przywoławczych:

- POCSAG (ang. Post Ofiice Code Standarisation Advisory Group);
- MBS (ang. MoBile Search);
- ERMES (ang. European Radio MEssaging System);
- APOC (ang. Advanced Paging Operators Code) - ulepszony POCSAG;
- FLEX - protokół z potwierdzeniem.

Systemy działające na terenie Polski oparte były o standardy: MBS i POCSAG. Jednakże mając na uwadze fakt powszechnego zastosowania w wielu państwach Europy systemu ERMES, warto rozważyć ewentualne zastosowanie tego standardu dla potrzeb polskich służb ratowniczych i zarządzania kryzysowego.

ERMES oferuje wszystkie podstawowe usługi realizowane przez inne systemy przywoławcze, a ponadto transmisję danych przez kanał przeźroczysty. Umożliwia realizację wywołań użytkowników indywidualnych oraz grupowych. ERMES poza podstawowymi usługami (wywołanie akustyczne, komunikaty numeryczne, alfanumeryczne, przesyłanie danych) oferuje: potwierdzenie, trójpoziomowe priorytety, usługi dla grup abonentów, usługi rozliczeniowe, usługi związane z ograniczeniem wywołań, usługi biurowe.

Kierunek rozwoju systemów przywoławczych to połączenie opcji wywołania z pocztą głosową.
Ze względu na zasięg systemy przywoławcze dzieli się na:

- lokalne;
- systemy dużego zasięgu.

Z uwagi na przeznaczenie i usługi oferowane przez systemy przywoławcze należy uznać, że częściej będą wykorzystywane przez służby ratownictwa i zarządzania kryzysowego na obszarze miasta, gminy, powiatu.

Zastosowanie systemów przywoławczych dla służb ratownictwa i zarządzania kryzysowego będzie malało wraz z upowszechnieniem się systemów trankingowych

(stworzeniem infrastruktury tych systemów dostępnej dla ratownictwa i zarządzania kryzysowego), systemów komórkowych i systemów komunikacji osobistej.

5.3.8. Systemy radioliniowe

Służby ratownictwa i zarządzania kryzysowego z uwagi na specyfikę działania (dynamika zmian w czasie i przestrzeni, dużą zmienność zakresu i wielkości prowadzonych akcji, wysoką gotowość do działania, autonomię w działaniu, itp.) powszechnie wykorzystują radiowe systemy teletransmisyjne, umożliwiające przekaz wielokanałowy w relacji punkt – punkt P-P *(ang. point – point)*. Systemy te noszą nazwę linii radiowych RL *(ang. radio link)* lub radiolinii. Radiolinie umożliwiają szybkie (w ciągu kilku godzin) wybudowanie nowego lub odtworzenie uszkodzonego odcinka stacjonarnego systemu teletransmisyjnego.

Zgodnie z tak rozumianą funkcją, radiolinie dla potrzeb służb ratownictwa i zarządzania kryzysowego powinny być mobilnymi stacjami lub zestawami do szybkiej instalacji w wyznaczonym miejscu (czas rozwinięcia i włączenia do pracy pojedynczego zestawu przez zespół max. 3 osobowy nie powinien przekraczać 120 min).

Powinny je cechować:

- możliwości transportowe (dojazd własny lub dowóz) i możliwość rozwinięcia w wyznaczonym miejscu terenowym, zgodnie z potrzebami i uwarunkowaniami technicznymi;
- ciągła praca w wyznaczonym czasie (intensywność działania 24h/dobę, łączny czas obsługi w cyklu miesięcznym 8 h) i miejscu;
- podatność na zdalne zarządzanie (w oparciu o agenta SNMP lub TMN) i diagnostykę (posiadanie BITE – ang. Built In Test Equipment);
- możliwość obsługi strumieni informacji o różnych przepływnościach: (64, 128, 256, 1024, 2048, 8448, 34368) kbit/s.;
- wielość interfejsów elektrycznych i optycznych;
- możliwość szybkiej zmiany konfiguracji eksploatacyjnej.

Linia radiowa wykorzystywana jako element zastępujący lub awaryjnie odtwarzający stałe linie przewodowe (miedziane lub światłowodowe) lub radiowe powinna zapewniać dwukierunkową łączność pomiędzy stacjami telekomunikacyjnymi. Komplet podstawowy linii radiowej może składać się z kilku zestawów radioliniowych, wykonanych identycznie, różniących się tylko ukompletowaniem. W zależności od potencjalnych zastosowań,

rozważyć należy wyposażenie służb ratowniczych i zarządzania kryzysowego w uniwersalne zestawy zawierające w swoim składzie stacje końcowe (2 szt.) i stacje tranzytowe (ich ilość powinna zostać określona w oparciu od kalkulacje uwzględniające doświadczenia służb ratownictwa i zarządzania kryzysowego).

Stacje końcowe umożliwiają przyjęcie strumieni informacyjnych z urządzeń komutacyjnych (np. centrala telefoniczna centrum zarządzania kryzysowego) lub urządzeń peryferyjnych (serwery wspomagania decyzyjnego centrum zarządzania kryzysowego) i transmisji ich do współpracującej stacji radioliniowej, przy zachowaniu wymaganych wskaźników dotyczących jakości usług QoS *(ang. Quality of Service)*.

Stacje tranzytowe (retransmisyjne) umożliwiają przyjęcie i transmisję strumieni informacji od współpracującej stacji radioliniowej, a także wydzielenie strumieni informacji i przekazania ich do wskazanej (następnej) stacji radioliniowej.

Z uwagi na fakt, że służby ratownictwa i zarządzania kryzysowego działają w bardzo różnych i zmiennych warunkach klimatycznych, systemy radioliniowe działające w warunkach zewnętrznych powinny być odporne na działanie opadów atmosferycznych, podmuchów wiatru o prędkości do 120 km/h i temperatury w przedziale (-30, +45) ^{0}C. Urządzenia radioliniowe zamontowane wewnątrz pomieszczeń powinny pracować poprawnie w zakresie temperatur $5 \div 55^{\circ}$C.

Radiolinie dla służb ratownictwa i zarządzania kryzysowego powinny być radioliniami ze zwielokrotnieniem cyfrowym, z rozdziałem kierunków transmisji FDM i TDM, o konstrukcji nierozdzielnej i rozdzielnej (zależnie od zastosowań i warunków montażu systemu anteny), ze stykiem elektrycznym lub optycznym o przepływnościach od 128 kbit/s do 155 Mbit/s, działającymi w zakresie częstotliwości nośnych od 200MHz do 60 GHz.

Powinny posiadać rezerwę sprzętową ciągłą (1+1), przełączanie na rezerwę powinno odbywać się bez utraty bitu. Ze względu na dużą manewrowość radiolinie powinny być wyposażone w lekkie systemy antenowe o średniej szerokości wiązek promieniowania. Zasięg działania radiolinii – pojedynczego przęsła systemu jest silnie uzależniony od warunków propagacyjnych oraz częstotliwości pracy, można przyjąć, że w paśmie (4,4 – 5) GHz przy przepustowości 8Mbit/s wynosi (35-50) km, natomiast w paśmie (14,52 – 15,229) GHz przy przepustowości 35Mbit/s wynosi do 35 km.

5.3.9. Systemy dynamicznej lokalizacji obiektów

System dynamicznej lokalizacji obiektów stanowi istotny element systemu łączności służb ratownictwa i zarządzania kryzysowego. Jego zadaniem jest przesyłanie informacji o położeniu obiektów w terenie (stałych, dynamicznych), co pozwala na sprawne i efektywne zarządzanie posiadanymi zasobami.

System, aby spełniać swoją rolę musi:

- gwarantować wystarczającą dokładność wskazań w celu umożliwienia jednoznacznej lokalizacji,
- zapewniać efektywne wykorzystanie pasma dla przekazywania informacji o położeniu obiektu.

System dynamicznej lokalizacji obiektów powinien być wyposażony w oprogramowanie zbierające informacje za pomocą interfejsu programowego aplikacji API *(ang. Application Program Interface)* od:

- globalnego systemu określania położenia GPS (ang. Global Positioning System),
- systemu GLONASS (ang. GLObal Navigation Satellite System, ros. Globalnaja Nawigacjonnaja *Satelitarnaja Sistemma)*.

Oba systemy działają na zasadzie biernego pomiaru odległości między odbiornikiem a satelitami. Wyznaczenie położenia odbiornika w przestrzeni wymaga odbioru sygnału z minimum trzech satelitów (zalecane są cztery). Pomiaru odległości dokonuje się poprzez dokładny pomiar czasu, w którym sygnał radiowy dociera z satelity do odbiornika. System GPS przewiduje dwa poziomy dokładności:

- PPS *(ang. Precise Positioning System)* - dokładny system nawigacji;
- SPS *(ang. Standard Positioning System)* - standardowy system nawigacji.

PPS jest wykorzystywany głównie przez armię USA i państw NATO oraz przez niektóre agencje rządowe i autoryzowanych użytkowników cywilnych, w tym również służby ratownictwa i zarządzania kryzysowego. Jego dokładność wynosi:

- przy pomiarach dwuwymiarowych co najmniej 10 m;
- przy pomiarach trójwymiarowych 27.7 m.

SPS jest przeznaczony dla użytkowników na całym świecie bez żadnych ograniczeń i opłat. Dokładność SPS wynosi:

- przy pomiarach dwuwymiarowych co najmniej 100 m (w praktyce osiągalna jest powtarzalna dokładność rzędu 40 m);
- przy pomiarach trójwymiarowych:156 m.

Zastosowanie systemu GPS w akcjach ratowniczych (szczególnie w górach, na morzu, katastrofach urbanistycznych, likwidacji skutków trzęsień ziemi, itp.) i zarządzania kryzysowego (koordynacja działań służb, określanie miejsc katastrof, itp.) wymaga eliminacji zakłóceń i ograniczenia do minimum błędów określania położenia. W związku z tym proponuje się wykorzystanie na potrzeby służb ratowniczych różnicowego zarządzania kryzysowego różnicowego DGPS *(ang. Differential GPS)*. Dla zwiększenia dokładności i pewności działania stosuje się rozszerzenie GPS o różnicowe stacje stałe (referencyjne).

Stacje referencyjne GPS mają precyzyjnie określone koordynaty przestrzenne. Dzięki temu, iż błędy obserwowane przez dwa odbiorniki znajdujące się w tym samym obszarze są skorelowane, stacje te na bieżąco porównując swoje współrzędne z wynikami pomiarów określają dane różnicowe, poprawki dla poszczególnych satelitów. Systemy różnicowe zapewniają dane GPS wolne od błędów i przerw, wywołanych przez niejednorodność warstw atmosfery, opóźnień sygnałów wskutek odbić od obiektów terenowych czy okresowo powstających odchyleń w satelitarnych wzorcach czasu.

W systemie tym uzyskuje się korekcję zakłóceń dzięki przestrzennej metodzie pomiarów, którą realizuje się wprowadzając dodatkową stację nadawczą sygnału odniesienia. Jako odbiornik sygnału GPS, ze względu na dokładność zaleca się zastosowanie urządzenia pracującego w systemie różnicowym, zapewniającym dokładność lokalizacji rzędu 1- 15 m. Dodatkowo dla poprawnej pracy systemu lokalizacji w skrajnie trudnych warunkach wykorzystany może być moduł nawigacji inercyjnej.

Istotne dla służb ratowniczych i zarządzania kryzysowego jest dołączenie się do systemów różnicowych o dużym zasięgu WAAS (ang. Wide Area Augmentation System).

Najbardziej perspektywicznym systemem stacji różnicowych GPS/GLONASS jest europejski program EGNOS *(ang. European Geostationary Navigation Overlay Service*), będący częścią projektu cywilnego systemu nawigacji GNSS -2 *(ang. Global Navigation Satellite System*).

Projekt przewiduje użycie czterech do sześciu satelitów geostacjonarnych w charakterze orbitalnych stacji DGPS. Taki różnicowy segment satelitarny SBAS (ang.

Satellite Based Augmentation System) pozwala uzyskać pokrycie większej części powierzchni Ziemi.

System GLONASS, podobnie jak GPS ma dwa kanały: standardowy (o dokładności poziomej 60 m i pionowej 75 m) i kanał precyzyjny. Sygnały są nadawane metodą FDMA *(ang. Frequency Division Multiple Access*), co oznacza, że każdy satelita ma swoje częstotliwości L1 i L2. Częstotliwości te są uzależnione od miejsca satelity w konstelacji.

W odróżnieniu od GPS kanał dokładnosci standardowej jest dostępny na częstotliwościach L1 i L2, a kanał precyzyjny i depesza nawigacyjna tylko na L2. Użycie kodu precyzyjnego wymaga zezwolenia rosyjskiego Ministerstwa Obrony. Nie stosuje się sztucznego błędu ani dodatkowego kodowania kanału precyzyjnego (anti-spoofing).

Dużą zaletą systemu GLONASS jest jego potencjalnie lepsza dokładność oraz to, że produkcja i umieszczanie na orbitach satelitów dwukrotnie tańsze niż w USA, co przy znacznym zainteresowaniu państw europejskich systemem, może być istotnym czynnikiem jego rozwoju. Należy zatem mieć na uwadze zastosowanie tego systemu jako źródła informacji o położeniu obiektów dla potrzeb służb ratowniczych i zarządzania kryzysowego.

Typowy odbiornik GPS składa się z anteny, podzespołu elektronicznego przetwarzającego sygnał oraz procesora. Główną funkcją odbiornika jest "uchwycenie" sygnału, odtworzenie danych orbitalnych, wyznaczanie zakresów i miar Dopplera oraz bieżące przetwarzanie informacji o pozycji użytkownika, jego prędkości oraz aktualnego czasu.

5.4. Ogólna koncepcja wykorzystania podsystemu łączności i teleinformatycznego w systemie reagowania kryzysowego

5.4.1. Funkcje podsystemu

Organizacja współczesnego Centrum Powiadamiania Ratunkowego (na poziomie powiatu) czy Centrum Zarządzania Kryzysowego (na poziomie województwa), wymaga dostępu do wielu źródeł informacji, zgromadzonych w bazach danych oraz dostarczanych przez liczne systemy teleinformatyczne obsługujące obywateli oraz instytucji i służb powołanych do reagowania kryzysowego.

Dla zapewnienia efektywnej pracy ww. centrów musi być zapewniona skoordynowana praca wielu nowoczesnych podsystemów informacyjnych, a z drugiej strony musi istnieć swobodny przepływ informacji pomiędzy nimi oraz pomiędzy ludźmi zaangażowanymi

w proces zgłaszania zdarzeń, podejmowania decyzji i realizowania zadań. Podstawowym elementem takiego centrum powinien być nowoczesny, niezawodny, żywotny i łatwy w eksploatacji system komutacyjny, umożliwiający organizację efektywnie działającego systemu łączności.

W dalszej części niniejszego opracowania będziemy rozważać podsystem łączności przeznaczony dla potrzeb sił i środków reagowania kryzysowego działających na poziomie powiatu.

Duże znaczenie w ramach systemu łączności działającego na rzecz zapewnienia dowodzenia, kierowania oraz koordynacji sił reagowania kryzysowego mają urządzenia łączności telefonicznej.

Do funkcji, jakie powinien realizować system komutacyjny obsługujący Centrum Zarządzania Kryzysowego, łączący poszczególne Centra Powiadamiania Ratunkowego należy zaliczyć realizację połączeń:

1. Z siecią użytku publicznego:
   - Z wykorzystaniem łączy cyfrowych 30B+D z sygnalizacją DSS1 lub po łączach cyfrowych z sygnalizacją R2 (DLB/DLM).

Powyższe łącza zestawione byłyby do wybranych central tranzytowych dla abonentów, którzy wybierają numery Pogotowia Policji „997", Dyżurnego Jednostki Ratowniczo – Gaśniczej „998" oraz Pogotowia Ratunkowego „999" lub numer „112", bezpośrednio do dyżurnego Centrum Powiadamiania Ratunkowego. Ilość kanałów powinna zostać określona na podstawie analizy generowanego ruchu. Należy zwrócić uwagę, iż ilość kanałów 64 kbit/s niezbędnych dla odbierania ruchu w trakcie 2 Mbit/s może być dowolnie deklarowana,

- Po łączach EURO ISDN, 2B+D.

Przewiduje się zmianę istniejących łączy analogowych przychodzących do służb reagowania kryzysowego na łącza 2B+D z sygnalizacją DSS1. Ilość łączy określona zostanie na podstawie generowanego ruchu. Należy sądzić, że ruch do Centrum Powiadamiania Ratunkowego po wiązce obejściowej będzie niewielki, jeśli uruchomione zostaną wiązki łączy cyfrowych z central tranzytowych. Szacunkowo przyjmuje się ilość 12 łączy pełniących rolę wiązki obejściowej.

- Po łączach analogowych z sygnalizacją stałoprądową.

Obecnie wszystkie służby pracujące z wykorzystaniem łączy analogowych nie mają możliwości identyfikacji numeru abonenta A. Jest to dużym utrudnieniem i niemo-

żliwiłoby uzyskanie pełnej funkcjonalności projektowanych Centrów Powiadamiania Ratunkowego. Łącza analogowe pozostałyby jako ostateczność i pełniłyby rolę kolejnej drogi obejściowej. W przypadku przyjęcia koncepcji pozostawienia tylko tych łączy, konieczne będzie zwiększenie ich ilości.

2. Z siecią MSWiA:

   Współpraca Centrów Powiadamiania Ratunkowego z centralami resortowymi MSWiA będzie się odbywała z wykorzystaniem:

   - łącza o przepustowości 2 Mbit/s z sygnalizacją R2 zmodyfikowaną,
   - łącza o przepustowości 2 Mbit/s, 30 B+D z sygnalizacją Q-SIG.

   Zgodnie z wymaganiami Ministerstwa Infrastruktury instalowane centrale abonenckie specjalne współpracują z centralami publicznymi po łączach cyfrowych za pomocą systemu uproszczonej sygnalizacji R2 lub sygnalizacji DSS1.

   W niektórych sytuacjach do współpracy central abonenckich z centralami publicznymi i centralami branżowymi wykorzystuje się pełną sygnalizację R2 (taką jak pomiędzy centralami sieci publicznej).

3. Z łączami dyspozytorskimi, za pomocą:

   - łączy cyfrowych EURO ISDN - przewiduje się zainstalowanie 60 wyposażeń. Będą to stanowiska abonentów systemu wspomagania dyspozytorów systemu i abonentów specjalnych,
   - łączy analogowych do podległych instytucji i służb uczestniczących w reagowaniu kryzysowym. Przewiduje się wyposażenia dla 100 linii analogowych z sygnalizacją stałoprądową na łączu pracującym w ruchu pełnoautomatycznym przychodzącym i wychodzącym do central PBX podległych instytucji i służb.
   - łączy analogowych dla dołączenia użytkowników systemu: Przewiduje się dołączenie 180 użytkowników systemu po łączach analogowych z sygnalizacją stałoprądową.

Ponadto system komutacyjny winien realizować następujące funkcje:

- przekazywanie wywołania na dowolną linię wewnętrzną lub zewnętrzną,
- kontrolowanie stanu wszystkich linii wewnętrznych i zewnętrznych,
- możliwość kierowania sygnalizacji wywołania na jeden lub kilka pulpitów jednocześnie,
- natychmiastowe dołączenie łącza wybranego przez operatora, bez względu na jego stan.

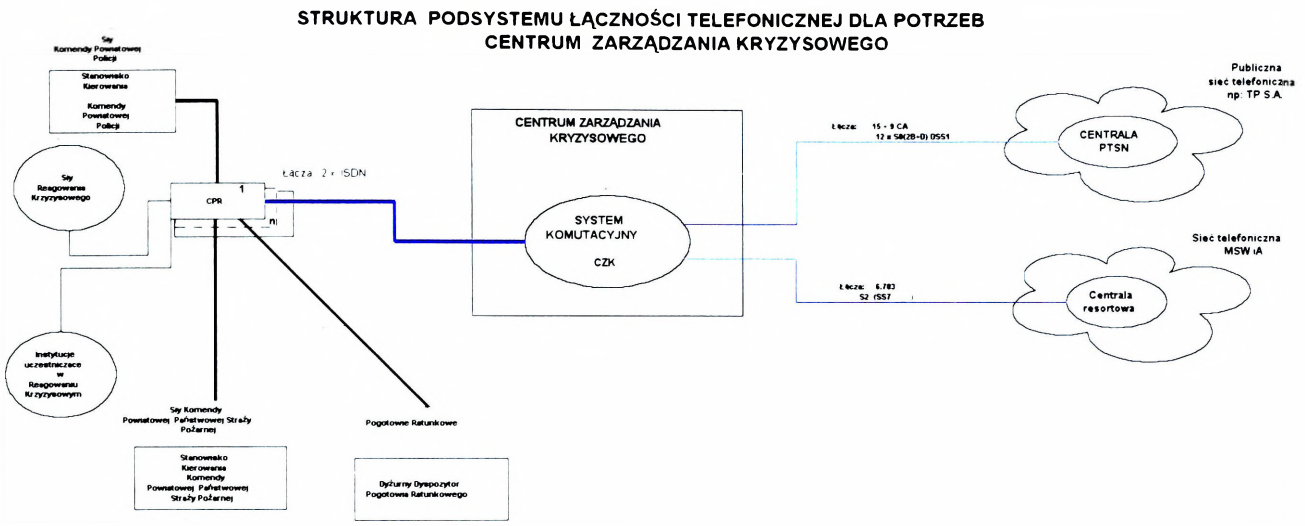
- ustawienie w kolejkę połączeń wychodzących i przychodzących na pulpicie dyspozytorskim,
- możliwość programowej zmiany numeru abonenta,
- możliwość przyznania dowolnych uprawnień dla każdego abonenta wewnętrznego,
- pierwszeństwo dostępu do linii wewnętrznych i zewnętrznych przez abonentów uprzywilejowanych,
- skrócone wybieranie numerów na pulpitach,
- realizacja połączeń telekonferencyjnych,
- praca łącza abonenckiego w trybie "gorącej linii" (w obu kierunkach),
- realizacja funkcji "biura zleceń",
- system głośnomówiący,
- wprowadzenie w stan oczekiwania zestawionych połączeń z abonentami central telefonicznych i powrót do tych połączeń,
- powiadamianie abonentów o nieobecności dyspozytora,
- automatyczne przeniesienie wywołania pod wskazany numer abonenta,
- możliwość wybierania: dekadowe/DTMF,
- możliwość podłączenia cyfrowych abonentów ISDN (2B+D),
- nagrywanie zapowiedzi słownych,
- nagrywanie rozmów przez urządzenia rejestrujące,
- umożliwienie dołączenia punktów alarmowych,
- dźwiękowa i wizualna informacja o stanach alarmowych,
- możliwość dołączenia bezprzewodowego systemu przywoławczego,
- automatyczna diagnostyka łączy,
- zdalny nadzór systemu i pomiar parametrów łączy,
- możliwość zorganizowania systemu rozgłaszania przewodowego,
- transmisja danych komputerowych pomiędzy abonentami z przepływnością do 64 kbit/s.

5.4.2. Struktura podsystemu łączności telefonicznej

Na rysunku 5.4.2.1. przedstawiono strukturę systemu łączności telefonicznej dla potrzeb Centrum Zarządzania Kryzysowego. Niniejsza koncepcja przedstawia dwa warianty opracowania systemu łączności telefonicznej Centrum Zarządzania Kryzysowego:

- Wariant I – rozbudowa na bazie sprzętu i technologii oferowanej przez firmę ERICSSON;

- Wariant II – rozbudowa na bazie sprzętu i technologii oferowanej przez firmę DGT.



Rys. 5.4.2.1. Struktura podsystemu łączności telefonicznej dla potrzeb Centrum Zarządzania Kryzysowego

Wariantowe przedstawienie koncepcji bazuje na założeniu, że obecnie w MSWiA powszechnie wykorzystuje się te dwa typy central telefonicznych, więc założenie racjonalnego wykorzystania posiadanych zasobów oraz minimalizacji nakładów na stworzenie efektywnie funkcjonującego systemu łączności nakazuje ich uwzględnienie dla potrzeb zarządzania kryzysowego tym bardziej, że służby stanowiące „szkielet" sił reagowania kryzysowego na poziomie wojewódzkim i powiatowym (Państwowa Straż Pożarna i Policja), wchodzą w skład MSWiA.

Wariant I – system komutacyjny MD 110 CA firmy ERICSSON

Podsystem dyspozytorskiej łączności przewodowej MD110 CA

Na bazie systemu MD110, jednej z najlepiej znanych central abonenckich na świecie, powstał system dyspozytorski MD110 CA *(ang. Control Application).*

Proponowany system MD110 CA oferuje:

- bezpieczeństwo (system Consono MD110 posiada wszelkie cechy systemu o całkowicie rozproszonej komutacji i sterowaniu),

- łatwą implementację (dostępne są wszystkie funkcje, aplikacje i terminale systemu telekomunikacyjnego MD110),
- filozofię ciągłego rozwoju „ever green".

Dyspozytorzy Centrum Zarządzania Kryzysowego pracują na stanowiskach, gdzie koncentracja i szybkość są ważnymi elementami decydującymi o ciągłości pracy i bezpieczeństwie współpracowników.

W pokoju operacyjnym Dyspozytor musi być przygotowany do odbierania wielu zgłoszeń, jednoczesnego nasłuchiwania wielu rozmów, rozgłaszania wiadomości dla wielu użytkowników równolegle, itp. Wymaga to zastosowania systemu telekomunikacyjnego o znacznie większych możliwościach niż oferuje typowa centrala abonencka.

System MD110 CA jest właśnie takim systemem; szybkim w działaniu, prostym w obsłudze, elastycznym i efektywnym. Zaawansowany technologicznie system telekomunikacyjny opracowany z myślą o zastosowaniach w specjalnych działach gospodarki.

System ma możliwość m.in.:

- nadzoru i wizualnej kontroli wszystkich połączeń,
- oferuje specjalne usługi sieciowe (możliwość integracji różnych systemów telekomunikacyjnych i radiowych),
- ingerencji bez ostrzeżenia ze stanowiska kontrolnego do prowadzonych rozmów,
- programowania rodzaju przychodzącego dzwonienia od abonentów (możliwość wyboru jednego z 7 trybów dzwonienia, włącznie z alarmowym, który umożliwia przełamywanie blokad),
- potwierdzenie wykonania połączenia,
- w sytuacjach alarmowych istnieje możliwość przerwania wszystkich prowadzonych połączeń,
- system pozwala na bardzo prosty nadzór nad częścią radiową z możliwością zestawiania połączeń abonentów radiowych i telefonicznych,
- system telekomunikacyjny MD 110 CA posiada interfejsy dla dołączenia konsoli operatorskich. Zastosowanie ich umożliwia kontrolę w czasie rzeczywistym połączeń telefonicznych.

- funkcjonalność łączności dyspozytorskiej i resortowej osiągana jest nie tylko poprzez wykorzystanie zaawansowanych typów konsoli i terminali dyspozytorskich, wbudowanych, praktyczne nieograniczonych możliwości konferencyjnych, ale także poprzez współpracę jednostki komutacyjnej Consono MD110 CA z siecią publiczną i resortową.

Obsługa Call Center

Po zainstalowaniu nowego Systemu Wspomagania Dowodzenia dla jego prawidłowej pracy niezbędne będzie stworzenie podsystemu przyjmowania zgłoszeń „Call Center". Będzie on zapewniać realizację następujących funkcji:

1. Przyjmowanie wielkiej liczby jednoczesnych wywołań i ich kolejkowanie.
2. Dzięki funkcjonalności Call Center (zrealizowanej jako kolejna aplikacja w systemie komutacyjnym Consono MD110) wzrośnie efektywność działania systemu i jego operatorów, gdyż żadne wywołanie nie będzie utracone.
3. Kontrola i zapewnienie optymalnego obciążenia ruchem poszczególnych operatorów, poprzez równomierny lub liniowy (według określonych wcześniej priorytetów) rozdział wywołań, kontrolę czasu i efektywności pracy operatorów, w tym możliwość programowania przerw po przyjęciu każdego wywołania (kilka sekund), lub dłuższych przerw, w czasie których stanowisko nie otrzymuje nowych wywołań.
4. Informowanie głosowe dzwoniącego o wejściu do systemu (2 kolejne, różne zapowiedzi), ewentualnie o konieczności oczekiwania w kolejce (powtarzana informacja kolejkowa), wykorzystujące wyposażenie systemu komutacyjnego Consono MD110 w 2 karty serwerów głosowych VSU2 o pojemności 7 minut zapowiedzi oraz 24 kanałów niezależnego dostępu.
5. Zapewnienie przyjęcia i wyświetlenia na aparacie w stanowisku operatora numeru łącza aparatu, z którego przychodzi wywołanie („numeru abonenta A"), o ile numer taki będzie w sieci publicznej dostępny.
6. Zapewnienie automatycznego przekazania informacji o „numerze abonenta A" do systemu informatycznego, poprzez specjalizowane, cyfrowe łącze informacyjne „Aplication Link 3.0" pomiędzy systemem komutacyjnym a komputerem Host systemu wspomagania. Numer abonenta A dzięki funkcjonowaniu łącza „Aplication Link 3.0" może być także kryterium dla innego kierowania wywołań, tzn. obsługi wyróżnionych kierunków i abonentów sieci resortowej i publicznej przez dedykowane

grupy lub stanowiska operatorskie systemu.

Wymaganą funkcjonalność podsystemu „Call Center" osiągać się będzie poprzez aplikację CCM („Call Center Manager"), służącą do kontroli „on-line" parametrów ruchowych systemu, a także do kontroli prawidłowości obsługi osobowej stanowisk, długości kolejek, sprawności systemu, a także danych statystycznych dotyczących parametrów pracy całego systemu oraz każdego z operatorów indywidualnie.

Na podstawie informacji z aplikacji CCM możliwe będzie planowanie wymaganej obsady stanowisk operatorskich, a w razie zdarzeń nadzwyczajnych szybkie dołączenie innych abonentów systemu, dla czasowego wzmocnienia obsady tych stanowisk i to zarówno będących abonentami lokalnego systemu Consono MD110, jak i będących abonentami innych systemów Consono MD110.

Wszystkie sygnały akustyczne stanowisk operatorskich (zarówno głos operatora jak i abonenta A) będą wyprowadzone do podsystemu rejestracji, gdzie będą podlegały rejestracji na cyfrowym rejestratorze rozmów.

Wariant II – system komutacyjny 3450 firmy DGT

Cyfrowy System Dyspozytorski DGT

Cyfrowy system dyspozytorski DGT należy do szerokiej rodziny urządzeń telekomunikacyjnych wchodzących w skład Cyfrowego Systemu Telekomunikacyjnego DGT 3450. Ma zastosowanie wszędzie tam, gdzie niezbędnym elementem zarządzania, sprawnego działania i zachowania bezpieczeństwa pracy jest zapewnienie szybkiego i niezawodnego przepływu informacji. Szczególnie przydatny jest do realizacji łączności w systemach reagowania kryzysowego.

W skład cyfrowego systemu dyspozytorskiego DGT wchodzi:

- cyfrowa centrala telefoniczna DGT 3450 zaaranżowana jako dyspozytorska lub dyspozytorsko-abonencka,
- stanowiska dyspozytorskie wyposażone w cyfrowe pulpity dyspozytorskie,
- terminale lokalne operatora systemu,
- system zdalnego nadzoru systemu (opcjonalnie),
- przełącznica,
- buforowany zasilacz

Cyfrowy system dyspozytorski DGT oprócz funkcji określanych jako dyspozytorskie (min. natychmiastowe połączenie dyspozytora z abonentem sieci dyspozytorskiej) realizuje

również funkcje transmisji danych (z możliwością równoczesnego prowadzenia rozmowy) oraz wiele użytecznych funkcji komutacyjnych i usług zamawianych przez abonentów.

Możliwe są dwa warianty aranżacji systemu dyspozytorskiego (w zależności od oprogramowania zaimplementowanego w centrali):

- system dyspozytorski (centrala DGT 3450 zaaranżowana jako dyspozytorska), w którym cały ruch telefoniczny nadzorowany jest przez stanowiska dyspozytorskie,
- zintegrowany system dyspozytorsko-abonencki (centrala zaaranżowana jako dyspozytorsko-abonencka), w którym, poza ruchem do i od stanowisk dyspozytorskich, ma miejsce standardowy ruch telefoniczny.

Podstawowe cechy i struktura systemu dyspozytorskiego DGT

System dyspozytorski DGT umożliwia pełne monitorowanie stanów łączy abonentów sieci dyspozytorskiej, realizację szybkich i niezawodnych połączeń od i do dyspozytora oraz wykonywanie w prosty sposób złożonych funkcji komutacyjnych. Działanie systemu opiera się na wykorzystaniu możliwości cyfrowej centrali telefonicznej DGT 3450 i współpracujących z nią pulpitów dyspozytorskich.

Wielkość sieci dyspozytorskiej (użytkownicy pod kontrolą pulpitów dyspozytorskich) nie powinna przekraczać 1600 NN. Dla tej liczby gwarantowany jest pełny monitoring łączy. Sieć dyspozytorską obsługuje zespół dyspozytorów, którzy wyposażeni są w pulpity dyspozytorskie serii DGT 3490D.

Podstawowe funkcje sytemu dyspozytorskiego DGT:

- **dla ruchu wychodzącego:**
  - łącze sieci dyspozytorskiej jest dostępne z każdego stanowiska dyspozytorskiego,
  - łącze jest dostępne dla innych uprawnionych użytkowników systemu
- **dla ruchu przychodzącego:**
  - łącze po zajęciu skierowane jest bezpośrednio na wybrane stanowisko dyspozytorskie,
  - łącze po zajęciu skierowane jest na wszystkie stanowiska lub zdefiniowaną

grupę stanowisk dyspozytorskich,

- łącze może pracować w trybie „gorącej linii" z opóźnieniem (dzięki temu może osiągać łącza inne niż przypisane mu łącze(a) dyspozytorskie lub osiągać konkretnego dyspozytora po numerze katalogowym)

Pulpit dyspozytorski DGT 3490D współpracuje z jednostką komutacyjną poprzez dwuprzewodowe cyfrowe łącze abonenckie typu 2B+D (styk U_{p0}, U_{k0}). Pulpit może być wyniesiony od centrali na odległość:

- do 3 km (na styku U_{p0}) lub
- do 10 km (na styku U_{k0}).

Pulpit produkowany jest w różnych wersjach różniących się liczbą klawiszy do bezpośredniego osiągania abonentów.
Obecnie wytwarzane są następujące wersje:

- DGT 3490D 40,
- DGT 3490D 60,
- DGT 3490D 120,
- DGT 3490D 180.

Liczba występująca po literce „D" określa maksymalną liczbą łączy monitorowanych (liczbę klawiszy, do których przypisani są konkretni abonenci sieci dyspozytorskiej).

Podstawowe funkcje wykonywane przy użyciu pulpitu DGT 3490D

Pulpit dyspozytorski DGT 3490D zrealizowany jest w nowoczesnej technice i technologii, z elementów elektronicznych o wysokiej niezawodności i małym poborze mocy. Jest urządzeniem uniwersalnym tzn. oprócz funkcji przydatnych do pracy na stanowisku dyspozytorskim umożliwia równoczesną z mową transmisję danych lub spełniania, przy odpowiednim zaprogramowaniu, funkcję awiza cyfrowego lub wielofunkcyjnego cyfrowego aparatu systemowego. Pulpit dyspozytorski posiada klawiaturę wybiorczą, klawisze funkcyjne, klawisze obsługi wyświetlacza oraz pole klawiszy programowalnych.

Łącze monitorowane przez dany pulpit jest skojarzone z klawiszem programowalnym określonym jako klawisz „gorącej linii". Klawiszem takim, poprzez jego naciśnięcie, wywołujemy dane łącze oraz w ten sam sposób odbieramy wywołanie z niego przychodzące. Monitorowanie łącza przypisanego do obsługi przez dany pulpit odbywa się poprzez diody

(dwie lub jedną) umieszczone przy klawiszu do obsługi tego łącza. Stan diody (świeci, nie świeci oraz kolor świecenia) odzwierciedla stan monitorowanego łącza.

Najważniejsze funkcje pulpitu DGT 3490D:

- ❑ sygnalizacja optyczna (monitoring) łączy przypisanych do obsługi dla danego pulpitu; min. sygnalizowanie następujących stanów:
  - łącze wolne,
  - łącze w stanie rozmowy, bez możliwości wejścia na trzeciego,
  - łącze w stanie rozmowy z możliwością wejścia na trzeciego,
  - łącze wywołujące dany pulpit,
  - łącze w stanie rozmowy z pulpitem,
  - wywoływanie łącza z danego pulpitu,
- ❑ sygnalizacja optyczna wywołań od innych łączy,
- ❑ sygnalizacja dźwiękowa wywołań z możliwością:
  - określenia brzmienia dzwonka dla określonych grup lub indywidualnych abonentów,
  - określania priorytetów wywołań,
- ❑ praca z mikrotelefonem lub zestawem głośnomówiącym,
- ❑ przyjmowanie połączeń:
  - z łączy monitorowanych,
  - od innych abonentów,
  - od innych dyspozytorów,
- ❑ inicjowanie połączeń do:
  - abonenta łącza monitorowanego,
  - innego abonenta,
  - innego dyspozytora,
- ❑ zawieszenie połączenia,
- ❑ podjęcie połączenia ze stanu zawieszenia,
- ❑ inicjowanie nowego połączenia w trakcie trwania innego połączenia w celu:
  - konsultacji,
  - przekazania połączenia do innego dyspozytora,
  - przekazania połączenia do innego abonenta,

- przekazania połączenia ze zwrotem ,

❑ połączenia uprzywilejowane:
  - wejście na trzeciego:
    - do abonenta łącza monitorowanego,
    - do innego abonenta,
    - do abonenta innej centrali,
  - wyjście z połączenia na trzeciego,
  - rozbicie połączenia po wejściu na trzeciego,
  - zaoferowanie połączenia zajętemu abonentowi,

❑ powtórzenie ostatnio wybranego numeru,

❑ wyłączenie mikrofonu w zestawie głośnomówiącym/mikrotelefonie,

❑ realizowanie konferencji z maksimum 64-oma uczestnikami:
  - ręcznie,
  - automatycznie z przygotowanej listy uczestników,
  - wyjście z konferencji w celu konsultacji z innym abonentem,
  - dołączenie do konferencji abonenta, z którym prowadzono konsultację,
  - przekazanie konferencji,

❑ historia połączeń,

❑ definiowanie klawiszy programowalnych:
  - klawisz monitorowanego łącza,
  - klawisz wybierania natychmiastowego,
  - klawisz usługi,
  - klawisz konferencji z zaprogramowaną listą uczestników,

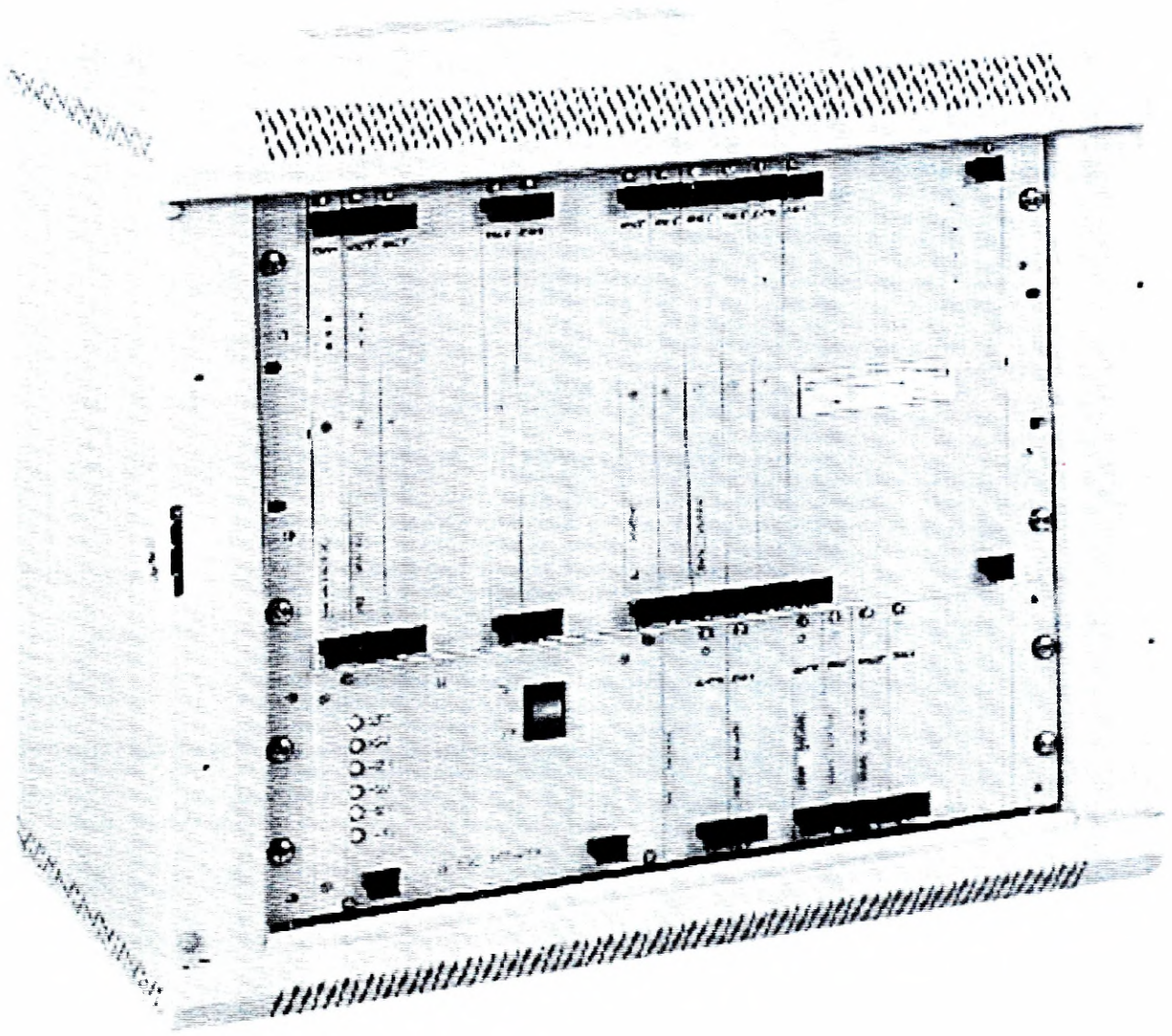
❑ możliwość automatycznej rejestracji rozmów na magnetofonie,

❑ możliwość dołączenia komputera,

❑ funkcje dodatkowe, min.
  - kontrola opłat za połączenia telefoniczne,
  - przegląd dzwonków,
  - wyświetlanie aktualnej daty i czasu itd.

Inne funkcje i możliwości systemu dyspozytorskiego DGT

W wyniku zastosowania jednostki komutacyjnej w postaci cyfrowej centrali DGT 3450 system dyspozytorski DGT realizuje szereg dodatkowych funkcji i możliwości, z których wymienione zostaną najważniejsze.



Rys. 5.4.2.2. Centrala DGT 3450 jako dyspozytorska lub abonencko-dyspozytorską

Dodatkowe funkcje i możliwości systemu dyspozytorskiego DGT:

- praca w sieci ISDN,
- możliwość kierowania wywołania na jeden lub kilka pulpitów dyspozytorskich,
- dyskryminacja połączeń,
- rejestracja połączeń,
- rejestracja połączeń złośliwych,
- zamawianie linii,
- zamawianie połączeń do zajętego abonenta,

- ❑ powiadamianie abonentów o nieobecności dyspozytora,
- ❑ test dzwonka,
- ❑ wyodrębnianie zamkniętych grup użytkowników,
- ❑ usługa nie przeszkadzać,
- ❑ możliwość podstawiania zapowiedzi słownych zamiast sygnału zgłoszenia,
- ❑ bezpośrednie wybieranie numeru abonenta wewnętrznego PABX przy pomocy wybierania tonowego DTMF,
- ❑ kontrola prawidłowości zamawianych usług w postaci zapowiedzi słownych,
- ❑ taryfikacja połączeń:
  - rozliczanie połączeń indywidualnych,
  - rozliczanie grupowe,
- ❑ możliwość dołączenia systemu przywoływania,
- ❑ możliwość dołączenia systemów radiowych.

Użytkownicy sieci dyspozytorskiej

Użytkownikiem sieci dyspozytorskiej nazywamy abonenta systemu, który monitorowany jest przynajmniej na jednym stanowisku dyspozytorskim.

Abonent taki może być wyposażony w aparat:

- ❑ typu MB,
- ❑ typu CB:
  - bez możliwości wybierania,
  - z możliwością wybierania:
    - w kodzie dekadowym,
    - w kodzie DTMF
- ❑ cyfrowe aparaty systemowe typu DGT 3490
- ❑ cyfrowe aparaty ISDN

Szczególnymi użytkownikami systemu mogą być łącza central PABX, central resortowych, central publicznych, a także dyspozytorzy z innych systemów dyspozytorskich. System dyspozytorski DGT umożliwia różne sposoby komunikowania się abonenta z dyspozytorami oraz z innymi abonentami sieci czy też abonentami innych central. Wynika to z odpowiedniego przydzielenia kategorii zakończeniom abonenckim dokonanym w bazie danych centrali DGT 3450.

Generalnie abonent sieci dyspozytorskiej może pracować w jednym z trzech trybów:

- tryb „gorącej linii" (abonent po podniesieniu mikrotelefonu jest bezwarunkowo skierowany do obsługi na stanowisko dyspozytora lub grupy dyspozytorów),
- tryb „gorącej linii" z kalibrowanym opóźnieniem (skierowanie na stanowisko obsługi dyspozytora(ów) jest warunkowe, następuje wtedy gdy abonent nie rozpocznie wybierania w ustalonym okresie czasu; w trybie tym abonent może wybierać innych abonentów systemu i abonentów sieci publicznej),
- tryb swobodnego wyboru numerów katalogowych (stosowany w zintegrowanym systemie dyspozytorsko-abonenckim).

Organizacja stanowisk dyspozytorskich

Stanowiska dyspozytorskie wyposażone są w pulpity typu DGT 3490D. Wykorzystując podstawową właściwość systemu dyspozytorskiego polegającą na tym, że łącze abonenta sieci dyspozytorskiej może być skojarzone z dowolną ilością stanowisk dyspozytorskich, można w sposób dowolny pogrupować abonentów i zorganizować stanowiska dyspozytorskie.

Przy omawianiu organizacji stanowisk dyspozytorskich należy zwrócić szczególną uwagę na różne warianty obsługi wywołań realizowanych na pulpicie.

W wariancie najbardziej typowym wywołania pochodzące od abonentów monitorowanych na danym pulpicie odbierane są spod klawisza przyporządkowanego do obsługi danego łącza. Wszystkie inne wywołania kierowane i odbierane są spod jednego zdefiniowanego klawisza zwanego „Urządzeniem Przyjściowym" (UP).

Możliwe są inne kombinacje. Wywołania z pewnej liczby łączy monitorowanych mogą być obsługiwane spod klawisza UP łącznie z innymi wywołaniami. Jednocześnie stany łączy tych abonentów będą monitorowane.

Wykorzystując te dwie możliwości można dowolnie organizować zarówno podział abonentów na grupy, jak i organizację stanowisk dyspozytorskich oraz określać metody obsługi abonentów sieci dyspozytorskiej.

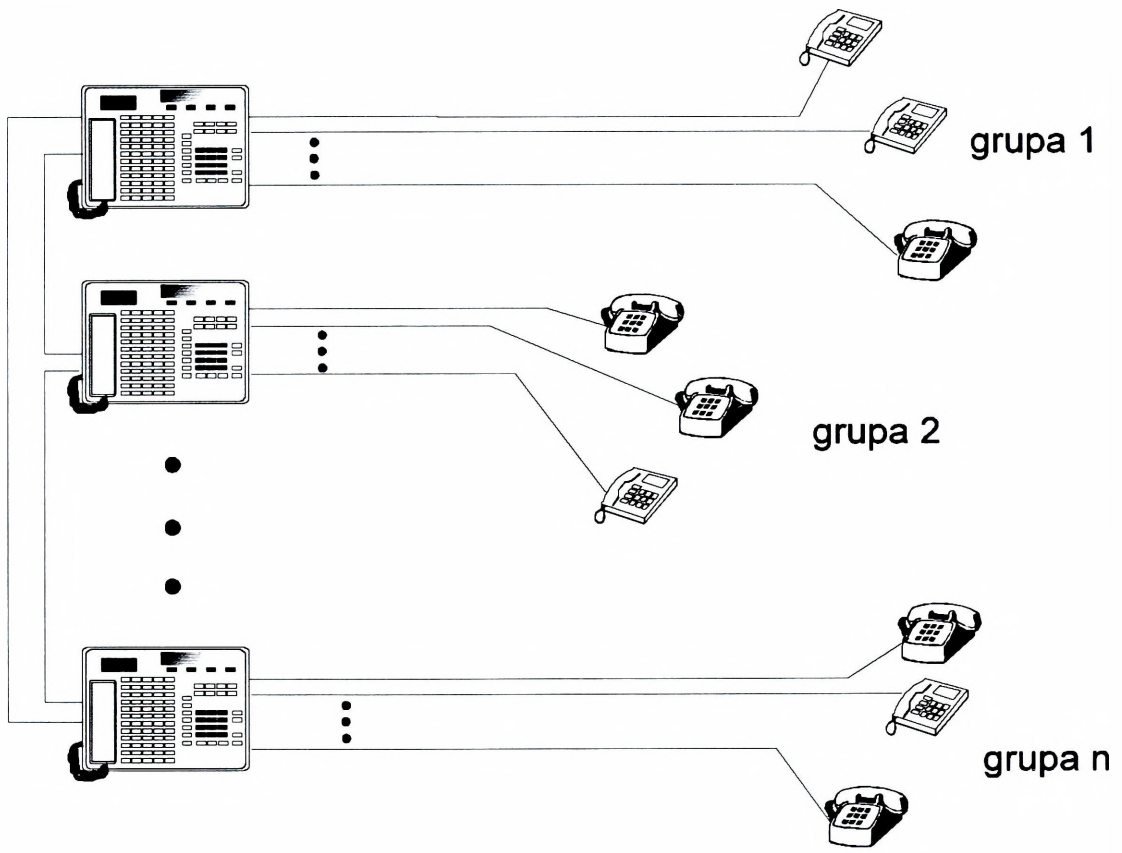
Możliwości systemu dyspozytorskiego DGT

Wykorzystując możliwości funkcjonalne pulpitów dyspozytorskich istnieje wiele sposobów zorganizowania sieci dyspozytorskiej. Wiąże się to ze sposobem pogrupowania abonentów sieci dyspozytorskiej oraz przyporządkowania poszczególnych łączy konkretnym dyspozytorom (pulpitom dyspozytorskim).

Przy omawianiu aranżacji sieci należy wyobrazić sobie, że łącza monitorowane osiągalne bezpośrednio spod klawisza pulpitu są do niego dołączone (w rzeczywistości wszystkie połączenia są komutowane w centrali DGT 3450).

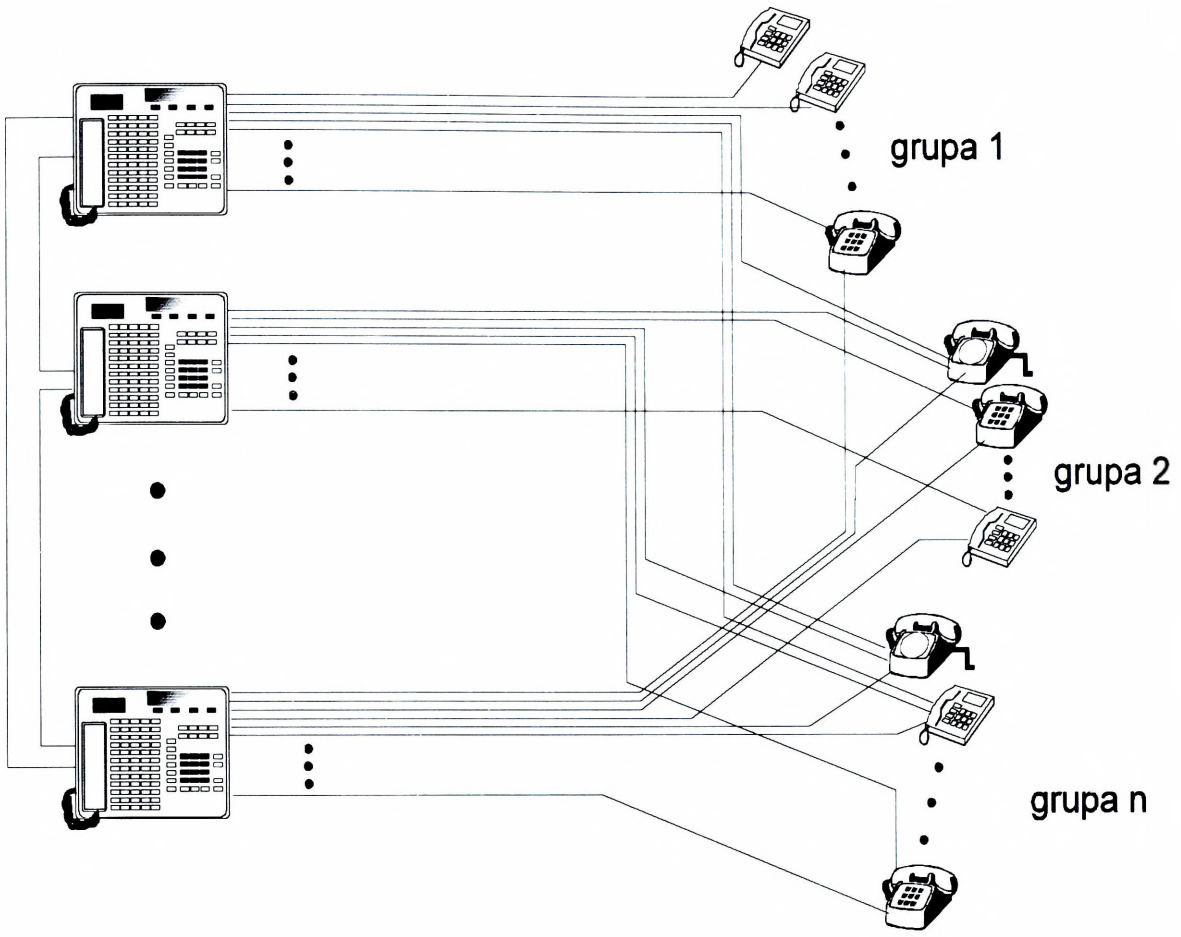
Łącze abonenta sieci dyspozytorskiej może być przypisane do jednego lub wielu pulpitów. Właściwość ta pozwala w sposób dowolny konfigurować taką sieć.

Poniższe przykłady pokazują możliwości konfiguracji takiej sieci.



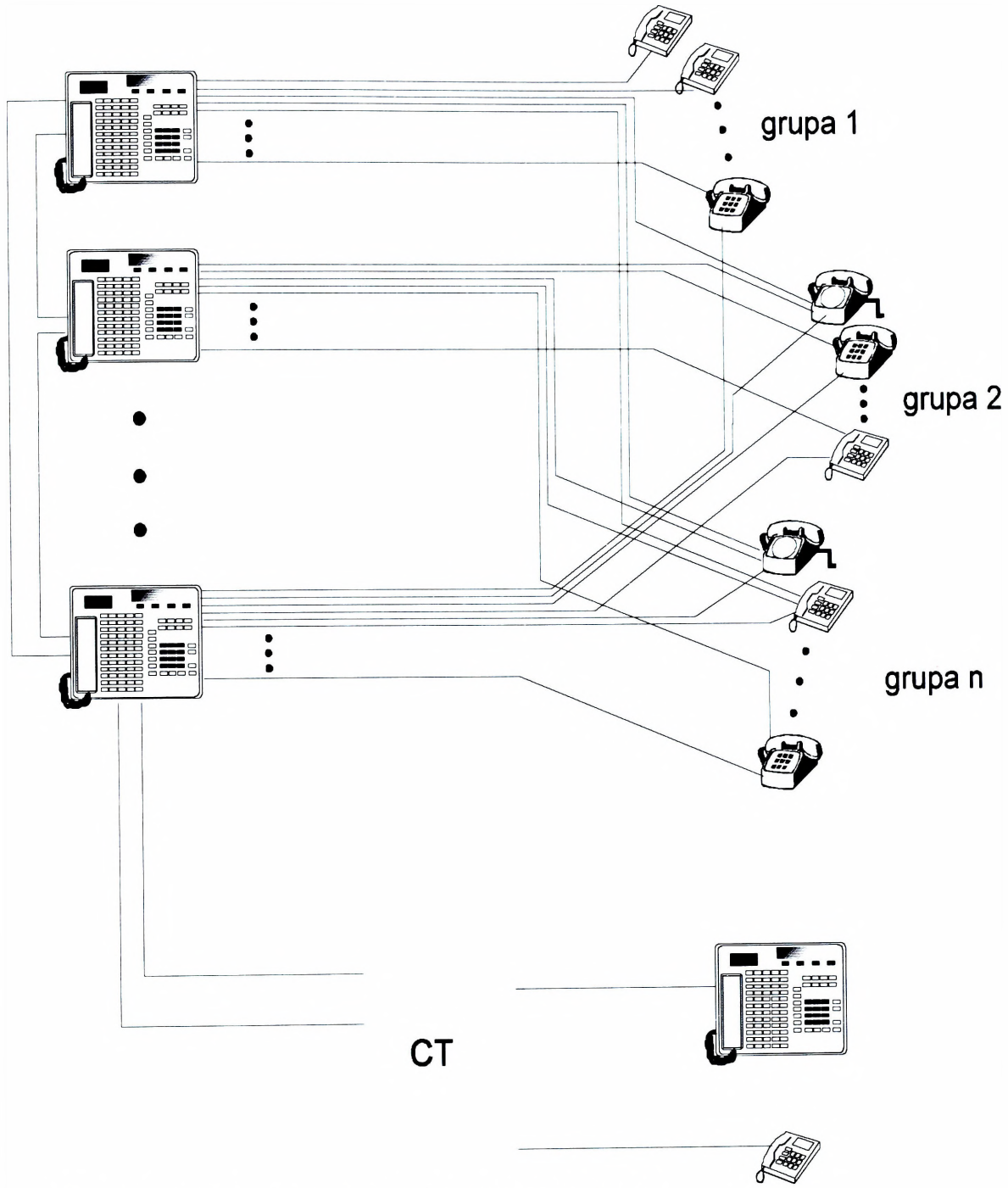
Rys. 5.4.2.3. Przykład 1 konfiguracji sieci dyspozytorskiej

Powyższy przykład jest czysto teoretyczny i nie ma raczej zastosowanie w praktyce. Abonenci sieci dyspozytorskiej zostali podzieleni na grupy i przypisani do pojedynczych dyspozytorów.



Rys. 5.4.2.4. Przykład 2 konfiguracji sieci dyspozytorskiej

Powyżej pokazano inny sposób przyporządkowania łączy poszczególnym dyspozytorom. Jak widać abonenci sieci mogą być monitorowani na kilku stanowiskach jednocześnie. Można powiedzieć, że abonent określonej grupy jest monitorowany na kilku stanowiskach dyspozytorskich jednocześnie, zaś patrząc ze strony dyspozytora istnieje możliwość monitorowania abonentów różnych grup.



CT - centrala telefoniczna innego systemu dyspozytorskiego

Rys. 5.4.2.5. Przykład 3 konfiguracji sieci dyspozytorskiej

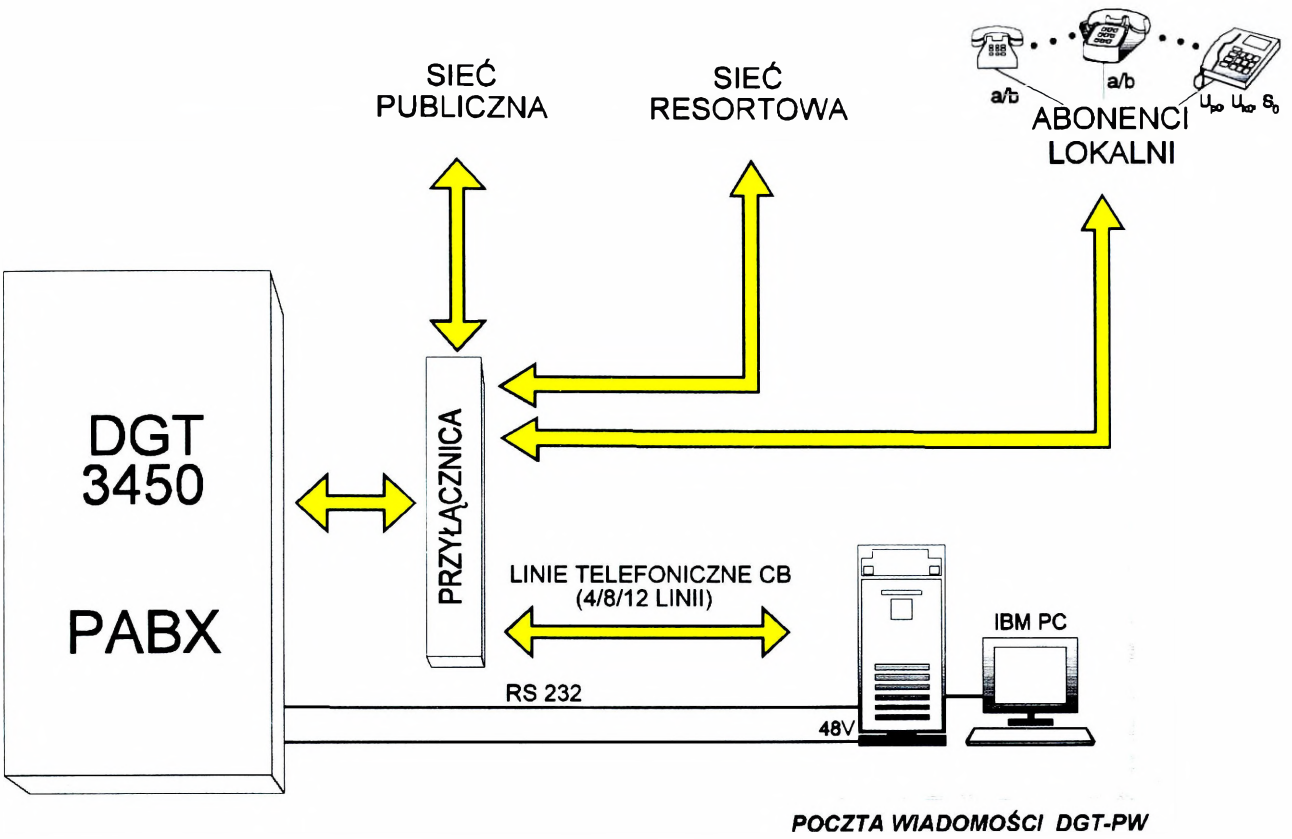
Na przykładzie powyżej zaznaczona jest jeszcze inna właściwość systemu dyspozytorskiego DGT. Otóż w systemie szybkiego osiągania abonenta (po naciśnięciu klawisza) można uzyskać dyspozytora lub użytkownika innego systemu dyspozytorskiego (użytkownicy ci podłączeni są do innej jednostki komutacyjnej).

Poczta Wiadomości

Poczta Wiadomości DGT-PW jest systemem zapamiętywania, przekazywania i odtwarzania informacji w postaci naturalnej mowy i sygnałów faksowych. System przetwarzania głosu Poczty Wiadomości rozszerza możliwości sieci telefonicznych w zakresie:

- poprawy organizacji pracy,
- usprawnienia przepływu informacji,
- DGT-PW eliminuje kolejne próby uzyskania połączenia z abonentem zajętym lub nieobecnym.
- ułatwia rozsyłanie informacji ogólnych dotyczących wybranych grup lub ogółu pracowników,
- eliminacji niedogodności wynikających z różnicy odległości i stref czasowych,
- kontaktu z firmą po godzinach pracy,
- DGT-PW pozwala na pozostawienie i odczytanie wiadomości głosowych oraz faksowych z dowolnego miejsca i aparatu telefonicznego, o dowolnej porze, każdego dnia w roku,
- ograniczenia kosztów połączeń telefonicznych,
- sprawnej obsługi klientów,
- skutecznej informacji o firmie,
- telefonicznego przyjmowania zleceń,
- DGT-PW daje możliwość automatycznego połączenia ze skrzynką Poczty Wiadomości, która wita klienta odpowiednim tekstem, udostępnia określone informacje i pozwala na pozostawienie wiadomości,
- zapewnienia prywatność informacji, DGT-PW udostępnia informacje pozostawione w indywidualnych skrzynkach po podaniu prawidłowego hasła.

Ogólną zasadę współpracy Poczty Wiadomości z centralą DGT pokazano na rys.5.4.2.6.



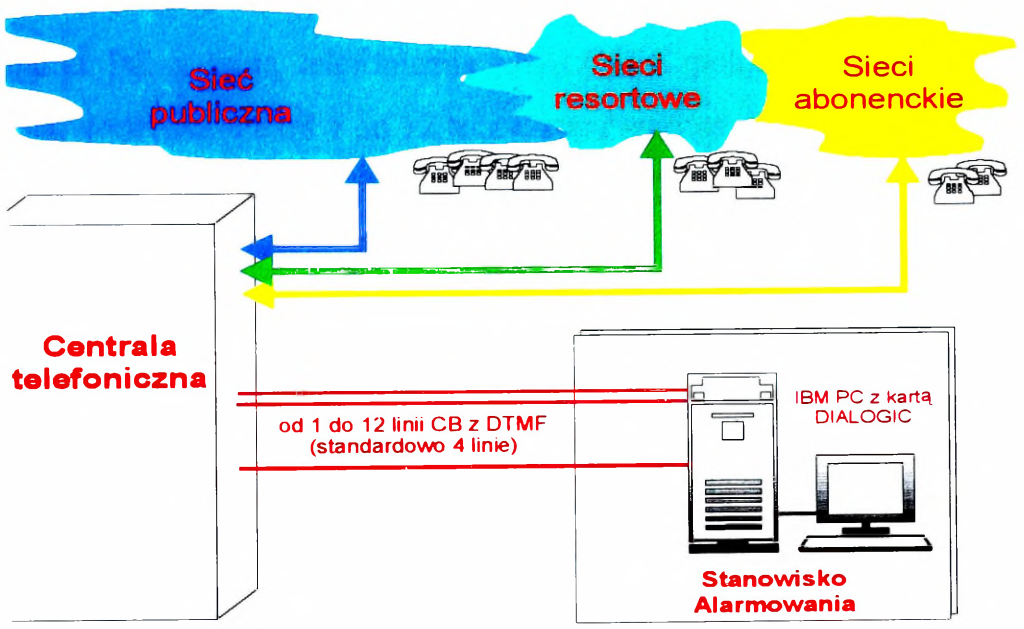
Rys. 5.4.2.6. Schemat blokowy przyłączenia Poczty Wiadomości.

Przekazywanie połączenia przychodzącego na skrzynkę głosową poczty odbywa się z wykorzystaniem standardowych usług centrali, tzn. stosując warunkowe bądź bezwarunkowe przeniesienie numeru na prefiks typu Poczta Głosowa. Wyjątek od tej zasady stanowią pulpity dyspozytorskie, dla których nie przewiduje się korzystania z usług przeadresowania. W tym przypadku skierowanie wywołania przychodzącego na skrzynkę głosową odbywa się poprzez mechanizm dróg obejściowych w prefiksach kierujących ruch do pulpitu. Urządzeniem wyjściowym takiej drogi obejściowej powinien być prefiks poczty głosowej.

W wyniku wykonania przeadresowania, połączenie przychodzące jest kierowane na jedno z łączy poczty głosowej. Po zgłoszeniu poczty, centrala nadaje w kodzie DTMF cyfry, z których pierwsza to informacja dla systemu poczty o przyczynie przeadresowania (tzn.: przeadresowanie bezwarunkowe, warunkowe przy nieobecności abonenta, warunkowe przy zajętości abonenta) a kolejne to numer, jaki został wybrany przez abonenta A. Informacje te mają na celu ustalenie sposobu obsługi połączenia przez system poczty

5.4.3. Telefoniczny system alarmowania DGT-TSA2

Telefoniczny system alarmowania DGT-TSA2 umożliwia autoryzowane powiadamianie określonych grup abonentów za pośrednictwem sieci telefonicznej. Komunikat może być wysłany do dowolnego abonenta dysponującego aparatem z sygnalizacją DTMF. System jest w pełni zautomatyzowany i posiada zabezpieczenia kodowe przed dostępem osób nieupoważnionych. Oprogramowanie do obsługi systemu alarmowania działa w środowisku Windows 95.



Rys. 5.4.3.1. Koncepcja wykorzystania telefonicznego systemu alarmowania DGT - TSA2

Cechy systemu DGT-TSA2

- możliwość powiadamiania abonenta dowolnej centrali telefonicznej
- adresowanie informacją wybierczą z dodatkowymi znakami kodowymi (jak w DTMF lub inne na przykład: „ , ” - pauza itd.)
- pełna rejestracja wszystkich czynności od momentu uruchomienia systemu
- obserwacja wyników alarmowania abonentów w czasie rzeczywistym
- odsłuchanie alarmu tylko po podaniu hasła (kombinacja cyfr w DTMF)
- rozbudowana strategia powiadamiania (czy powtarzać alarm, ile razy?, liczba odtworzeń komunikatu)
- tworzenie grup złożonych (również grupa „Wszyscy”)

- różne tryby zakończenia alarmu (automatyczne, na żądanie operatora, po zaprogramowanym czasie)
- wydruk listy abonentów
- automatyczny start alarmu po uruchomieniu aplikacji z parametrem wywołania
- zdalne inicjowanie alarmu.

Architektura systemu

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

- komputer PC z kartą telefoniczną DIALOGIC połączoną z centralą łączami CB z DTMF (opcjonalnie od 1 do 12 łączy, standardowo 4),
- specjalistyczne oprogramowanie systemu DGT-TSA2 pracujące w środowisku Windows 95.

Baza danych systemu powiadamiania

Baza danych systemu DGT-TSA2 zawiera:

1. **Zestaw danych poszczególnych abonentów:**
   - nazwisko i imię
   - tytuł (stopień, stanowisko)
   - adres
   - strategia powiadamiania (oddzielna dla każdego numeru)
   - hasło (do identyfikacji abonenta)
   - uwagi
2. **Dane dotyczące podziału na grupy**

W grupie powiadamiania może się znaleźć dowolny abonent z bazy danych. W skład grup powiadamiania mogą wchodzić zarówno abonenci indywidualni, jak i grupy zdefiniowane wcześniej. Możliwe jest utworzenie grupy **„Wszyscy”**, do której zostaną automatycznie przepisani wszyscy abonenci ze wszystkich grup.

3. **Zestaw komunikatów słownych**

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

Sesja powiadamiania

Sesję alarmową uruchamia upoważniona osoba po wybraniu właściwej grupy i komunikatu, który ma zostać nadany. Procedura powiadamiania abonenta jest następująca:

- Po uzyskaniu połączenia z powiadamianym abonentem otrzymuje on standardową zapowiedź informującą o tym, że jest dla niego wiadomość, którą usłyszy po podaniu swojego osobistego hasła (cyfry wybrane z klawiatury jego aparatu w kodzie DTMF). Po sprawdzeniu zgodności hasła rozpoczyna się odtwarzanie komunikatu (przynajmniej jeden cykl). Zakończenie nastąpi, gdy abonent się rozłączy lub kiedy wiadomość zostanie powtórzona określoną przez operatora liczbę razy (wynik: „przyjęto").
- Realizacja zlecenia zostanie przerwana (z przekazaniem wyniku: „nie przyjęto" i podaniem przyczyny), gdy przesłanie komunikatu nie będzie możliwe (np. abonent nie zgłasza się dłużej niż 1 minutę od momentu uzyskania zgody na połączenie, linia jest zajęta lub uszkodzona, abonent nie podał hasła lub zrobił to niepoprawnie, zgłosił się faks itd.).

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

Zakończenie sesji alarmowej następuje:

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

Historia każdej sesji jest zapamiętywana w zbiorze dyskowym. W dowolnym momencie możliwe jest przeanalizowanie wybranej sesji, a także filtrowanie danych (abonenci niepowiadomieni, łącza uszkodzone itd.), tworzenie i drukowanie zestawień (liczebność grupy, liczba wywołań przyjętych, łączy uszkodzonych, średni i maksymalny czas zgłoszenia itd.).

Parametry

1. **Czas powiadamiania**
   - Jeśli liczba abonentów w grupie nie jest większa od liczby linii w karcie telefonicznej, powiadomienie wszystkich trwa ok. 1 min. (czas ten obejmuje cały

cykl, czyli: dzwonienie - np. 3 dzwonki, zgłoszenie, zapowiedź komunikatu, podanie prawidłowego hasła, odtworzenie komunikatu, rozłączenie).

- Jeśli liczba abonentów w grupie jest większa od liczby linii, czas powiadamiania stanowi wielokrotność pojedynczego cyklu, uzależnioną od liczby linii w karcie telefonicznej (np.: karta z 4 liniami, grupa 20 abonentów, czas 5 x 1 min. = 5 min., o ile każdy abonent zgłosi się za pierwszym razem).

2. Liczba abonentów

Jedynym czynnikiem determinującym liczebność grupy abonentów jest czas, w jakim operator chce ich powiadomić. Powiadamianie odbywa się sekwencyjnie (liczba abonentów powiadamianych jednocześnie jest równa liczbie linii dołączonych do karty telefonicznej komputera).

Zastosowanie

System DGT-TSA2 można zastosować w następujących wariantach:

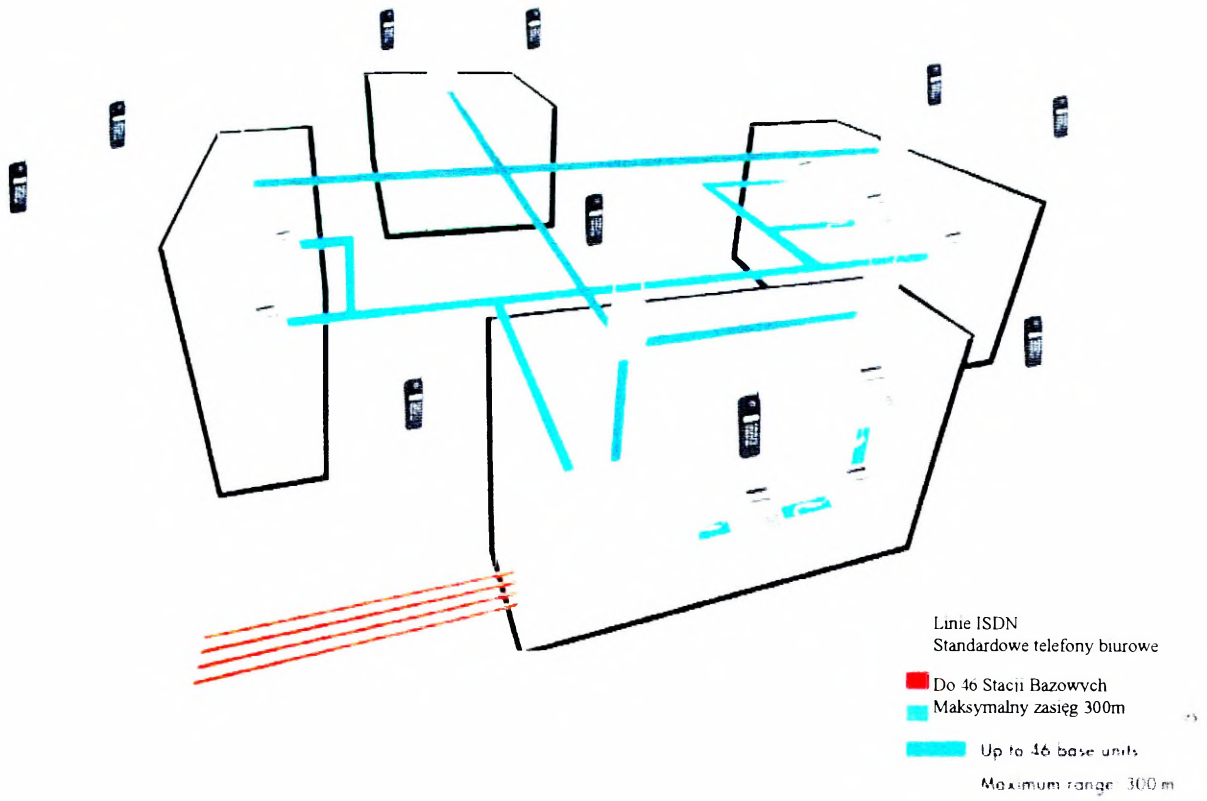
1. Telefoniczny system alarmowania dowolnych abonentów - adresowanie informacją wybierczą; lista abonentów w grupie powiadamiania realizowana sekwencyjnie, porcjami zależnymi od liczby linii w karcie telefonicznej; dołączany do dowolnej centrali,
2. Telefoniczny system alarmowania z opcjonalnym adresowaniem informacją wybierczą (dowolni abonenci) oraz numerami fizycznymi (abonenci centrali DGT 3450) - dołączany tylko do centrali DGT 3450 (konfiguracja: zintegrowany system DGT-TSA i DGT-TSA2, czyli doposażenie DGT-TSA2 w kartę dźwiękową z mikrofonem oraz aparat DGT 3490C z modułem transmisji danych),

Telefoniczny system alarmowania w dowolnym wariancie jako element systemu dyspozytorskiego DGT; dołączany do dowolnej centrali przez analogowe linie CB (4, 8 lub 12)

5.4.4. System łączności bezprzewodowej DECT

Centrala DGT 3450 może współpracować z różnymi systemami lokalnej telefonii komórkowej. System Varix łączony jest z centralą za pomocą traktu PCM z sygnalizacją QSIG i może być rozbudowany do 46 stacji bazowych i 128 handsetów.

Zasięg stacji bazowej zależnie od rodzaju otoczenia, typu zastosowanej anteny może wynosić od 20 - 50 m w budynkach, do 500 - 700 m w otwartej przestrzeni przy zastosowaniu anten sektorowych.



Rys. 5.4.4.1. System Varix (przykład topologii)

System jest bardzo wygodnym rozwiązaniem, szczególnie na terenie Centrum Zarządzania Kryzysowego, gdzie osoby funkcyjne powinny być w ciągłym kontakcie. Mimo że zasięg aparatów bezprzewodowych nie jest duży, (przy użyciu odpowiedniej ilości baz można go powiększyć) można łączyć się pomiędzy handsetami, jak również z abonentami wewnętrznej centrali abonenckiej i abonentami centrali publicznej.

System w wersji podstawowej składa się z:

1. Sterownik VARIX 14 - 1 szt.
2. Karta UPDTS dla podłączenia do 4 baz (jako wyposażenie radiocentrali) - 1 szt.
3. FP outdoor (Stacja Bazowa zewnętrzna) - 4 szt.
4. PP (bezprzewodowe aparaty DECT) - 12 szt.

Sterownik można podłączyć do centrali abonenckiej za pomocą traktu PCM - QSIG, łączy cyfrowych na styku S0, lub nawet zwykłych linii analogowych CB. Oczywiście najbardziej wskazane jest łącze cyfrowe, ponieważ mamy wtedy najwięcej możliwości. Nowa wersja oprogramowania umożliwia połączenia przez sieć korporacyjną z protokołem QSIG i realizację połączeń przez wirtualną sieć połączeniową EURO - ISDN. System posiada funkcję „hand-over", t.j.: automatyczne przełączanie między Stacjami Bazowymi bez przerw w łączności, a także roaming - możliwość przechodzenie z jednej sieci do drugiej. Możliwy jest również automatyczny wybór bazy o najsilniejszym sygnale. System oparty na sterowniku VARIX 14 jest systemem małym.

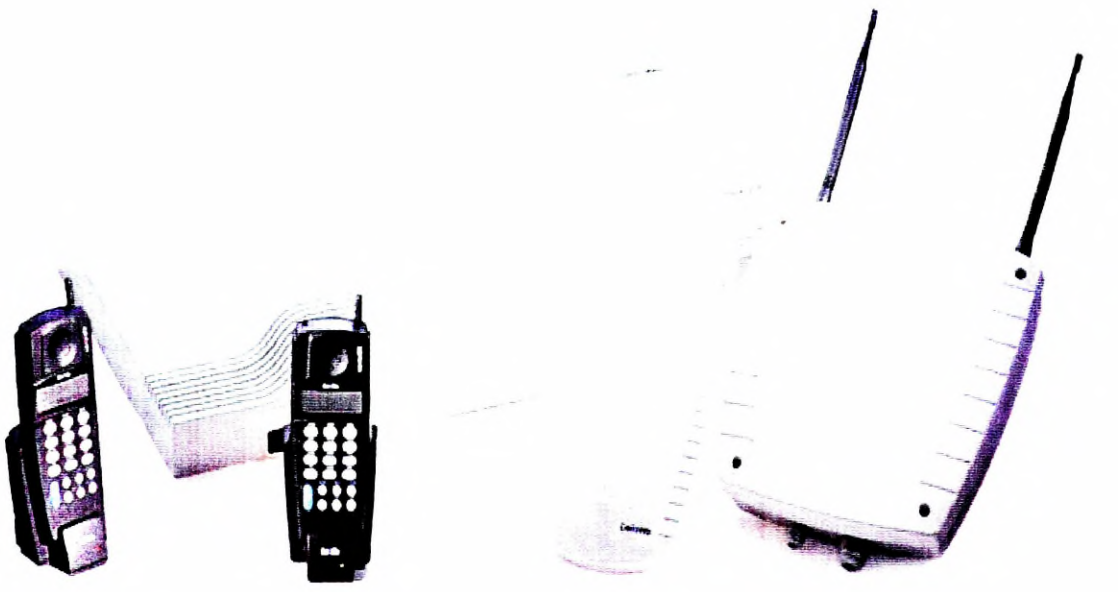
Rys. 5.4.4.2. System wykorzystujący sterownik VARIX 200

Chcąc uzyskać system o większych możliwościach i większej liczbie abonentów, należy zastosować sterownik VARIX 200, która umożliwia podłączenie maksymalnie 46 Stacji Bazowych. Ponieważ np.: w Centrum Zarządzania Kryzysowego zasięg pojedynczej bazy jest niewielki, przed instalacją systemu należy dokonać pomiarów propagacji, aby określić ile baz należy zastosować. Należy przy tym pamiętać, że obszary pokrywane przez poszczególne Bazy powinny nieco zachodzić na siebie na brzegach.

FP - jest to Stacja Bazowa z czterema kanałami do przesyłania rozmów lub danych, może obsługiwać 8 abonentów (w tym czterech jednocześnie). Można je umieszczać wewnątrz budynków (wersja indoor) lub na zewnątrz (wersja outdoor). Dodatkowe wyposażenie to antena kierunkowa, lokalne zasilanie, itp.

PP - bezprzewodowy aparat DECT w wersji M1 i M2, podstawa z możliwością przymocowania do ściany, uchwyt umożliwiający przyczepienie do paska, opcjonalnie - możliwość zakłócenia podsłuchu.

Możliwe jest wykorzystanie dla potrzeb Centrum Zarządzania Kryzysowego wersji dualnej, łączącej w sobie cechy telefonu GSM i DECT (po wyjściu poza zasięg działania stacji bazowych systemu DECT, aparat bezprzewodowy automatycznie przestawia się w tryb pracy jako GSM).



Rys. 5.4.4.3. Urządzenie dualne GSM/DECT (przykład)

Zasięgi działania:

- pomiędzy PABX i FP (Sterownik - Baza) kabel czterożyłowy ϕ - 0,6mm- ok. 800m
- przy lokalnym zasilaniu FP - 3km. (FP może być zasilane bezpośrednio z linii)
- odległość pomiędzy Stacją Bazową i aparatem bezprzewodowym PP:
  - w obszarze niezabudowanym 200 - 300m
  - wewnątrz budynków, w obszarze zabudowanym 20 - 80m
  - FP z anteną dookolną - 80 - 300m
  - FP z anteną kierunkową 300 - 800m

Do VARIX 14/DECT można podłączyć również aparaty sieci abonenckiej PABX, zarówno analogowe, jak i cyfrowe.

Dla poprawnego określenia ilości i punktów rozmieszczenia stacji bazowych systemu, zamawiający powinien dostarczyć następujące informacje:

- zwymiarowane plany pomieszczeń obiektu (wszystkie kondygnacje), w którym ma być używany system (także klatki schodowe i inne pomocnicze pomieszczenia),
- przebiegi instalacji teletechnicznych mogących wprowadzać zakłócenia jak i tłumić sygnał użyteczny (sieci energetyczna, telefoniczna, antenowa, wodociągowa, gazowa, grzewcza, alarmowa),
- liczba i rodzaj innych systemów radiowych używanych na obiekcie (radiostacje, radiotelefony, telefony komórkowe, telefony bezprzewodowe, systemy monitoringu, alarmowe i przywoławcze),
- plan zagospodarowania otoczenia obiektu (jeżeli użytkownicy systemu mają znajdować się także poza budynkiem obiektu),
- opis najczęściej występującej na obiekcie techniki zbrojenia ścian i stropów,
- planowana ilość używanych w systemie telefonów przenośnych,
- szczegółowy opis sposobu współpracy z centralą nadrzędną.

Dopiero po uzyskaniu tych informacji może przyjechać na obiekt ekipa serwisowa i dokonać niezbędnych pomiarów:

- natężenie pola elektromagnetycznego,
- przenikalność elektromagnetyczna ścian i stropów,
- wpływ pokrycia powierzchni ścian zewnętrznych).

Na podstawie przeprowadzonych pomiarów zostają określone ilość i miejsca zainstalowania stacji bazowych. Użytkownik (odpowiednie centrum reagowania kryzysowego) powinien doprowadzić do tych miejsc przewody od przełącznicy (skrętka 2 pary) i zakończyć je gniazdami.

Z uwagi na powszechność zastosowania, elastyczność rozbudowy systemu komutacyjnego oraz możliwość integracji nowych usług, a także dogodne warunki serwisowe proponuje się, aby system łączności telefonicznej Centrów Zarządzania Kryzysowego oprzeć o system komutacyjny DGT 3450 i system łączności dyspozytorskiej DGT 3490 firmy DGT Sp. z o.o.

5.4.5. Podsystem teleinformatyczny

Funkcje podsystemu

W koncepcji podsystemu teleinformatycznego dla potrzeb służb reagowania kryzysowego, podległych operacyjnie Centrum Zarządzania Kryzysowego szczególnie uwzględniono takie wymagania jak:

- otwartość – proponowane rozwiązania sieci powinny mieć cechy systemu otwartego, co umożliwi jej rozwój,
- standaryzacja sieci i elementów wchodzących w skład systemu teleinformatycznego;
- modyfikowalność sprzętu teleinformatycznego;
- niezawodność i żywotność - wykorzystanie w sieci urządzeń i systemów charakteryzujących się dużą wartością współczynnika wskaźnika gotowości operacyjnej, umożliwiających prostą i tanią ich obsługę oraz umożliwiających łatwe diagnozowanie ich stanu technicznego,
- bezpieczeństwo - zapewnienie wymaganego stopnia poufności, integralności i niezaprzeczalności przekazywanych informacji, efektywny system kontroli bezpieczeństwa, skuteczny system kontroli dostępu,
- podatność na zarządzanie,
- możliwość pełnej kontroli i sterowania systemem w ustalonym stopniu;
- zwiększenie wymaganej wierności przesyłania informacji.

Proponowany system teleinformatyczny będzie zbudowany w oparciu o technologie cyfrowe i będzie zapewniał następujące usługi:

- transmisji danych komputerowych (plików graficznych, tekstowych, innych dużych plików binarnych);
- transmisji głosu;
- video i telekonferencję;
- usługi faksowe grupy IV;
- usługi radiodostępu poprzez analogowe łącze radiotelefoniczne lub z wykorzystaniem cyfrowego systemu łączności trankingowej;
- usługi cyfrowej sieci z integracją usług wąskopasmowej (N-ISDN) i szerokopasmowej (B-ISDN);
- pocztę elektroniczną (e-mail);

- możliwość korzystania ze stron WWW zamieszczanych w sieci intranetowej,
- obsługę sieci intranetowej (wydzielonej sieci teleinformatycznej) Centrum Reagowania

Kryzysowego z serwisami:

- bezpiecznym ftp;
- bezpiecznym WWW;
- bezpiecznym systemem pracy grupowej.

System teleinformatyczny dedykowany na potrzeby Centrum Zarządzania Kryzysowego powinien zapewniać komunikację pomiędzy dowolnymi węzłami sieci w relacji punkt-punkt, charakteryzującą się niezawodnością, krótkim czasem zestawiania połączenia, efektywnością, transferu danych oraz odpowiedzi systemu.

System powinien być wyposażony w łatwe w obsłudze terminale. System teleinformatyczny powinien zapewniać zdolność działania nawet w warunkach skrajnie niekorzystnych np.: w warunkach celowego destruktywnego oddziaływania.

Struktura podsystemu teleinformatycznego

Mając na uwadze wymagania odnośnie systemu teleinformatycznego oraz oszacowania dotyczące zapotrzebowania na przekazywanie informacji w projektowanym systemie, przyjęto następujące elementy składowe sieci teleinformatycznej:

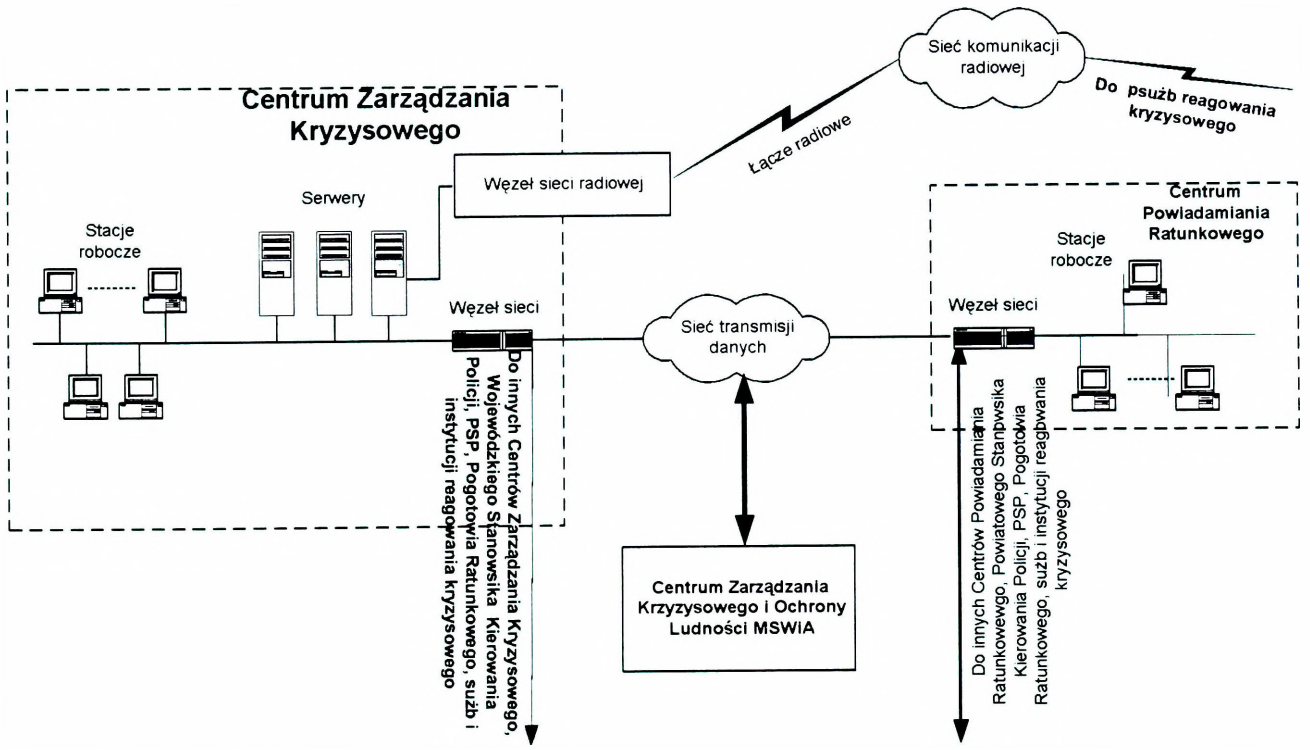
- ***podsystem łączności trankingowej*** – działający w oparciu o międzynarodowy standard TETRA . Standard TETRA umożliwia przesyłanie w kanale radiowym zarówno sygnały mowy jak i danych w trybie połączeniowym, a także w trybie pakietowym.
- ***podsystem dynamicznej lokalizacji sił i środków*** - zadaniem systemu będzie przesyłanie informacji o położeniu sił reagowania kryzysowego, operujących w terenie, co pozwoli na sprawne i efektywne zarządzanie posiadanymi zasobami. System musi gwarantować wystarczającą dokładność wskazań w celu umożliwienia jednoznacznej lokalizacji.
- ***podsystem monitoringu i automatycznego powiadamiania o zdarzeniach***.
- ***podsystem teletransmisyjny*** – tworzy sieć węzłów Centrów Powiadamiania Ratunkowego podległych danemu Centrum Zarządzania Kryzysowego oraz węzłów zlokalizowanych w instytucjach i służbach reagowania kryzysowego, powiązanych ze sobą siecią wymiany danych. Sieć wymiany danych będzie szkieletem całego

podsystemu, stanowi medium transmisji danych pomiędzy poszczególnymi stanowiskami. Umożliwia dostęp do baz danych samego systemu jak i systemów zewnętrznych, wymianę komunikatów, obsługę poczty elektronicznej oraz komunikację z obiektami sieci zewnętrznych.

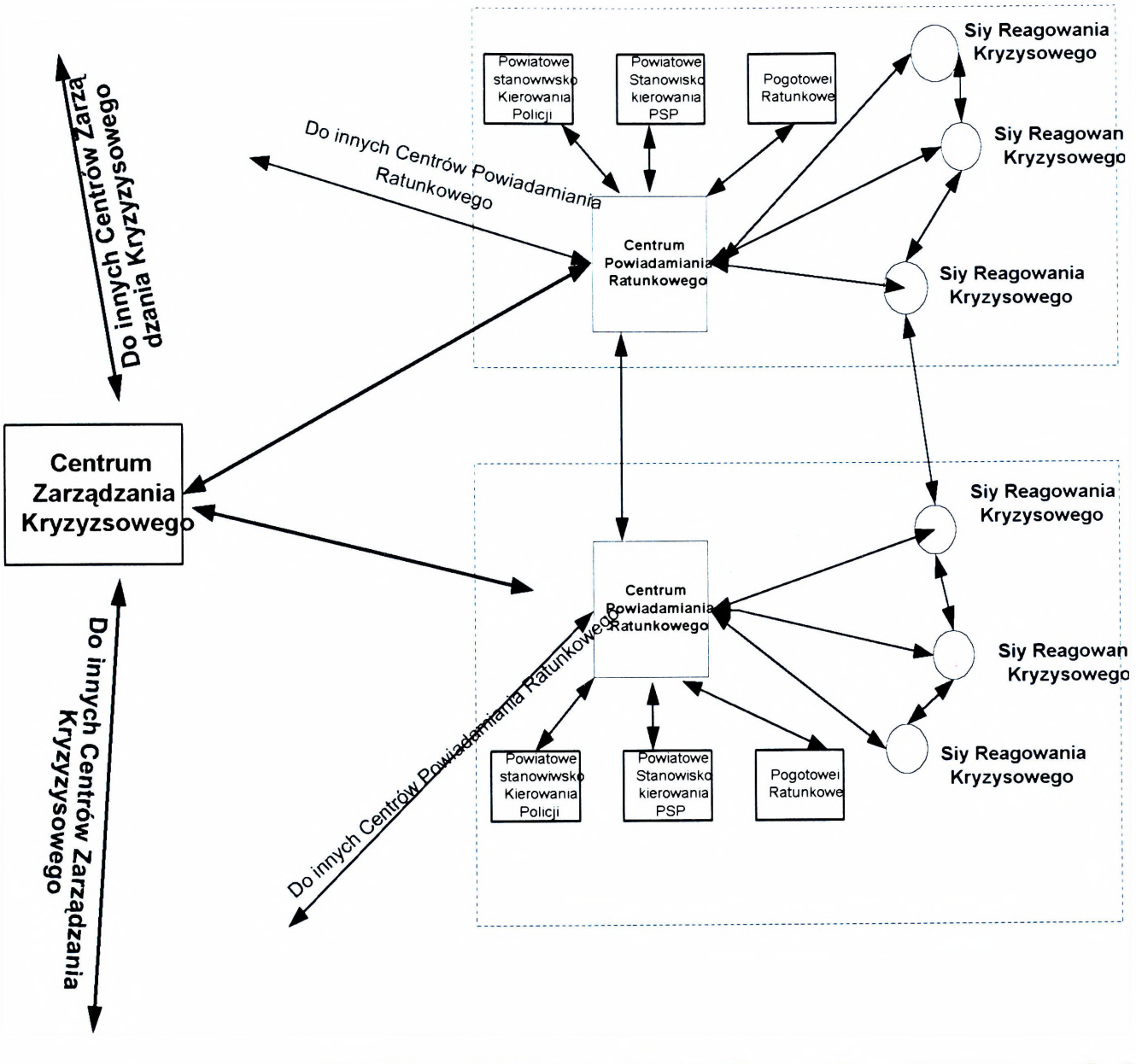
Należy przyjąć topologię podsystemu teleinformatycznego typu gwiaździsto-pierścieniową co umożliwia zapewnienie dużej redundancji w zakresie wykorzystywanych łączy. Takie rozwiązanie zapewnia realizację połączenia punkt-punkt. Połączenia pomiędzy Centrum Zarządzania Kryzysowego a poszczególnymi węzłami mogą być zrealizowane poprzez sieć szkieletową, mogą być dodatkowo dublowane łączami radiowymi trankingowymi lub istniejącymi łączami radiowymi KF/UKF.

Połączenie pomiędzy węzłami Centrów Powiadamiania Ratunkowego a siłami reagowania kryzysowego powinno się odbywać poprzez sieć szkieletową i łącza radiowe. Ponieważ siły reagowania kryzysowego działające w obrębie danego Centrum powiadamiania Ratunkowego bardzo często współpracują ze sobą zapewniono między nimi dedykowane łącza przewodowe jak również dedykowane łącza radiowe.

Podsystem powinien mieć możliwość obsługi informacji z różnymi priorytetami, co wiąże się z określeniem tzw. „czasu życia".



Rys. 5.4.5.1. Relacje informacyjne podsystemu teleinformatycznego dla potrzeb reagowania kryzysowego



Rys. 5.4.5.2. Struktura logiczna podsystemu teleinformatycznego dla potrzeb Centrum Zarządzania Kryzysowego

Zrealizowanie dostępu do zasobów informacyjnych przechowywanych w bazie danych i do zasobów informacyjnych sieci LAN Centrum Zarządzania Kryzysowego będzie możliwe za pomocą węzła dostępowego. Umożliwi on dostęp do zewnętrznych systemów informatycznych (PESEL, EWID itp.). Proponowane rozwiązanie zakłada, że Centrum Zarządzania Kryzysowego oraz Centra Powiadamiania Ratunkowego będą przyłączone do sieci transmisji danych, zorganizowanej w oparciu o łącza dzierżawione X.25, komutowane B-ISDN lub półstałe Frame Relay.

System monitorowania położenia służb reagowania kryzysowego będzie zbudowany w oparciu o system *GPS (ang. Global Positioning System).* Poprzez węzeł radiowy będzie on połączony do sieci LAN w Centrum Zarządzania Kryzysowego. W sieci LAN Centrum

Zarządzania Kryzysowego przewidziano zainstalowanie komputera, pełniącego rolę serwera komunikacyjnego, który zostanie wyposażony w oprogramowanie przechwytujące informacje o położeniu patroli z przekazywanych za pośrednictwem sieci radiowej, a następnie po odpowiednim przetworzeniu zawartej w nich informacji będzie zasilał system informatyczny.

Stacjonarna część systemu powinna się składać ze sterownika stacji bazowych, gateway'a radiowego, routera i lokalnej sieci komputerowej LAN. Uwzględniając liczbę terminali ruchomych w celu prowadzenia wielu transmisji jednocześnie, gateway radiowy powinien być wyposażony po stronie sterownika stacji bazowych w porty komunikacyjne.
Od strony sieci LAN zaleca się stosowanie protokołu UDP/IP, optymalnego z punktu widzenia generowanego obciążenia systemu radiowego.

Konfiguracja i liczba portów modułu szyfrowania/deszyfrowania będzie zależeć od wymaganej liczby kluczy szyfrowych jednocześnie wykorzystywanych w systemie oraz liczby jednocześnie prowadzonych połączeń szyfrowanych.
Rozpatrzono dwa warianty realizacji przedstawionej koncepcji:

- **W wariancie 1.** jako terminale łączności bezprzewodowej części mobilnej proponuje się wykorzystanie radiotelefonów cyfrowych, aktualnie będących na wyposażeniu patroli służb reagowania kryzysowego. Radiotelefony powinny umożliwiać pracę w systemie, w trybie transmisji pakietowej, poprzez łącze RS-232 C z przepływnością, co najmniej 9,6 kbit/s, z zastosowaniem protokołu korekcji błędów oraz z potwierdzeniem poprawności transmisji. Radiotelefony powinny posiadać możliwość szyfrowania oraz mieć włączone funkcje transmisji danych.
- **W wariancie 2.** część mobilna będzie oparta o system trankingowy w standardzie TETRA. Celem zapewnienia efektywnej wymiany danych pomiędzy terminalami noszonymi, lub przewoźnymi a systemem komputerowym na Centrum Zarządzania Kryzysowego oraz Centrum Powiadamiania Ratunkowego proponuje się wykorzystanie centralnego gateway'a radiowego systemu trankingowego z protokołem IP.

Od strony radiowej gateway będzie współpracował z komutatorem radiowym nadając i odbierając informacje z/do radiotelefonów trankingowych. Od strony systemu komputerowego wykorzystywany będzie protokół TCP/IP.

Zaleca się, ze względu na dokładność, zastosowanie odbiornika GPS pracującego w systemie różnicowym, zapewniającym dokładność lokalizacji rzędu 1- 15 m. Dodatkowo dla poprawnej pracy systemu lokalizacji w skrajnie trudnych warunkach, wykorzystany może być moduł nawigacji inercyjnej.

Głównym elementem części mobilnej dla służb reagowania kryzysowego będzie komputer przenośny (doręczny – palmtop) o podwyższonej wytrzymałości, połączony z odbiornikiem GPS i radiotelefonem.

ZAKOŃCZENIE

płk dr hab. inż. Józef Władysław MICHNIAK

W ostatnich latach prowadzi się intensywne prace nad powszechnym wdrożeniem do eksploatacji radiostacji definiowanych programowo SDR (*ang. Software Defined Radio)*. Z tymi urządzeniami należy wiązać duże nadzieje, gdyż można w zależności od wymagań użytkownika „dostosować", za pomocą odpowiedniego oprogramowania, właściwości takiej radiostacji do aktualnych potrzeb, co przy dużej zmienności sytuacji i potrzeb występujących w ratownictwie i zarządzaniu kryzysowym jest cenne.

Dynamiczny rozwój systemów telefonii komórkowej doprowadził do prac nad systemami telefonii komórkowej III generacji IMT *(ang. International Mobile Telecommunications)*, które zakładają integrację segmentu naziemnego z segmentem satelitarnym, udostępnianie w pełni zintegrowanych usług dla użytkowników w ruchu, niezależnie od tego, gdzie się znajdą, szeroką integrację z sieciami inteligentnymi i sieciami IP, maksymalną miniaturyzację terminali abonenckich, rozwijanie idei SDR w odniesieniu do terminali a ponadto udostępnienie otwartej i podatnej na integrację architektury. Wykorzystanie tak rozumianych terminali do rozważanych zastosowań byłoby bardzo wskazane.

Bez efektywnie funkcjonujących środków łączności organy zarządzania kryzysowego byłby pozbawione komunikacji ze służbami reagowania kryzysowego, dla których z założenia mają stanowić kolegialne ciało decyzyjne. Brak możliwości komunikacyjnych oznacza również nie posiadanie aktualnych danych na temat stanu otoczenia (środowiska, społeczeństwa, gospodarki, itp.), który jest jednym z istotniejszych czynników przy opracowaniu decyzji (dyrektyw wykonawczych dla służb) dotyczących zarządzania kryzysowego.

Projektanci i analitycy opracowywanych obecnie systemów komputerowego wspomagania zarządzania kryzysowego, niezależnie od ich merytorycznego zakresu funkcjonowania (czy wspomagają tylko i wyłącznie monitorowanie sytuacji kryzysowych, czy służą również do wsparcia procesów analityczno-decyzyjnych, planowania, tworzenia strategii powrotu do stanu równowagi) muszą na etapie ich tworzenia uwzględniać właściwości aktualnie dostępnych technologii telekomunikacyjnych.

Podejście polegające na „dostawieniu" do opracowanego już systemu wspomagania zarządzania kryzysowego komponentu telekomunikacyjnego jest dziś mocno nie adekwatne do

oczekiwań, gdyż nie zapewnia dostosowania sposobu dostarczania (przekazywania) informacji do specyfiki systemu, nie gwarantuje pełnej integracji oraz nie zawsze zapewnia skalowalność.

Dostępne systemy i technologie telekomunikacyjne są mocno wspierane przez oprogramowanie, większość głównych funkcji jest realizowana za pomocą specjalizowanych modułów programowych, komunikujących się za pomocą API.

Ten fakt dostarcza dodatkowego argumentu za tym, aby integrację komponentu telekomunikacyjnego projektowanego systemu wspomagania zarządzania kryzysowego zaczynać od początku jego opracowywania, traktując usługi telekomunikacyjne niezbędne do działania systemu jako jego funkcje organiczne, a nie jako funkcje dostępne w „jakimś" istniejącym systemie (urządzeniu) telekomunikacyjnym, który „później" zostanie dołączony (niekoniecznie zintegrowany).

Taki sposób postępowania gwarantuje prostą i tanią rozbudowę systemu wspomagania zarządzania kryzysowego o nową funkcjonalność, gdyż „wzrost" systemu dotyczy całości a nie osobno systemu informatycznego i telekomunikacyjnego.

Aby takie działanie było możliwe konieczne jest uświadomienie sobie stanu rozwoju współczesnych technologii telekomunikacyjnych oraz śledzenie ich rozwoju pod kątem zastosowań oferowanej funkcjonalności w systemach wspomagania zarządzania kryzysowego.

BIBLIOGRAFIA

1. BARANOWSKI Z., ZMYSŁOWSKI D. "Zastosowanie standardu DECT dla potrzeb dowodzenia kierowania i zarządzania" Materiały VIII Konferencji Naukowej "Automatyzacja Dowodzenia" 2000;
2. BEM D. J., GRZYBOWSKI M. J., WIĘCŁAWSKI T. W., ZIELIŃSKI R. J. "Systemy komunikacji ruchomej trzeciej generacji" Materiały Krajowego Sympozjum Telekomunikacji 1999;
3. BIAŁAS R. "Możliwości aplikacji sieci łączności komórkowej dla potrzeb obronności RP" Materiały Krajowej Konferencji Radiokomunikacji i Radiodyfuzji 1996;
4. DUDEK Z. T "Nowe systemy telefonii satelitarnej" Wiadomości Telekomunikacyjne 9/1998;
5. FRĄCZYK P., MODLIŃSKI G. "Opis systemu GPS" Materiały Krajowego Centrum Informacji GPS;
6. FIOŁNA Z., MICHNIAK J. "Sieć łączności państwa" AON, Warszawa 2000;
7. HOŁUBOWICZ W., PÓŁCIENNIK P., RÓŻAŃSKI A. "Systemy łączności bezprzewodowej" Wydawnictwa EFP, Poznań 1996;
8. HOŁUBOWICZ W., PÓŁCIENNIK P. "GSM cyfrowy system telefonii komórkowej" Wydawnictwa EFP, Poznań 1995;
9. HUK R, KOŁODZIŃSKI E., ZMYSŁOWSKI D. "Wykorzystanie technologii internetowych w systemach dowodzenia, kierowania i zarządzania. Perspektywy, szanse i zagrożenia" Materiały IX Konferencji Naukowej „Automatyzacja Dowodzenia" 2001;
10. KOŁODZIŃSKI E., MATELA J., PIETKIEWICZ T. "System reagowania kryzysowego MON w systemie bezpieczeństwa państwa" Materiały X Konferencji Naukowej „Automatyzacja Dowodzenia" 2002;
11. KOŁODZIŃSKI E., MATELA J. "Model systemu reagowania kryzysowego państwa" Materiały IX Konferencji Naukowej „Automatyzacja Dowodzenia" 2002;
12. KRASON J. "TETRA - otwarty standard cyfrowej łączności trankingowej" Wiadomości Telekomunikacyjne 3/2000;
13. ORŁOWSKI A. "Systemy trankingowe" Materiały Seminarium „Łączność w stanach nadzwyczajnych zagrożeń" Instytut Łączności, Warszawa 2000;
14. RYCZER A. "Satelitarne systemy monitorowania i lokalizacji pojazdów samochodowych" Wiadomości telekomunikacyjne 9/1998;

15. GÓRNY P., SIENKIEWICZ P. ZASKÓRSKI P. "Teoria sytuacji kryzysowych" AON, Warszawa 2002;
16. WOJCIECHOWSKI M., WRONA T. "Zintegrowany programowany system łączności dla potrzeb służb ratownictwa i ochrony ludności" Materiały Seminarium „Łączność w stanach nadzwyczajnych zagrożeń" Instytut Łączności, Warszawa 2000;
17. WRAŻEŃ M. "Centrum Zarządzania Kryzysowego i System Łączności Służb Ratowniczych" WAT, Warszawa 2002;
18. Materiały Seminarium "Łączność w stanach nadzwyczajnych zagrożeń" Instytut Łączności, Warszawa 2000;
19. ZASKÓRSKI P. "Koncepcja systemu reagowania kryzysowego MON" AON, Warszawa 2002;
20. ZMYSŁOWSKI D. "Charakterystyka działania, właściwości i rozwiązania programowo-sprzętowe bezprzewodowych sieci LAN" Materiały IX Konferencji Naukowej „Automatyzacja Dowodzenia" 2001;
21. Materiały firmy Ericsson: "Systemowo- techniczne aspekty standardu DECT";
22. Materiały firmy Ericsson: "System EDACS";
23. "Satelitarne techniki sieciowe" - III Krajowa Konferencja Zastosowania Satelitarnych. Systemów Lokalizacyjnych GPS, Glonass Krajowe Centrum Informacji GRPS, Poznań 1998;
24. Specyfikacja standardu Bluetooth;
25. "Systemy satelitarne powszechnego użytku" Centrum Promocji i Szkolenia Teleinformatyki APEXIM, Warszawa 1998;

INTERNET

1. www.alcatsel.pl
2. www.bluetooth.com
3. www.netplan.dk
4. www.wapforum.com
5. www.siemens.pl
6. www.telbank.pl
7. www.wlana.com.pl