ZNAJOMOŚĆ ZASAD ORGANIZACJI ŁĄCZNOŚCI RADIOWEJ UKF W JEDNOSTKACH ORGANIZACYJNYCH PSP I KSRG, W SZCZEGÓLNOŚCI NAWIĄZYWANIA I PROWADZENIA KORESPONDENCJI RADIOWEJ W SIECIACH RADIOWYCH PSP ORAZ ZNAJOMOŚĆ ZASAD TWORZENIA SCHEMATÓW ORGANIZACJI ŁĄCZNOŚCI PODCZAS AKCJI RATOWNICZO GAŚNICZEJ

(wersja do Internetu)

Materiały dydaktyczne dla studiów podyplomowych SPO w Szkole Głównej Służby Pożarniczej z tematu **„Znajomość zasad organizacji łączności radiowej UKF w jednostkach organizacyjnych PSP i KSRG, w szczególności nawiązywania i prowadzenia korespondencji radiowej w sieciach radiowych PSP oraz znajomość zasad tworzenia schematów organizacji łączności podczas akcji ratowniczo gaśniczej”.**

W ramach tej części wykładu omówione zostaną następujące zagadnienia:

1. *Wiadomości wstępne z zakresu telekomunikacji* - definicje; pojęcia podstawowe; telekomunikacja w różnych aspektach działalności człowieka, historia rozwoju dziedziny.
2. *Kryteria klasyfikacyjne i podział telekomunikacji* - podział telekomunikacji ze względu na zdefiniowane kryteria - przeznaczenia, rodzaju przesyłanych wiadomości, procesów zachodzących w trakcie przesyłania informacji, media transmisyjne, wielokrotne wykorzystanie łączy - zwielokrotnienie częstotliwościowe; modulacje impulsowe i cyfrowe; zwielokrotnienie czasowe.
3. *Zintegrowane systemy łączności* - cyfryzacja systemów łączności; systemy IDN; systemy ISDN i rodzaje usług.
4. *Propagacja fal radiowych* - budowa atmosfery i jej wpływ na propagację fali elektromagnetycznej; podział i przeznaczenie zakresów fal radiowych.
5. *Urządzenia radiokomunikacyjne i systemy radiokomunikacji ruchomej* - budowa, zadania

   i podstawowe parametry urządzeń nadawczych; budowa zadania i podstawowe parametry urządzeń odbiorczych; podział i przeznaczenie poszczególnych typów radiokomunikacji ruchomej; systemy przywoławcze; systemy telefonii bezprzewodowej; systemy trankingowe analogowe; systemy trankingowe zamknięte EDACS; trankingowe systemy cyfrowe TETRA; systemy telefonii komórkowej analogowe i cyfrowe standardów GSM900 i DCS (GSM 1800); systemy radiokomunikacji satelitarnej; satelitarne systemy łączności osobistej.
6. *Bezpieczeństwo systemów łączności* - usługi ochrony informacji; przedsięwzięcia organizacyjne i techniczne zabezpieczające przed ucieczką informacji; systemy kryptograficzne symetryczne i asymetryczne; autentyzacja i autoryzacja użytkownika terminala abonenckiego.

Spis treści

I. Wstęp.

Niniejsze opracowanie materiału dydaktycznego, powstało w oparciu o prowadzony od wielu lat w Szkole Głównej Służby Pożarniczej w Warszawie przedmiot „Łączność i alarmowanie". Przedmiot ten obejmuje 60 godzin zajęć (30 wykładów, 15 ćwiczeń i 15 laboratorium). Na studiach podyplomowych dla strażaków ubiegających się o pierwszy stopień oficerski w PSP, problemy łączności i alarmowania „włożono" do bloku „Informatyka i Łączność" w postaci tematu; „Znajomość zasad organizacji łączności radiowej UKF w jednostkach organizacyjnych PSP i KSRG, w szczególności nawiązywania i prowadzenia korespondencji radiowej w sieciach radiowych PSP oraz znajomość zasad tworzenia schematów organizacji łączności podczas akcji ratowniczo – gaśniczej" w wymiarze 16 godzin wykładów i 10 godzin ćwiczeń. Z tego powodu wynikła konieczność szerszego opracowania materiałów dydaktycznych aby zapoznać słuchaczy z całością problematyki podsystemu łączności w systemie wspomagania dowodzenia i zarządzania kryzysowego ponieważ „przydzielona" liczba godzin nie wystarcza na pełne omówienie, ważnej z punktu widzenia działalności PSP, problematyki.

Opracowując ten materiał korzystałem z doświadczeń własnych i przytoczonej poniżej literatury. Rysunki zamieszczone w opracowaniu są autorstwa piszącego bądź zaczerpnięte z umieszczonego poniżej wykazu literatury, jak również niektóre fragmenty opracowania są wypisami z przywołanej literatury.

II. Literatura.

1. Dębicki St.: *Historia telekomunikacji.* WKiŁ, Warszawa 1963.
2. Turski W.M.: *Propedeutyka informatyki.* PWN, Warszawa 1975.
3. Barczak A. Florek J. Sydoruk T.: *Podstawy telekomunikacji dla informatyków.* WAP, Siedlce 2010.
4. Praca zbiorowa: *Komutacyjne systemy cyfrowe.* WSOWŁ, Zegrze 1996.
5. Pod red. Bromirski M.: *Materiały – Sieci inteligentne.* Instytut Łączności , W-wa 2000.
6. Praca zbiorowa pod red Dąbrowski M.: *Sterowanie i oprogramowanie w telekomunikacyjnych sieciach zintegrowanych.* WK i Ł, Warszawa 1990.
7. Janulis R.: *Urządzenia nadawcze radiokomunikacyjne i radiofoniczne.* WSiP, Warszawa 1975.
8. Wesołowski K.: *Systemy radiokomunikacji ruchomej.* WK i Ł, Warszawa 1999,
9. Chaciński H.: *Urządzenia radiowe.* WS i P, Warszawa 1989.
10. Wodzyński B.: *Radiotelefony.* WK i Ł, Warszawa 1981.
11. Hołubowicz W. Szwabe M.: *GSM ależ to proste.* Wyd. Holkom, Poznań 1999.
12. Górz A.: *Dlaczego radiotelefony.* Wyd. MON, Warszawa 1960.
13. Gotfryd M.: *Podstawy telekomunikacji, telekomunikacja analogowa i cyfrowa.* OWPRz, Rzeszów 2011.
14. Lisicki W.: *Propagacja fal radiowych..* WK i Ł, Warszawa 1962.
15. Dołuchanow M. P. *Rozchodzenie się fal radiowych.* PWN, Warszawa 1965.
16. Bem D. J.: *Anteny i rozchodzenie się fal radiowych..* WNT, Warszawa 1973.
17. Lubański A.: *Podstawy transmisji danych.* WSOWŁ, Zegrze 1973.
18. Baran Z. (red.): *Podstawy transmisji danych..* WKiŁ, Warszawa 1982.
19. Haykin S.: *Systemy telekomunikacyjne. T 1 i 2.* Wyd. WKiŁ, Warszawa 2000.
20. Jajszczyk A.: *Wstęp do telekomutacji.* WNT, Warszawa 2004.
21. Kościelnik D.: *ISDN. Cyfrowe sieci zintegrowane usługowo.* WKiŁ, Warszawa 2001.
22. Norris M.: *Teleinformatyka..* Wyd. WKiŁ, Warszawa 2002.
23. Trusz W. (red.): *Poradnik teleelektronika.* WKiŁ, Warszawa 1974
24. Read R.: *Telekomunikacja..* WKiŁ, Warszawa 2000.
25. Tadeusiewicz R.: *Sygnał mowy.* WKiŁ, Warszawa 1988.
26. Urbanek A.: *Ilustrowany Leksykon Teleinformatyka*. Wyd. IDG, Warszawa 2001.

27. Praca zbiorowa.: *Vademecum Teleinformatyka I.* Wyd. IDG, Warszawa 1999.
28. Molski M.: *Podstawy bezpieczeństwa systemów informatycznych.* MSG Media, Bydgoszcz 1998.
29. Molski M. Opala S.: *Bezpieczeństwo systemów informatycznych..* Wyd. Mikom 2002.
30. Denning D.: *Kryptografia i ochrona danych.* WNT , 1992.
31. Rączkiewicz M.: *Bezpieczeństwo sieci komputerowych.* Wyd. FPT, Kraków 1995.
32. Hucał M.: *Podstawy radiokomunikacji.* CSŁiI Zegrze 1999.
33. Ogólnodostępne materiały dydaktyczne udostępniane na stronach internetowych Uczelni Technicznych: Politechnika Warszawska, Politechnika Gdańska, Politechnika Wrocławska, Politechnika Szczecińska (obecnie ZUT), Akademia Górniczo Hutnicza, Akademia Techniczno Rolnicza Bydgoszcz (obecnie UTP), Politechnika Poznańska oraz internetowe materiały Instytucji „z branży" UKE (Urząd Komunikacji Elektronicznej), WBZC (Wojskowe Biuro Zarządzania Częstotliwościami), IŁ (Instytut Łączności), CSŁiI (Centrum Szkolenia Łączności i Informatyki) Zegrze i inne.
34. Materiały konferencyjne cyklicznych corocznych konferencji branżowych: Krajowe Sympozjum Telekomunikacji (obecnie KSTiT), Krajowa Konferencja Radia i Telewizji, Konferencja Systemy Ochrony Informacji Enigma, tematyczne Konferencje SEP (Stowarzyszenie Elektryków Polskich).
35. Hołubowicz W., Płuciennik P., Różański A.: *Systemy łączności bezprzewodowej.* Wyd. EFP, Poznań 1997.
36. Ludwin W. (red), *Bluetooth.* Uczelniane Wyd. Naukowo-dyd. AGH, Kraków 2003.
37. Wrona M., *Niebezpieczeństwa komputerowe.* Wyd.RM, Warszawa 2000.
38. Stokłosa J., *Algorytmy kryptograficzne.* OWN Poznań 1994.
39. Praca zbiorowa, *Analiza możliwości wykorzystania łączności satelitarnej jako segmentu hiperkomórek satelitarnych systemów GSM/3G/4G.* IŁ Gdańsk 2009.
40. Hoffman L.J., *Poufność w systemach informatycznych.* WNT Warszawa 1982.
42. Kusina B., *Analiza ryzyka wstępem do projektowania bezpieczeństwa teleinformacyjnego firmy.* Enigma 99 - Tutorial III. Warszawa 1999.

1. Pojęcia podstawowe, definicje.

1.1. Historia dziedziny

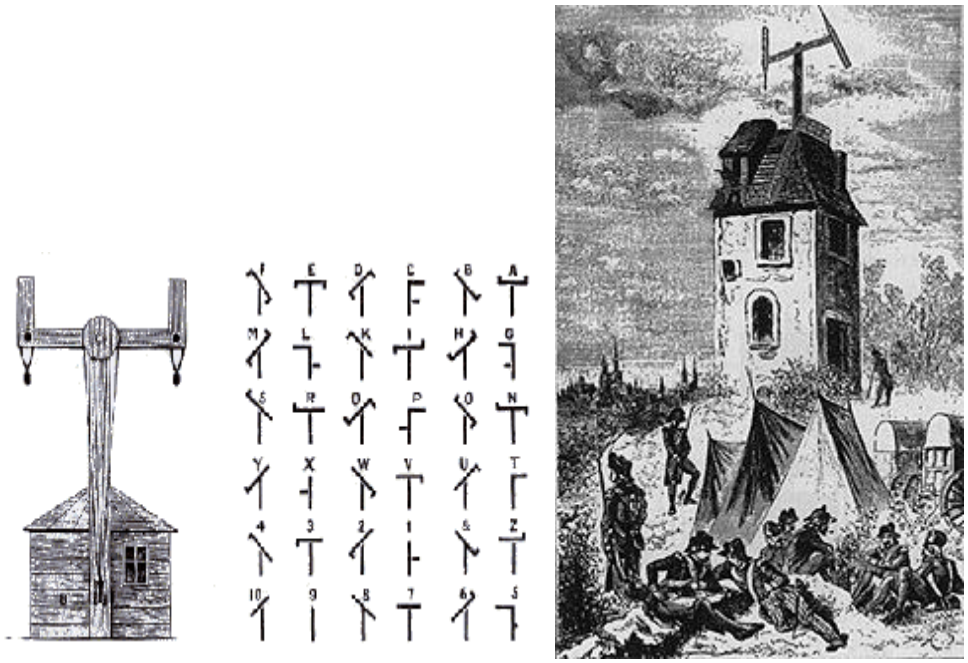
Pragnąc przekazać informację, człowiek, wykorzystując swe zmysły, podobnie zresztą jak inne żywe istoty, już od najdawniejszych czasów posługiwał się odpowiednimi sygnałami. Wykorzystując słuch i rozwijając system sygnałów dźwiękowych wytwarzanych w krtani i jamie ustnej – stworzył mowę. Ten ciągle doskonalony instrument wymiany informacji – porozumiewania się, miał zawsze jednak istotną wadę: bardzo ograniczony zasięg, wynikający zarówno z niewielkiej mocy źródła dźwięków mowy i niezbyt wysokiej czułości ucha jako ich odbiornika, jak i silnego tłumienia dźwięków w powietrzu. W najlepszych warunkach zasięg ten przekroczyć może niewiele ponad kilkadziesiąt metrów. Zastosowanie silniejszych źródeł dźwięku (np. bębnów tam-tam) i odpowiedniego kodu dźwiękowego umożliwiało bezpośredni zasięg przekazu informacji na kilka, a przy wielokrotnej „retransmisji" – nawet na setki kilometrów. Zastosowanie „transformatorów akustycznych" – telefon tubowy, telefon rurowy (odbijanie się fal głosowych w rurze, do dnia dzisiejszego wykorzystywane na okrętach i łodziach podwodnych) umożliwiło porozumiewanie się na odległości do 4 km balony, statki. Powstawały „galerie szeptów" zamki, kościoły dawały możliwość podsłuchiwania osób rozmyślnie ustawionych w konkretnych miejscach (odbijanie się fal głosowych na odpowiednio zakrzywionych ścianach – krzywizny eliptyczne lub paraboliczne). Zmysły dotyku, węchu i smaku tylko w niewielkim stopniu nadawały się do wykorzystania w porozumiewaniu się. I tak pozostało po dzień dzisiejszy. Pozostał jeszcze jeden zmysł: wzrok. Niemal doskonały ze względu na swą czułość i zdolność wprowadzania do mózgu w krótkim czasie ogromnych ilości informacji, zróżnicowanych barwą, jaskrawością, kontrastem, rozmiarami, odległością od przedmiotu i między przedmiotami obserwacji itd. Wzrok bezbłędnie identyfikuje ruch jako zmianę położenia. Nie jest zatem nic dziwnego w fakcie, że właśnie zmysł wzroku posłużył do stworzenia i udoskonalenia do dzisiejszej postaci systemu pisma. Aby jednak pismo niosące informację mogło spełnić swą rolę, należało je dostarczyć adresatowi. Od doraźnie wysyłanego gońca, poprzez regularne linie kurierskie, rozwinął się system przemieszczania listów i innych przesyłek – poczta. I przez wieki wystarczał list. Przekazywanie wiadomości tym sposobem zawsze miało jednak określone wady, bowiem przenoszenie lub przewożenie listu absorbuje tym więcej czasu, im większa odległość dzieli nadawcę i adresata oraz im wolniejszy jest środek lokomocji, jakim list

jest przewożony. Na przestrzeni dziejów możemy wybrać pewne „kamienie milowe" w rozwoju systemów porozumiewania się na odległość. Według Tragedii Ajschylosa, z 458 r. p.n.e. grecki wódz Agamemnon przesłał swojej żonie Klitajmestrze wieść o upadku Troi w 1184 r. p.n.e. Wiadomość była podana do Myken w ciągu 1 dnia za pomocą sygnałów ogniowych. Pierwsze ognisko było wzniecone w Małej Azji na górze Ida, drugie na wyspie Lemnos na Morzu Egejskim. Następnie na górze Atos na wyspie Eubei, dalej przez góry Mezapich, górę Kithairon w Attyce do góry Arachny i wartownika na dachu zamku Argos. Ciekawym jest, że nie było ogniska pośredniczącego na Sporadach, jakkolwiek odległość od góry Atos do Eubei wynosi 180 km. Sygnały ogniowe oraz dymne umożliwiały jedynie przesyłanie wiadomości uprzednio umówionych, a nie dowolnych. Problem ten próbowali rozwiązać około 450 roku p.n.e. dwaj Grecy z Aleksandrii: Kleozenes i Demokleites, których telegraf opisany został przez Polibiosa około 200 r. p. n.e. Skonstruowali oni telegraf, którego zasada działania polegała na zastosowaniu pięciu pochodni i tablic z alfabetem rozmieszczonym na dwudziestu pięciu polach, jakby na szachownicy. Na stacji nadawczej i odbiorczej znajdowały się ściany odpowiedniej wysokości i długości, zasłaniające zapalone pochodnie. Poziome szeregi liter liczyło się od góry w dół, a pionowe - od lewej strony ku prawej. Jeżeli przekazywana litera znajdowała się np. w drugim szeregu poziomym i trzecim pionowym, to wysuwano ponad ścianę najpierw dwie pochodnie z strony lewej a potem trzy z prawej strony. W ten sposób przekazywano wszystkie litery poszczególnych wyrazów przesyłanej wiadomości, którą zapisywała stacja odbiorcza.

Pojawił się „telegraf wodny", pomysł jego stworzenia przypisywany Aleksandrowi Macedońskiemu. W tym rozwiązaniu używano dwu pojemników na wodę (nadajnik i odbiornik) z zaworami umieszczonymi w dole zbiornika. Na machnięcie pochodnią otwierano oba kraniki i spuszczano wodę aż do drugiego machnięcia pochodni. To drugie było nakazem zamknięcia kranów. Treści komunikatów (rozkazów) zapisane były na tychże pojemnikach a poziom wody wskazywał właściwą treść (np. „atakujemy o świcie").

Innym przykładem może być przypadek Filipidesa. W 490 r.p.n.e. – wiadomość o zwycięstwie Miltiadesa nad Persami pod Maratonem przekazał przez przeniesienie gałązki laurowej (przebiegł do Aten 42 km 195 cm). W czasach już nowożytnych sir Robert Hooke wdrożył w Europie „telefon sznurkowy" (podobno wynalazek chiński) i rozmawiał na „wielkie" odległości do 800 m (dwa pojemniki metalowe połączone

naprężonym sznurkiem, fala głosowa przenoszona jako drgania mechaniczne poprzez ten sznurek, pobudzała do drgań pudełko po stronie odbiorczej co wywoływało drgania otaczającego powietrza i można było usłyszeć przekazywaną wiadomość. Szczytowym osiągnięciem systemów porozumiewania się na odległość ery z przed wynalezienia elektryczności jest skonstruowany w 1794 roku telegraf Chapp'a (nazwany tak na cześć jego wynalazcy Francuza Cloude Chappe). Był to telegraf optyczny. Pierwsza linia tego telegrafu łączyła miasta Paryż i Lille o długości 220 km którą to odległość podzielono 20-toma podstacjami. Czas przekazywania wiadomości wynosił kilka minut. Urządzenie to składało się z wysoko umieszczonego, drewnianego poziomego dźwigara i dołączonych na końcach ruchomych ramionach których położenie poprzez system cięgieł można zmieniać. Odpowiednie ich ustawienie odpowiadało określonej literze, a czasem całym słowom. Linie telegrafu optycznego składały się z wież oddalonych od siebie o 10 - 20 km.

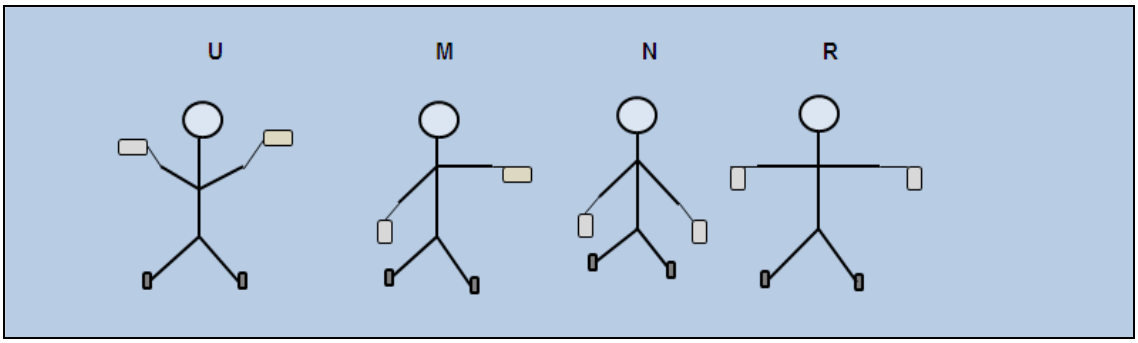


Rys.1.1. *Telegraf Chapp'a*

Dzięki temu wiadomość z Lyonu do Paryża docierała w ciągu 2 minut. W roku 1795 pierwsza linia telegrafu optycznego połączyła Londyn z portami południowej Anglii.

W Polsce pierwsza linia telegrafu optycznego powstała na trasie Warszawa - Modlin w roku 1830. W 1835 roku, po zbudowaniu 146 przekaźników, uruchomiono linię na trasie Warszawa - Sankt Petersburg. Sieć ta zaczynała się na dachu, zbudowanego dwa lata wcześniej, Teatru Wielkiego na warszawskim Placu Teatralnym. Z poziomu placu widoczny jest dziś taras małego balkonu, na którym przypuszczalnie

znajdował się telegraf. W 1838 roku uruchomiono sieć telegrafów na trasie Warszawa - Moskwa składającą się z 220 stacji obsługiwanych przez 1320 operatorów. Rozwój telegrafu elektrycznego spowodował około połowy XIX wieku zmierzch telegrafu optycznego i jego całkowite wyeliminowanie około 1880 roku. Pozostałością tego systemu jest stosowana do dnia dzisiejszego we wszystkich marynarkach świata łączność znana jako semafor (telegraf chorągiewkowy). Sygnalista trzymając w rękach chorągiewki i układając ramiona w właściwej dla danej litery pozycji przekazuje treść komunikatu.



Rys.1.2. *Telegraf chorągiewkowy - semafor*

Metody porozumiewania się na odległość zmieniły się radykalnie po wynalezieniu elektryczności. Za początek „ery" elektryczności uznać należy odkrycie przez Alesandro Volta baterii, było to początek elektrotechniki co spowodowało rozwój telekomunikacji, elektroniki i informatyki. Określenia **„Telekomunikacja"** - po raz pierwszy użył w 1904 r. M. Estaunie w pracy „*Traite prakttigue des Telekomunications electriques*". (dosłownie: *Rozprawa praktyczna o telekomunikacji elektrycznej*"), Dyrektor Departamentu Ministerstwa Poczt i Telekomunikacji, elektryk, literat, członek Akademii Francuskiej. Termin ten powstał z dwu określeń TELE – odległy, oddalony (od greckiego Tele – „daleko") oraz KOMUNIKACJA (od łacińskiego communicare – „dzielić; brać udział", communis – wspólny, powszechny). Więc mówimy, że ***„Telekomunikacja jest to dziedzina wiedzy i działalności naukowo – badawczej, gospodarczej zajmującej się przekazywaniem na odległość informacji z wykorzystaniem przeważnie energii elektrycznej".*** Termin telekomunikacja oznacza więc przesyłanie od nadawcy do odbiorcy informacji, danych multimedialnych w postaci sygnałów elektrycznych analogowych lub cyfrowych a medium fizycznym jest energia pola elektromagnetycznego. Ważnym jest aby

pamiętać, że telekomunikacja, w odróżnieniu od klasycznej teorii informacji, nie analizuje zawartości merytorycznej ani uczuciowej przesyłanej wiadomości.

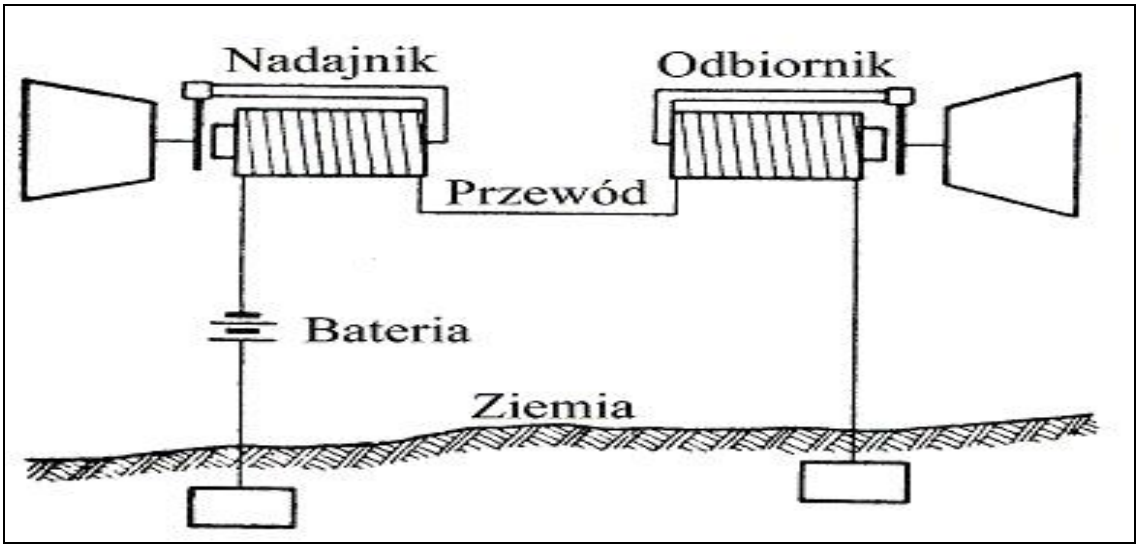
Podstawowe zadania telekomunikacji to:

1. Przekazanie szeroko rozumianej informacji z umownego punktu A do B w akceptowalnym przez uczestników procesu czasie.
2. Przekazanie tej informacji w niezniekształconej formie (informacja po stronie odbiorczej ma być „tożsama" co po stronie nadawczej. W praktyce oznacza to, że ma być odtworzona z akceptowalnym poziomem błędu.
3. Podczas procesu przekazu, należy zapewnić właściwą ochronę treści przekazywanej informacji. Tajemnica korespondencji jest jedną z około 30 tajemnic prawnie chronionych w systemie prawnym Polski.

Za początek **telegrafii** uznaje się datę 24 maja 1844 roku gdy została uruchomiona pierwsza linia telegraficzna z Sądu Najwyższego w budynku Kapitolu w Waszyngtonie – do odległego o 60 km Baltimore. Samuel Morse przesłał pierwszy komunikat w języku staroangielskim; „What hath God wrough?" – „Co stworzył Bóg ?". Istota tego wynalazku, obecnie wydaje się bardzo prosta. Po stronie nadawczej klucz przerywał obwód zasilania (plus baterii, przewód linii, uzwojenie elektromagnesu do „ziemi" i powrót do minusa baterii) elektromagnesu po stronie odbiorczej. Mechanizm sprężynowy przesuwał ze stałą prędkością taśmę papierową i umieszczony na kotwiczce elektromagnesu rysik kreślił linię odpowiadającą czasowi zamknięcia klucza, kropkę lub kreskę. Zachowanie tajemnicy korespondencji było trudne, gdyż jej treść trzeba było ujawnić telegrafiście. Stąd też duży wysiłek wkładano w prace nad systemem w którym można by było wyeliminować pośrednictwo tegoż telegrafisty, czyli zbudowania systemów telefonicznych.

Za początek przewodowej **telefonii** uznaje się datę 10 marca 1876 rok, a za jej twórcę Alexandra Grahama Bell'a. Był to pochodzący ze Szkocji lekarz który zawodowo pracował w Ameryce Północnej. Prowadził zajęcia z dziećmi niesłyszącymi. Nic więc dziwnego, że dźwięki i ich propagacja stały się przedmiotem jego zainteresowań. Początkowo zaczął wykorzystywać diafragmę, która wykonywała drgania pobudzana tembrem ludzkiego głosu. W trakcie swoich eksperymentów zaobserwował ciekawe zjawisko. Mianowicie zaobserwował, że taka diafragma umieszczona w pobliżu elektromagnesu wywoływała zmiany w polu magnetycznym emitowanym przez elektromagnes. A te zmiany w konsekwencji powodowały, że zmieniało się natężenie prądu elektrycznego w cewce elektromagnesu. Bell połączył

dwa takie elektromagnesy drutem. I tak na jednym końcu druta zachodziły opisane wyżej zmiany, a na drugim płynący prąd ulegał z powrotem transformacji w drgania diafragmy. Później nazwano to przetwornikami elektrodynamicznymi zaletą których jest to, że mogą one pracować jako mikrofon po stronie nadawczej i słuchawka po stronie odbiorczej. Po raz pierwszy udało się Bellowi przesłać wiadomość w obrębie tego samego budynku. Miała ona treść „Panie Watson, proszę przyjść tutaj, pilnie Pana potrzebuję".



Rys.1.3. *Telefon Bell'a*

Jak widać na przedstawionym schemacie, telefon Bella składa się z dwóch identycznych dwukierunkowych przetworników akustyczno-elektrycznych, które pełniły zarówno role mikrofonów, jak i głośników (słuchawek). Przetworniki składały się z membran o dużych powierzchniach, rdzeni ferromagnetycznych i nawiniętych cewek. Drgania membran połączonych z kotwicami magnetycznymi powodowały zmiany pola magnetycznego w obrębie cewek, co indukowało zmiany przepływającego przez cewki prądu elektrycznego. Obie cewki połączone są we wspólny obwód prądu stałego (w obwodzie włączone jest źródło napięcia stałego) i zmiennego (wywołanego w jednym i drugim przetworniku).

Jak widać ze schematu, telefon Bella pozwalał rozmawiać na odległość do 5 km. Warto też zauważyć, że „aparaty telefoniczne" połączone są jednym przewodem podobnie jak to było w telegrafie Morse'a a obwód elektryczny zamyka się przez Ziemię. Od tego przełomowego wynalazku, telefonu, nastąpił burzliwy rozwój systemów telefonicznych co z kolei spowodowało rozwój cywilizacji. Trudno sobie

dzisiaj wyobrazić jakąkolwiek celową działalność człowieka bez telefonu. Słynna wypowiedź Andrzeja Wajdy, reżysera, laureata Oskara, że film można nakręcić bez pieniędzy ale nie da się tego zrobić bez telefonu, potwierdza tą tezę. Z oryginalnego patentu Bela do dnia dzisiejszego w współczesnym telefonie pozostała słuchawka. Jako mikrofonu używamy rozwiązań innych niż przetwornik elektrodynamiczny, ze względu na małą czułość tego ostatniego, na przykład mikrofony elektretowe.

Przełom wieku XIX i XX to szereg prac poświęconych mediom transmisyjnym. Kilka najważniejszych dat to eksperymentalne potwierdzenie istnienia fal radiowych w 1887 roku przez Heinricha Hertza co potwierdziło teorię fal radiowych i elektromagnetyczną naturę światła Maxwella z 1873 r. opisane równaniami Maxwella. Guglielmo Marconiego przesłanie sygnału radiowego przez Atlantyk w roku 1901 i w 1906 r. nadanie programu radiowego zawierającego głos i muzykę, po zbudowaniu w tymże roku przez Dunwooda i Pickarda kryształkowego odbiornika radiowego co zapoczątkowało rozwój **elektroniki i radiokomunikacji.** Rok 1924 John Baird przesłał pierwszy obraz **telewizyjny**, znak krzyża nadany z odległości 3 m (pierwsze publiczne transmisje telewizyjne wprowadzono w Anglii w 1935 roku). Położenie trwałego kabla transatlantyckiego pomiędzy Europą i Ameryką, spowodowało upowszechnienie międzykontynentalnych systemów telekomunikacyjnych. W roku 1935 uruchomienie pierwszego działającego radaru w Anglii był początkiem **radiolokacji**. Rok 1938, cyfryzacja sygnału analogowego (telefonicznego) 8000 próbek/sek razy 8 bitów na próbkę daje przepływność binarną 64000 bitów/sek czyli 64 kb/s modulacja **PCM.** Rok 1946 na Uniwersytecie Pensylwanii J.W. Mauchly i J.P Eckert uruchomili **uniwersalny komputer elektroniczny ENIAC** (*Electronic Numerical Integrator And Calculator,* 18 tys. lamp, 6 tys. przełączników, masa 30 ton o częstotliwości taktowania 100 kHz) początek rozwoju **informatyki**. Lata 1948-49 w laboratoriach firmy Bell Telephone Laboratories przez Johna Bardeena oraz Waltera Housera Brattaina **(tranzystor ostrzowy)** i Williama Bradforda Shockley'a **(tranzystor złączowy)**. Ci trzej naukowcy, za wynalazek tranzystora otrzymali Nagrodę Nobla z fizyki w 1956. Data uważana jest za początek rozwoju **mikroelektroniki.** Wystrzelenie w październiku 1957 roku przez ZSSR pierwszego sztucznego satelity Sputnik uważane jest za początek **telekomunikacji satelitarnej** (pomimo że, pierwsze komercyjne wykorzystanie takiego systemu łączności nastąpiło w roku 1965). Wynalezienie w 1960 roku przez T. Maimana **lasera** na światło czerwone (W Polsce prace nad technikami laserowymi prowadzone były od lat 60 – dziesiątych w WAT przez profesorów Zbigniewa

Puzewicza i Kazimierza Dzięciołowskiego) uważane są za początek **optoelektroniki.** Bardzo ważną datą w rozwoju systemów porozumiewania się na odległość jest rok 1969. W okresie „zimnej wojny" na zlecenie ARPA (*Advances Research Project Agency* - Agencji Departamentu Obrony USA) powstaje sieć **ARPANet**. Zastosowana w niej decentralizacja zarządzania i zastosowanie pakietowej transmisji danych zapewniały większą odporność w przypadku zniszczenia części węzłów sieci. Sieć Arpanet, początkowo wojskowa, po połączeniu w 1973 roku komputerów w USA z komputerami w Anglii i Norwegi przybrała charakter „cywilny" i umożliwiła Uczelniom, Ośrodkom Naukowym, Instytucjom przesyłać pliki tekstowe, pocztę elektroniczną uważana jest za początek **Internetu**.

Rok 1976 - opublikowano projekt sieci komputerowej **LAN** w technologii **Ethernet**. Został on opracowany przez Roberta Metcalfe'a w Xerox PARC czyli ośrodku badawczym firmy Xerox. Bazuje na idei węzłów podłączonych do wspólnego medium, wysyłających i odbierających za jego pomocą specjalne komunikaty (ramki). Ta metoda komunikacji nosi nazwę CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*). Wszystkie węzły posiadają niepowtarzalny adres MAC (*Medium Acces Control*) i umożliwiała transmisję z prędkością 10 Mb/s.

Od 1991 r. Fast Ethernet realizuje transmisje 100 Mb/s a rozwój sprzętu sieciowego obecnie umożliwia transmisje z szybkościami 1 Gb/s, a najnowsze rozwiązania 10 Gb/s. Ważnym rokiem w historii rozwoju radiokomunikacji jest rok 1991 w którym na konferencji TELECOM 91 w Genewie uruchomiono najpopularniejszy system radiokomunikacji ruchomej **GSM 900 MHz** oraz określono standard systemu **DCS** jako rozszerzenie standardu GSM w paśmie częstotliwości 1800 MHz.

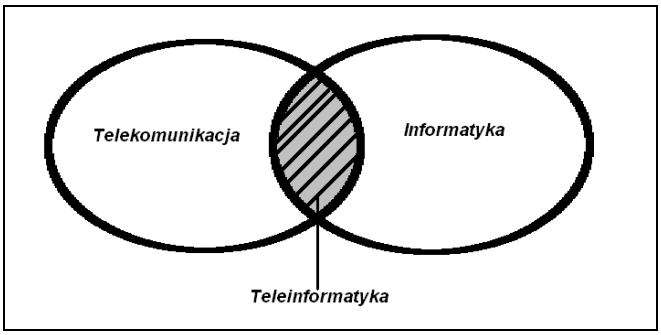
1.2. Technologie informacyjne

Informatyka jest nauką o przetwarzaniu informacji, zwłaszcza przy użyciu automatycznych środków pomocniczych. Myślenie – wyróżniająca cecha gatunku homo sapiens – jest specyficznym, wysoko zorganizowanym rodzajem przetwarzania informacji, ale przetwarzanie informacji jest także nieodłączną cechą każdego żywego organizmu, już nawet najprymitywniejszych jednokomórkowców.

Co więcej, przetwarzanie informacji zachodzi w żywych organizmach na różnych poziomach – poczynając od „wewnętrznego" przetwarzania informacji w obrębie jednej komórki i kończąc na „zbiorowym" przetwarzaniu informacji w kolektywie

porozumiewających się osobników, zbudowanych z wielu miliardów komórek każdy. Informatyka, jaką uprawia się obecnie, zajmuje się stosunkowo szczupłym obszarem przetwarzania informacji, dotyczącym najczęściej wiadomości z zakresu nauki, techniki, ekonomiki i danych społecznych, a w tym obszarze – takimi głównie procesami przetwarzania informacji, które są na tyle dobrze poznane, że można skonstruować urządzenia wykonujące te procesy zupełnie bez udziału człowieka lub przy jego niewielkiej pomocy. Termin informatyka (za francuskim *informatique*) zawdzięczamy prof. Romualdowi Marczyńskiemu, czyli dyscyplina inżynierska budowa komputerów - „maszyn cyfrowych" (chociaż komputer to nie tylko elektroniczna maszyna cyfrowa, ponieważ w pewnym okresie rozwoju systemów przetwarzania informacji stosowane były maszyny analogowe np. skonstruowana w WAT - UMA 601) oraz gromadzenie, organizowanie i przetwarzanie informacji. Trochę lepiej zdefiniowali problem Anglosasi. W USA mamy *computer science* – nauki komputerowe czy *information technology* – techniki informacyjne w skrócie określane jako IT czyli obecnie – technologia budowania zasobów wiedzy. Trzeba jednak pamiętać o słynnym zdaniu Vannevera Busha *„Wiedza nie polega na przechowywaniu informacji, lecz na umiejętności jej przetwarzania, powiązania ze sobą i przedstawiania w postaci która nadaje się do ogarnięcia dla pojedynczego umysłu…".* Współcześnie nastąpiła silna integracja dwu dominujących w zarządzaniu dziedzin **informatyki** i **telekomunikacji** (współczesna cyfrowa centrala telefoniczna jest niczym innym jak specjalizowanym komputerem, realizującym algorytm von Neumana – sterowanie programowe)

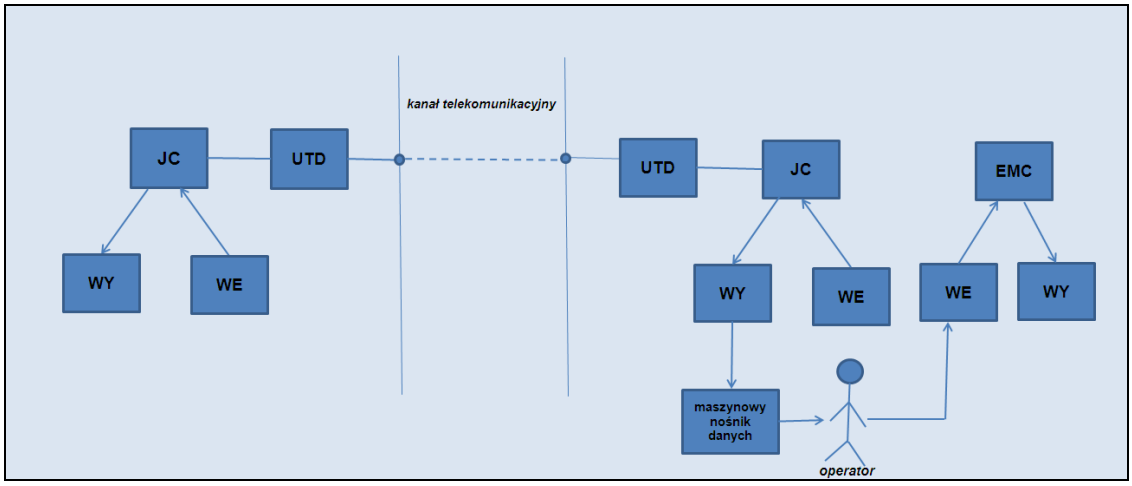
a technologie stosowane w produkcji urządzeń telekomunikacyjnych są takie same jak w produkcji komputerów (inny jest „środek ciężkości", komputer klasy DeskTop jest optymalizowany ze względu na cenę – nie może kosztować więcej niż 2000 zł, natomiast centrala jest optymalizowana ze względu na niezawodność – uszkodzenie 40% układów centrali nie może wyłączyć jej z ruchu, może pracować wolniej ale musi pracować a to przekłada się na cenę np. centrala Hicom 330 firmy Siemens (500 abonentów wewnętrznych i 90 linii zewnętrznych czyli nieduży system PABX to wydatek ponad 250 tys. zł.). Słynny slogan reklamowy firmy Sun Microsystems *„Sieć to dopiero komputer…".* Pojawiła się więc nowa jakość. Mówimy więc o nowej dziedzinie związanej z systemami przestrzennego przetwarzania jaką jest **teleinformatyka** znana również pod wywodzącym się z angielskiego akronimem **ICT** (*Information Communication Technology*).



Rys.1.4. *Technika ICM*

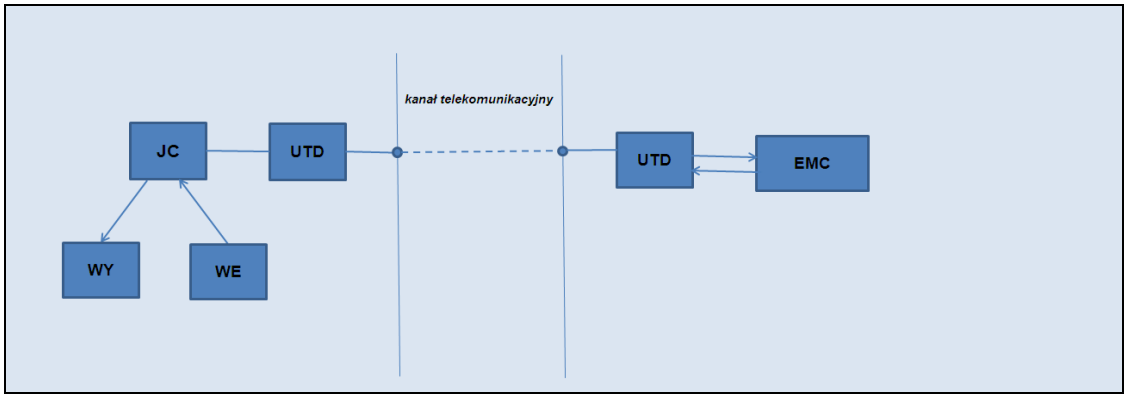
W tej nowej celowej działalności człowieka jakim jest teleinformatyka pojawił się problem przestrzennego przetwarzania danych. Znaczy to, że na geograficznie określonym terenie rozrzucone są zarówno stacje robocze jak i serwery połączone traktami telekomunikacyjnymi.

W zasadzie eksploatujemy dwa modele przestrzennego przetwarzania: system „off-line" i system „on-line" W systemie „off-line" pośrednim informacje przesyłane ze stacji roboczej do serwera (węzła) są zapisane na maszynowym nośniku danych (dyskietka, płytka CD-R) i za pośrednictwem operatora dostarczone do innego komputera (serwera czy Ośrodka Obliczeniowego), gdzie zostaną przetworzone. W tym przypadku do systemu przetwarzania włączony został najbardziej nieprzewidywalny, zawodny element jakim jest człowiek.



Rys.1.5. *System przestrzennego przetwarzania „off-line".*

Chcąc wyeliminować pośrednictwo operatora (człowieka) skonstruowano systemy „on-line" bezpośrednie (księgarnie Amazon, Merlin) w których zdalna stacja robocza łączy się bezpośrednio z serwerem.



Rys.1.6. *System przestrzennego przetwarzania „on-line”.*

Każdy z tych systemów ma określone ograniczenia np. kupując konkretną książkę

w Merlinie w systemie „on-line”, ale bez kodowego zabezpieczenia przed błędami, możemy otrzymać inną niż zamawiana książkę. Gdyby w takim systemie przekazywać dane do personifikacji dokumentów (paszporty, dowody osobiste) to ilość niepoprawnie wydrukowanych dokumentów byłaby duża. W takim przypadku lepszy okaże się system pośredni „off-line” w którym dane są zweryfikowane, zapisane np. na płytce CD-R i fizycznie ten nośnik danych przewieziony do Departamentu Personifikacji Dokumentów, a to ustrzeże przed błędnym wydrukiem dokumentów.

1.3. Pojęcie informacji

Pojęcie informacji, intuicyjnie oczywiste, nie jest wcale łatwe do zdefiniowania. Jak wiemy informatyka jest nauką o przetwarzaniu informacji zwłaszcza przy użyciu automatycznych środków pomocniczych. Pojawia się więc pojęcie informacji. Jak je zdefiniować pamiętając, że problem przesyłania i przetwarzania informacji jako dziedzina zainteresowań sięga bardzo dawnych czasów. Jednak w ciągu kilkudziesięciu lat problem ten pozostawał w cieniu problemów przesyłania i przetwarzania energii. Powstała cała dziedzina nauki traktująca o informacji, **teoria informacji.** Z punktu widzenia Teorii Organizacji i Kierowania (Zarządzania) **Informacją nazywamy wszystko to, co służy bardziej sprawnemu, bardziej celowemu działaniu**. Czyli w tym rozumieniu informacją mogą być np. pomiary, obserwacje, dane liczbowe, obrazy itp. To co jest informacją z punktu widzenia jednej celowej działalności człowieka z punktu widzenia innej celowej działalności może nie mieć takiego znaczenia. Jeśli na przykład, odbiorca informacji nie jest szyprem kutra rybackiego to

komunikat o stanie morza nie jest dla niego informacją; jeśli nie uprawiacie sportu szybowcowego to komunikat dla szybownictwa też nie jest dla Was informacją.

Z podanych przykładów i powyższej definicji informacji wynika, że taka definicja jest nieprecyzyjna i nie powinna mieć zastosowania w działaniach inżynierskich. Można więc pokusić się o inną definicję tego pojęcia. Według humanistów „królową nauk" jest filozofia, więc można sobie wyobrazić „filozoficzną" definicję informacji **Informacja jest to jeden z trzech składników obiektywnie istniejącej rzeczywistości (oprócz materii i energii).** Wiek XIX wiek zdobywania i przetwarzania materii; wiek XX a zwłaszcza jego pierwsza połowa to wiek wytwarzania i przesyłania energii; druga połowa XX wieku, od końca II Wojny Światowej i wiek XXI to wiek informacji. Obecnie dążymy do społeczeństwa informacyjnego i gospodarce opartej na wiedzy. Ta „filozoficzna" definicja informacji w zastosowaniach inżynierskich też okazała się niepraktyczna.

Aby zdefiniować pojęcie informacji jednoznacznie rozumiane w telekomunikacji, informatyce a zwłaszcza w teleinformatyce wymaga sprecyzowania pojęcia **procesu informacyjnego** czyli po co chcemy przekazywać informacje, co to nam da, ułatwi, usprawni. **Procesem informacyjnym nazywamy całokształt operacji przeprowadzonych nad informacjami w trakcie realizacji określonego zadania na przykład wypracowania decyzji.**

W procesie takim wyróżnia się 4 fazy:

1. Zbieranie informacji;
2. Przechowywanie informacji;
3. Przetwarzanie informacji;
4. Przesyłanie informacji.

Proces informacyjny jest procesem nadrzędnym w działalności każdego przedsiębiorstwa, instytucji czy organizacji. Od jego właściwego przebiegu zależy sukces firmy a poprawny, właściwy, spełniający współczesne wymagania (zwłaszcza teraz gdy mamy ciągle zmieniane normy prawne) jest niemożliwy bez szerokiego wprowadzenie do Systemów Zarządzania rozwiązań teleinformatycznych (głównie telekomunikacyjnych). Uwzględniając rolę jaką spełnia informacja w Systemach Zarządzania, A. Mazurkiewicz sformułował następującą definicję informacji: ***Informacją nazywamy wielkość abstrakcyjną, która może być przechowywana w pewnych obiektach, przesyłana między pewnymi obiektami, przetwarzana w pewnych obiektach i stosowana do sterowania pewnymi obiektami, przy czym przez***

obiekty rozumie się organizmy żywe, urządzenia techniczne oraz systemy takich obiektów.

W trakcie realizacji procesu informacyjnego informacje są w różnorodny sposób modyfikowane, zmienia się głownie forma informacji, jej ilość, użytkownik i miejsce jej wykorzystania. Na ogół są to informacje mające na celu podanie informacji w formie najbardziej przydatnej dla odbiorcy. Istotna rola przypada więc telekomunikacji. Przypomnijmy, że t**elekomunikacja -** jest to dziedzina wiedzy i działalności zajmująca się przekazywaniem na odległość informacji przeważnie za pomocą energii elektrycznej. Wiadomością w telekomunikacji są: mowa, muzyka, śpiew, znaki pisma, obrazy ruchome i nieruchome, wartości pomiarowe czy też dane cyfrowe. Ważnym jest żeby pamiętać, że telekomunikacja zajmuje się formą informacji oraz jej przekazywaniem w sposób możliwie wierny. Nie zajmuje się procesem powstawania informacji, jej treścią i sensem stąd w klasycznej teorii informacji mamy 8 faz procesu informacyjnego (1. generowania informacji, 2. gromadzenia informacji, 3. przechowywania informacji, 4. Transmisji informacji, 5. transformacji informacji, 6. udostępniania informacji, 7. interpretacji informacji, 8. wykorzystywania informacji) procesu a w telekomunikacji tylko, wymienione wcześniej cztery. Wyobraźmy sobie klasyczny system zarządzania (rys.1.7), istnieje obiekt zarządzany przez swoje kierownictwo. Do obiektu należy dostarczyć wszystkie niezbędne komponenty aby mógł wyprodukować konkretne wyroby, zaś kierownictwo i personel pomocniczy mając opracowane i przyjęte kryteria postępowania zbiera informacje zewnętrzne (otoczenie - liczność populacji, moda, możliwości zbytu i eksportu) oraz informacje wewnętrzne (stan obiektu) przetwarza je w decyzje – które również są informacjami (inna postać).

Z pojęciem informacji wiążą się jeszcze dwa dodatkowe terminy; **komunikat** i **wiadomość**. Komunikatem nazywamy więc zakodowaną wiadomość, zawierającą pewna ilość informacji. Z definicji komunikatu wynika, że jest **on** samoistnym bytem fizycznym (tekst pisany, modulowana fala elektromagnetyczna), podczas gdy **wiadomość traktujemy jako relację zachodzącą między nadawca i odbiorcą,** podkreślamy jednak ilościowy aspekt informacji tzn. że ogólną własnością komunikatów wyrażającą wiadomość jest posiadanie pewnej ilości informacji. Tą samą wiadomość można przekazać przy pomocy różnych komunikatów; „*Caius Julius Caesar*" i *„człowiek zasztyletowany przez senatorów na Forum Romanum w Idy Marcowe 44 p. n. e.",* DCC IX „ab urbe condita" mają to samo znaczenie (przekazują tą

samą wiadomość) mimo, że w tych dwu komunikatach nie powtarza się ani jedno słowo. Z drugiej strony ten sam komunikat (ten sam byt fizyczny) może przekazywać różne wiadomości dla różnych odbiorców; nadawane przez radio wspomniane już komunikaty *„dla szybownictwa”,* czy *„o stanie morza”* prawie nic nie mówią osobom nie wtajemniczonym, wiadomość o wszczęciu zbrojnego wystąpienia przeciwko rządowi republikańskiemu przekazali spiskowcy frankistowscy komunikatem „*nad Hiszpanią niebo jest czyste*”. Badaniem problemów ilości informacji, sposobów kodowania i przesyłania informacji zajmuje się teoria informacji stworzona przez Claude’a Shannona w latach 1948 – 1949. Podstawowe założenie ilościowej teorii informacji polega na tym, że komunikat zawiera tym więcej informacji im mniejsze jest prawdopodobieństwo jego wystąpienia. Przyjmuje się, że komunikat, którego prawdopodobieństwo wystąpienia czynności **p**, zawiera $\mathbf{k = \log_2 1/p = - lg_2 p,}$ jednostek ilości informacji.

Jeśli rozpatrywane źródło może nadawać tylko jeden komunikat, którego prawdopodobieństwo wynosi **1** to niesie on $\mathbf{lg_2(1/1) = lg_2 1 = 0}$ **[bitów informacji].** Jeśli źródło nadaje n różnych komunikatów odpowiednio z prawdopodobieństwami $p_1, p_2, \ldots, p_n$, to entropią informacyjną (w sensie Shannonowskim) jest średnia ważona ilość informacji w komunikatach z tego źródła:

$$H = \sum_{i=1}^{n} p_i \cdot \log_2 \quad \frac{1}{p_i} = -\sum_{i=1}^{n} p_i \lg_2 (p_i)$$

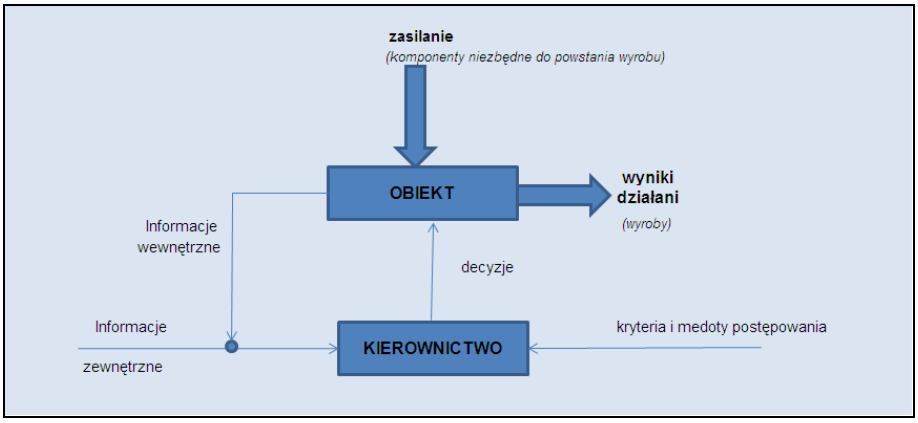
H - ilość informacji (w bitach);

n - ilość możliwych stanów nośnika informacji;

$\mathbf{p_i}$ – prawdopodobieństwo znalezienia się nośnika w i-tym stanie.

Generalnie więc entropia określa nasz stopień niewiedzy o źródle informacji. Im mniej o nim wiemy (źródle) tym entropia jest większa. Ma to duże znaczenie dla zapewnienia poufności przesyłanej informacji np. zastosowanie szyfru Cezara (przesunięcie stałe) nie zmienia cech statystycznych języka (w języku polskim 8,5% tekstu pisanego to litera A, pozostałe litery i ich złożenia też mają znaną częstość występowania) więc przechwytując zaszyfrowaną informację o której wiemy, że jest zapisana po polsku jej deszyfracja jest sprawą trywialnie prostą, najczęściej występującej literze szyfrogramu nadajemy znaczenie A kolejno pozostałe litery. Co innego gdy potrafimy tak zaszyfrować informację, że częstość występowania znaków

w szyfrogramie jest jednakowa dla wszystkich znaków alfabetu. Mówimy wtedy o szyfrowaniu idealnym.

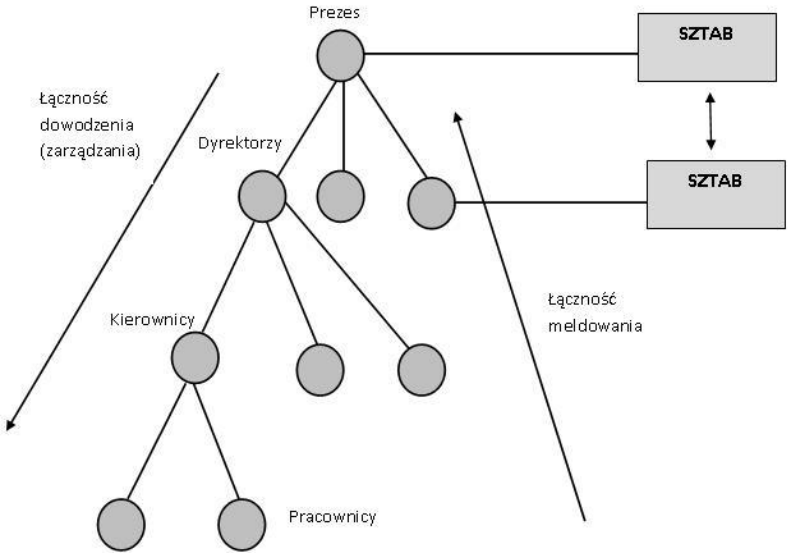


Rys.1.7. *Klasyczny system zarządzania*

W tym przypadku wymagania dla decydentów są bardzo wysokie (znajomość procesu produkcyjnego, umiejętność kierowania dużymi zespołami, właściwe przygotowanie ekonomiczne, umiejętność organizowania współpracy pomiędzy różnymi podmiotami gospodarczymi i wiele innych) powoduje to, że Szef aby to ogarnąć powinien być geniuszem a znanym faktem jest, że geniusze nie przeżywają „wieku chrystusowego" (matematycy Evariste Galois 21 lat, Niels Henrik Abel 27 lat; pisarz Michaił Lermontow 27 lat czy wreszcie największy Wódz starożytnego Świata Aleksander Macedoński przeżył 33 lata). Aby więc sprostać wymaganiom powołują w kierownictwie organy pomocnicze – sztaby których zadaniem jest przetwarzanie konkretnych informacji (zewnętrznych i wewnętrznych) w celu przygotowania dla decydenta projektów decyzji wstępnych. Zespoły tych sztabów w Firmie zaliczane są do tzw. Sfery nieproduktywnej (wydają a nie przysparzają pieniędzy Firmie). Prowadzi do najpopularniejszego hierarchicznego modelu zarządzania liniowo-sztabowego.

W takim modelu zarządzania oczekujemy, że wykorzystanie systemu wspomagania dowodzenia (zarządzania) SWD, w tym systemu telekomunikacyjnego zapewni wystarczającą przepływność, aby od najwyższego decydenta do szeregowego pracownika przekazać polecenia a w kierunku przeciwnym, od pracownika do decydenta, przekazać meldunki. Dla przeniesienia tego ruchu (traffiku) konstruowane są SWD. Dodatkowym problemem, niedocenianym w wielu firmach, instytucjach jest problem tzw. rozpiętości kierowania. Specjaliści od TOiK *(Teoria Organizacji i Kierowania)* udowodnili, że jeden decydent efektywnie może kierować co najwyżej

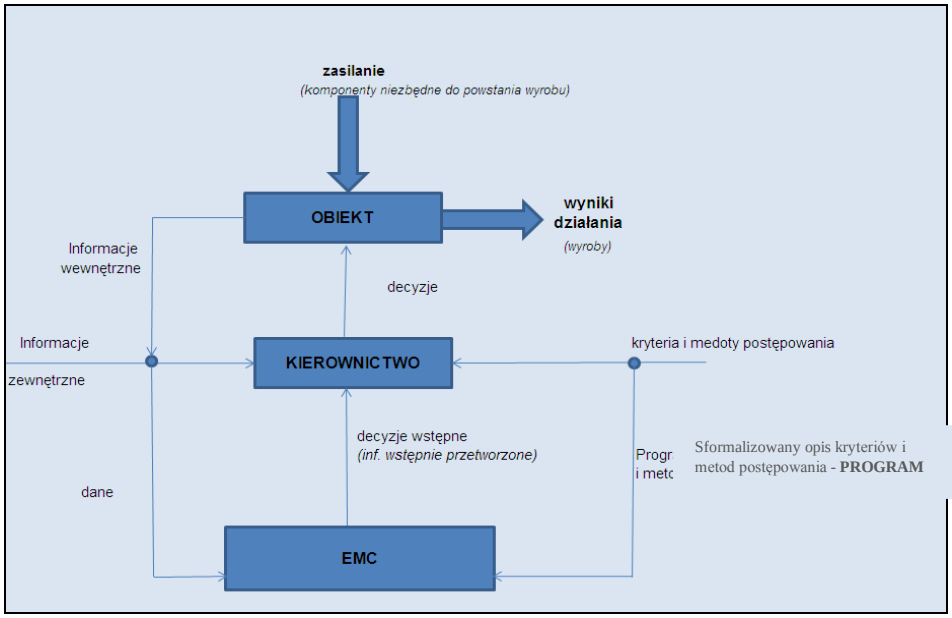
6 do 8 podwładnymi. Jeśli ma ich więcej to musi zaufać współpracownikom i część swoich uprawnień powinien na nich scedować.



Rys.1.8. *Hierarchiczny, liniowo – sztabowy model zarządzania*

Ruch telekomunikacyjny (traffik) góra – dół to łączność dowodzenia (zarządzania); ruch o kierunku odwrotnym (dół – góra) to łączność meldowania. Są to główne strumienie przepływu informacji w systemie zarządzania (dla zapewnienia tego określamy i budujemy systemy telekomunikacyjne). Ruch generowany przez sztaby, nie związany bezpośrednio ze strukturą zarządzania firmy (instytucji) to ruch zakłócający.

Ważnym jest aby racjonalizować wielkość sfery nieproduktywnej w trosce o kondycję finansową całego przedsiębiorstwa. W tym celu można wykorzystać nowe technologie informacyjne (Elektroniczne Maszyny Cyfrowe) dla przetwarzania najbardziej pracochłonnych, żmudnych, ale dających się zalgorytmizować, operacji w trakcie przetwarzania informacji w celu przygotowania projektów decyzji. Pamiętać jednak trzeba, że wdrażanie technik komputerowych w początkowym okresie nie przynosi oszczędności (konieczność prowadzenia „buchalterii" zarówno tradycyjnej jak i z wykorzystaniem komputera - zwiększa koszty, niechęć personelu do wprowadzania nowych rozwiązań i konieczność prowadzenia szkoleń zwiększają koszty prowadzenia działalności).



Rys.1.9. *System Zarządzania z użyciem komputera (metod i środków informatyki).*

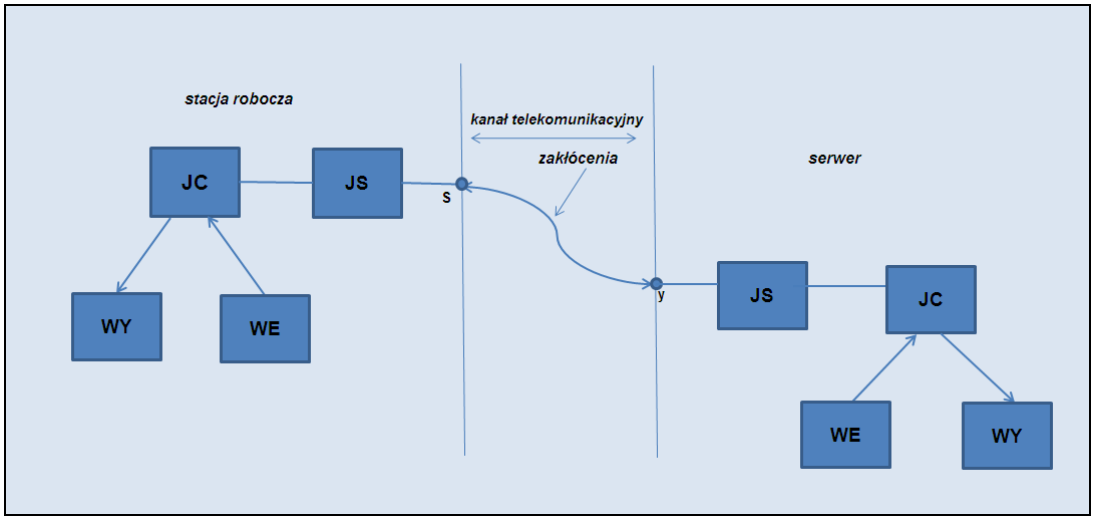
W takim przypadku mamy podział zadań w zakresie przetwarzania informacji. Część z nich jest wykonywana przez kierownictwo i personel pomocniczy, natomiast najbardziej pracochłonne czynności informacyjne (przetwarzania) wykonuje komputer na podstawie **programu będącego sformalizowaną reprezentacją kryteriów i metod postępowania** oraz wprowadzonych do tego programu **danych** (odpowiednio „zapisane" informacje zewnętrzne i wewnętrzne). Decyzje podejmowane są na podstawie informacji przetworzonych przez komputer oraz z informacji przetworzonych w sposób klasyczny.

Zakup komputera klasy serwer jest dużą inwestycją (niezależnie od czasu w którym dokonujemy tego zakupu) a którego okres amortyzacji, znacząco się skrócił (od średnio 5 lat w latach osiemdziesiątych ubiegłego wieku do 2 lat obecnie) więc pojawia się dodatkowy problem zwiększenia stopnia amortyzacji poczynionej inwestycji. W celu zwiększenia amortyzacji sprzętu informatycznego należy zrezygnować z tzw. **lokalnego (podstawowego) trybu pracy** – użytkownik ma możliwość wyłącznego dysponowania wszystkimi zasobami sprzętowymi to jest procesorem, pamięcią operacyjną i zewnętrzną oraz urządzeniami WE/WY. Komunikacja poprzez konsolę operatorską (uniemożliwia dobre wykorzystanie zasobów sprzętowych, a w szczególności powolne operacje WE/WY powodują stratę czasu drogiego procesora. Pewnym rozwiązaniem może być **przetwarzanie wsadowe** – wielozadaniowy system operacyjny poszerzony o moduł zarządzania wykonywaniem

programów może przyjąć polecenia wykonywania grupy programów, czyli udostępnienie naszych zasobów innym użytkownikom, płacą wtedy za korzystanie z naszej infrastruktury ale nie muszą inwestować w rozbudowę własnych Ośrodków Obliczeniowych (oczywiście w danej chwili procesor wykonuje tylko 1 program). Efektem ubocznym jest to, że użytkownik zostaje pozbawiony kontaktu ze sprzętem. Otrzymuje tylko wyniki działania programu (nanosi ewentualne poprawki i ponownie czeka na przetworzenie). Z tego powodu ten tryb pracy komputera jest rzadko stosowany. Wydaje się, że najlepszym rozwiązaniem jest stosowanie **wielodostępu** – istotą tego trybu pracy jest przekazywanie uprawnień do uruchamiania i przetwarzania programów, poprzednio przypisanego tylko operatorowi (dokładnie jednej konsoli operatora) również innym urządzeniem WE/WY nazwanych terminalami, które zostały wprost udostępnione użytkownikom (stacje robocze). Musiano wprowadzić tzw. podział czasu pracy procesora tzn. przełączania go w krótkich odcinkach czasu np. 1/50 sek. na realizację kolejnych programów tak, aby każdy z nich był przetwarzany na bieżąco.

Oczywistym jest fakt, że wielu użytkowników może pracować na wspólnych ciągle aktualizowanych bazach danych (systemy bankowe czy kasowe). Tryb ten umożliwia również zdalny dostęp przez łącza dzierżawione lub komutowane z wykorzystanie modemów. Kłopoty – różne komputery wymagają różnych typów terminali. Problem może rozwiązać poprzez zbudowanie **sieci komputerowych** (teleinformatycznych). Komputery są sprzężone miedzy sobą łączami umożliwiającymi przesyłanie informacji (danych) między dowolną parę komputerów, co nie oznacza konieczności połączeń każdy z każdym, przeciwnie wymianie danych między komputerami A i B mogą pośredniczyć komputery C i D. Terminal użytkownika jest dołączony na stałe, co prawda do jednego najbliższego komputera, ale przez ten terminal można korzystać z zasobów sprzętowych i programowych dowolnego włączonego w sieć komputera. Takie rozwiązanie wymaga dodatkowych zabiegów, związanym z zapewnieniem praktycznej bezbłędności przekazywanych informacji.

Należy przy tym pamiętać, że systemy łączności budowane były na potrzeby wymiany informacji w systemie „człowiek – człowiek” to znaczy, że źródłem i ujściem informacji była istota ludzka zdolna do abstrakcyjnego myślenia i wnioskowania. Niedostatki przekazu mogły być poprawione przez doświadczenie i intelekt rozmówców.



Rys.1.10. *Struktura przestrzennego przetwarzania z wykorzystaniem kanału telekomunikacyjnego mogącego wnosić błędy.*

Włączenie do systemu informacyjnego komputera powoduje, że informacja może również być nadawana i odbierana poprzez urządzenia techniczne czyli w systemie „człowiek – EMC" lub „EMC - EMC". W takim przypadku pojawia się problem. Sygnał odebrany **y(x)** nie jest tożsamy z sygnałem nadanym **s(x)** czyli **y(x)** ≠ **s**(x)**;** w najlepszym przypadku, jeśli zakłócenia w łączu miały charakter addytywny to **y(x) = s(x) + z(x)**. Jeśli zakłócenia mają charakter multiplikatywny (składowe sygnału **s(x)** wymnażają się ze składowymi zakłóceń **z(x)**) to nie ma analitycznej metody rozwiązania takiego przypadku. Trzeba stosować metody symulacji kanału transmisyjnego w oparciu o syntetyczne wskaźniki jakości transmisji. W takich systemach wymagane jest zestawienie specjalnych szerokopasmowych, zapewniających bezbłędną transmisję traktów teletransmisyjnych. Przekracza to możliwości inwestycyjne wielu państw, nie mówiąc o inwestorach prywatnych. (w kosztach przestrzennego przetwarzania 20% to koszt sprzętu i oprogramowania informatycznego a 80% to koszt łączy i wyposażenia telekomunikacyjnego). W związku z tym w współczesnych systemach przestrzennego przetwarzania wykorzystujemy łącza z systemu „czł – czł" uzupełnione o dodatkowe urządzenia nazywane **urządzeniami transmisji danych** (lub teledacyjnymi). Generalnie zadaniem UTD jest taka zmiana sygnału niosącego informację po stronie nadawczej tak, aby po stronie odbiorczej móc stwierdzić czy w trakcie transmisji wystąpił błąd czy nie i podjąć właściwe działanie.

1.4. Pojęcie błędu

Pod pojęciem błędu rozumiemy różnice w stanach znamiennych sygnału nadanego i odebranego. Komunikat *„ala ma kota”* w **kodzie telegraficznym nr 2** zapiszemy;

N ...11000 01001 11000 00100 00111 11000 00100 11110 00011 00001 11000….

O …11001 01000 11000 00101 00111 11001 00100 11010 00011 10011 11000….

ciąg błędów …00001 00001 00000 00001 00000 00001 00000 00100 00000 10010 00000….

W powyższym przykładzie wystąpiło 7 błędów. Charakter (jakość) łącza określa nam parametr znany jako ESB (elementowa stopa błędów). Jest to wskaźnik syntetyczny, gdyż definiuje wpływ wszystkich czynników które spowodowały błędy. Jest to stosunek elementów błędnie odebranych do ogólnej liczby elementów nadanych.

$$ESB = \frac{il.el.bł.odebranych}{og.il.el.nadanych}$$

Czyli w naszym przykładzie jest to 7/55. Proszę zwrócić uwagę, że powyższym przykładzie wystąpiło 7 błędów, ale przekłamane zostało 6 znaków a dla użytkownika (abonenta) najmniejszą rozpoznawaną cząstką informacji jest znak, to możemy zdefiniować inny syntetyczny wskaźnik jakości transmisji jakim jest ZSB (znakowa stopa błędów) definiowana jako stosunek ilości znaków błędnie odebranych do ogólnej ilości znaków nadanych,

$$ZSB = \frac{il.zn.bł.odebranych}{og.il.zn.nadanych}$$

czyli w naszym przykładzie będzie to 6/11. Przytoczony w przykładzie międzynarodowy kod nr 2 jest przykładem kodu oszczędnego tzn. wszystkie możliwe do utworzenia kombinacje zostały wykorzystane do zakodowania znaków alfabetu (litery, cyfry, inne znaki które chcemy zastosować). Liczbę możliwych do utworzenia kombinacji określa wzór; $\mathbf{K = W^D}$ gdzie W jest wartościowością kodu a D jego długością. W naszym przypadku $K = 2^5 = 32$, co daje 32 kombinacje. Przypisując dwu z nich znaczenie *„litery”* i *„cyfry”* (podwójne wykorzystanie pozostałych kombinacji) jesteśmy w stanie zakodować wszystkie znaki alfabetu wykorzystywane w łączności telegraficznej. Taki kod nie ma żadnych możliwości wykrycia błędu. Nadaliśmy literę A – 11000, na skutek przekłamań w łączu odebraliśmy kombinację 11010, co odbiornik zinterpretuje, że nadano literę J. Zarówno A i J są ciągami kodowymi, więc będzie to

przypadek błędu niewykrytego przez kod. Jeżeli wydłużymy ciąg kodowy o jeden bit tak aby liczba jedynek w całym ciągu była parzysta to co prawda zmniejszymy szybkość przekazywanych danych o 20% ale za to zyskamy możliwość wykrycia błędu. Pamiętamy A - 11000|0 (pozycja 6 to bit parzystości) a odebrano 11010|0 to odbiornik (dekoder) nie podejmie decyzji, że nadano J ale stwierdzi, że wystąpił błąd (nie wiadomo na której pozycji) i może zażądać powtórnego przesłania informacji. Jest to przypadek kodu detekcyjnego. W praktycznie stosowanych systemach transmisji danych nie stosujemy transmisji znakowych. Jedyny w świecie system pracujący w tym trybie to „gorąca linia" Moskwa – Waszyngton pracująca w oparciu o algorytm TOR *(Teleprining Over the Radio)* van Durena z 1958 roku. Pozostałe systemy stosują transmisje blokowe (pewna liczba znaków wspólnie objęta zabezpieczeniem przed błędami). Zastosujmy dwukrotnie kontrolę parzystości, poprzeczną i podłużną;

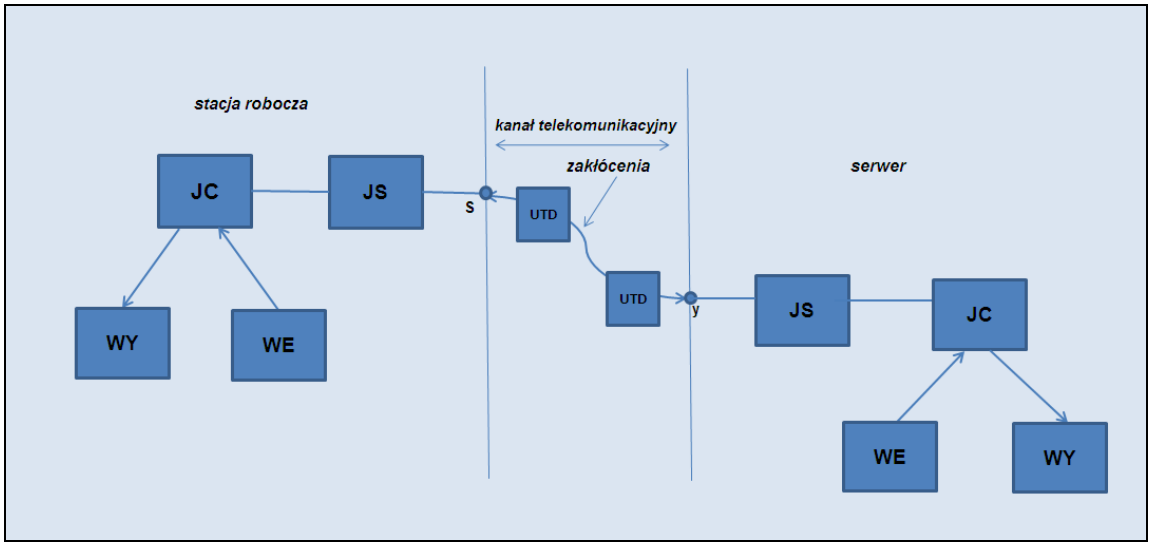
	Nadajnik			Odbiornik	
	→ parzystość poprzeczna			→ parzystość poprzeczna	
p		A	11000|0	p	11010|0
o				o	
d		L	01001|0	d	01001|0
ł				ł	
u		A	11000|0	u	11000|0
ż				ż	
n		-	00100|1	n	00100|1
a		M	00111|1	a	00111|1
			01010|0		01010|1

Z sprawdzenia parzystości po stronie odbiorczej wynika, że błąd jest w pierwszym wierszu i w czwartej kolumnie, więc wystarczy zamienić odebraną 1 na 0 (kod binarny) aby nie tylko wykryć ale również skorygować błąd. Okupione to zostało dużym zmniejszeniem szybkości transmisji, zamiast przesłania 25 bitów informacji trzeba przesłać 36 bitów (25 informacyjnych i 11 dodatkowych kontrolnych (nadmiarowych)). Z praktyki wiadomo, że w kanałach radiowych opłaca się korygować tylko błędy pojedyńcze. Błędy o większych krotnościach wymagają tak dużego nadmiaru kontrolnego, że szybkość transmisji danych użytkownika spada poniżej akceptowanej wielkości. Jest to przykład kodu korekcyjnego. W związku z transmisjami blokowymi pojawia się kolejny syntetyczny wskaźnik jakości transmisji, blokowa stopa

błędów BSB jest to stosunek bloków błędnie odebranych do ogólnej ilości bloków nadanych.

$$BSB = \frac{il.bloków\,bł.odebranych}{og.il.bloków nadanych}$$

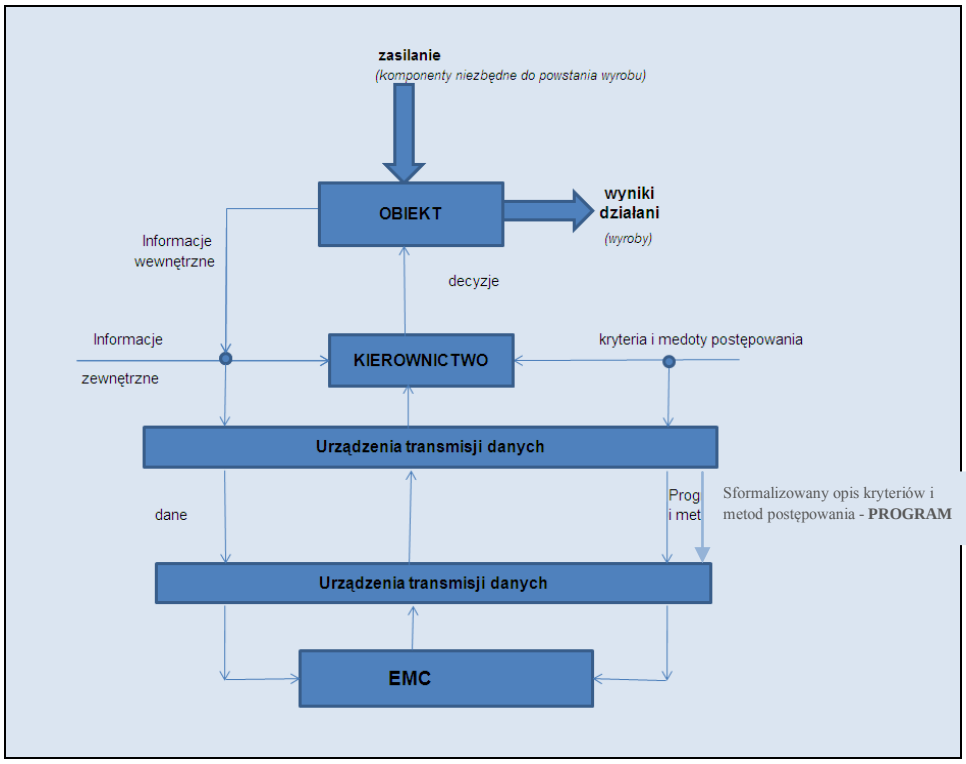
Te trzy wskaźniki (ESB, ZSB, BSB) charakteryzują jakość łączy Transmisji Danych. ESB mówi jaka jest jakość kanału podkładowego na którym chcemy zbudować system TD (dla kanału telefonicznego jest wielkość rzędu 10^{-3} dla łączy telegraficznych rzędu 10^{-5}). ZSB określa użytkownikowi ile błędnych znaków może wystąpić w otrzymanej korespondencji a BSB charakteryzuje cały system TD, jakie jest prawdopodobieństwo błędnej decyzji ostatecznej. Może to być wskaźnik pozwalający oceniać sprzęt różnych producentów. Zarówno kody detekcyjne jaki korekcyjne należą do grupy kodów nadmiarowych - liczba możliwych do utworzenia kombinacji jest większa niż liczba znaków alfabetu które należy zakodować. W praktyce stosuje się bardziej złożone kody np. kody cykliczne BCH, liniowe Reeda - Salomona czy inne dobrane do wagowego widma błędów łącza Transmisji Danych. Praktyczne realizacje kodowego zabezpieczenia przed błędami realizują, wspomniane już, urządzenia transmisji danych UTD. Miejsce ich włączenia w trakt teletransmisyjny przedstawia rysunek 1.10.



Rys.1.10. *Miejsce UTD w systemie przestrzennego przetwarzania*

a omawiany wcześniej system przestrzenny system zarządzania rys. 1.11. Oznacza to po prostu, że UTD o ustalonych algorytmach współpracy należy włączyć zarówno po

stronie terminala (stacji roboczej) jak i po stronie serwera. Z syntetycznymi wskaźnikami jakości transmisji wiążą się przejęte z amerykańskiego terminy BER *(Binary Error Ratio)* tłumaczone jako bitowa stopa błędów, oraz EER *(Estimate Error Ratio)* tłumaczone jako szacowana stopa błędów. Należy pamiętać, że oba te wskaźniki to nic innego jak nasza ESB – elementowa stopa błędów. Ale BER to jest konkretna, zmierzona wielkość statystyczna dla danego łącza, jeśli zaś badaliśmy dużą liczbę łączy tego samego typu to wówczas statystyka nabiera charakteru prawdopodobieństwa i mówimy wtedy nie o BER a o EER czyli, że prawdopodobieństwo wystąpienia błędu w łączach tego typu wynosi **p**.



Rys.1.11. *Przestrzenny System Zarządzania z włączonymi urządzeniami UTD*

2. Kryteria kwalifikacyjne i podział telekomunikacji

2.1. Kryteria kwalifikacyjne

Jak w każdej celowej dziedzinie działalności aby dokonać porównań, ocen obszaru działalności należy sformułować pewne kryteria kwalifikacyjne.

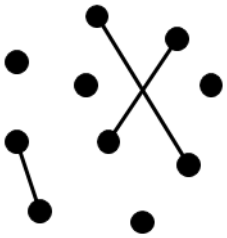
W telekomunikacji przyjęto trzy podstawowe:

1. Przeznaczenia,
2. Rodzaju przesyłanych informacji,
3. Procesów zachodzących w trakcie przesyłania informacji.

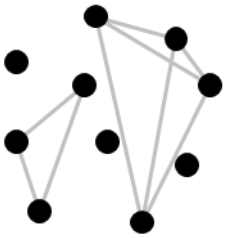
2.2. Podział telekomunikacji

W zależności od przeznaczenia albo celu przekazywania informacji, rozróżnia się:

a) **Telekomunikację porozumiewawczą**, utrzymującą łączność między dwoma albo wieloma punktami. W obu przypadkach łączność może mieć charakter stały (sieć stała), albo punkty mogą być wybierane spośród pewnej liczby punktów sieci komutowanej.

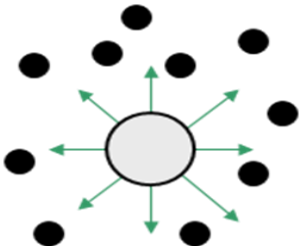


typu: punkt – punkt

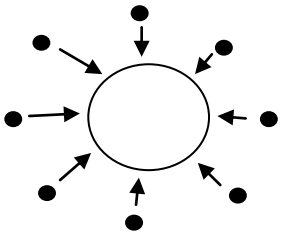


typu: wiele punktów

b) Telekomunikację rozsiewczą (rozgłoszeniową), rozpowszechniającą informację w jednym kierunku od punktu nadawczego do dużej liczby punktów odbiorczych. Telekomunikacja rozsiewcza (dyfuzyjna) typu punkt – wiele punktów, np.: radiofonia, telewizja



c) Telekomunikację zbiorczą, jednokierunkową zbierającą w jednym punkcie informacje przechodzące z wielu punktów (telekomunikacja zbiorcza typu wiele punktów nadawczych – jeden punkt zbiorczy).



Ze względu na rodzaj przesyłanych wiadomości telekomunikację dzielimy na:

1) telefonię – przekazywanie mowy,

2) radiofonię – przekazywanie dźwięku i muzyki,
3) telegrafię – przekazywanie znaków pisma,
4) symilografię (telekopię, faksymilografię) – przekazywanie obrazów nieruchomych,
5) telewizję – przekazywanie obrazów ruchomych i skojarzonych z nimi dźwięków,
6) telemetrię – przekazywanie danych pomiarowych,
7) sygnalizację – przekazywanie sygnałów umownych,
8) telemechanikę – przekazywanie impulsów sterujących
9) teledację (transmisję danych) – przekazywanie danych cyfrowych.

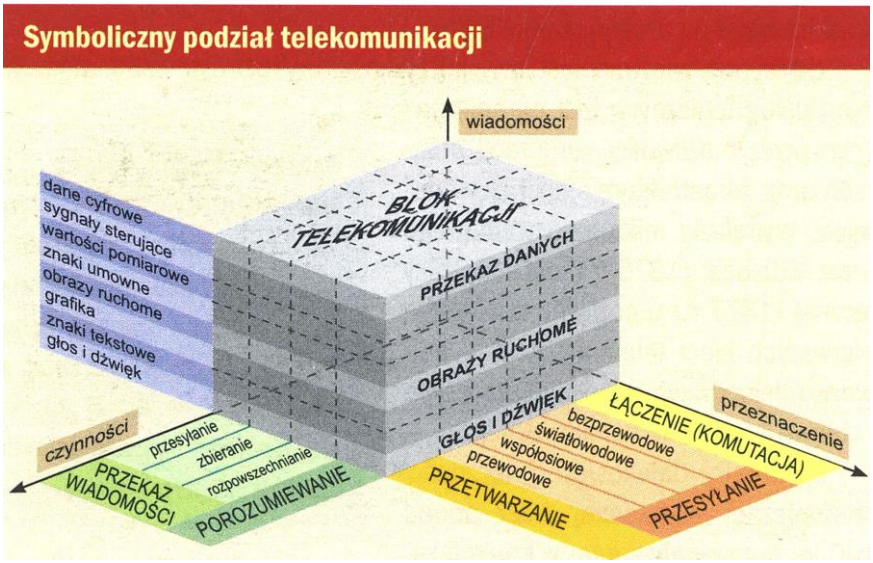
Generalnie ten podział nie budzi wątpliwości z wyjątkiem, być może, odróżnienia telefonii i radiofonii. Telefonia gałąź telekomunikacji zajmująca się przekazywaniem tylko sygnału mowy, czyli ograniczonego pasma częstotliwości od 300 Hz do 3400 Hz, wystarczającego do zapewnienia właściwej zrozumiałości odtworzonego sygnału (bez możliwości oceny stanu emocjonalnego osoby mówiącej). Od radiofonii oczkujemy czegoś więcej – możliwości odbioru „wrażeń artystycznych" np. emocji, poprawnego zaśpiewania „górnego C", czyli pasmo przenoszonych przez systemy radiofoniczne częstotliwości jest szersze niż w sieciach telefonicznych, na ogół od 50 Hz do 10 kHz (czasem do 15 kHz).

Ze względu na procesy zachodzące w trakcie przekazywania informacji telekomunikację dzielimy na:

1. **Technikę przetwarzania** zajmuje się urządzeniami służącymi do przetwarzania informacji na sygnał i odwrotnie; aparat telefoniczny, telegraf, skanery itp.
2. **Technikę przesyłania czyli teletransmisję** (przewodowa, radiowa, światłowodowa, podczerwień), zajmuje się zagadnieniem przesyłania sygnałów (elektrycznych, optycznych) od punktu do punktu sieci telekomunikacyjnej,
3. **Technikę komutacji** – komutacja, zajmuje się zestawianiem i rozłączaniem łączy czyli elementów drogi przesyłowej sygnałów w celu dokonania czasowego połączenia między żądanymi punktami sieci telefonicznej, telegraficznej, obejmuje projektowanie, wytwarzanie, instalację i eksploatację urządzeń telekomunikacyjnych oraz zagadnieniem ruchu w sieciach telekomunikacyjnych.

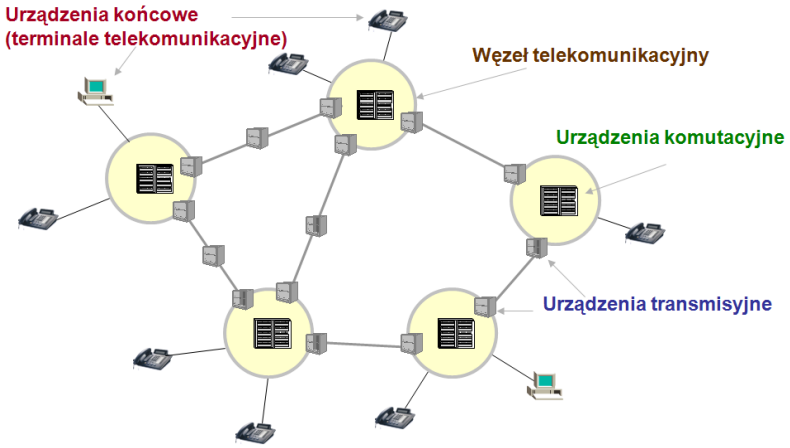
Sieć telekomunikacyjna - funkcjonalna całość przeznaczona do świadczenia usług telekomunikacyjnych umożliwiająca korzystanie z usług telekomunikacyjnych (*telefonia, telegrafia, telekopia, teledacja i innych*). Rozróżnia się sieci telekomunikacyjne ***powszechnego użytku*** przeznaczone dla ogółu użytkowników i sieci

specjalne (np. sieci resortowe MON i MSWiA, kolejnictwo, energetyka). Sieci powszechnego użytku różnych krajów są ze sobą powiązane tworząc ***sieć międzynarodową kontynentalną,*** a sieci kontynentalne – ***sieć światową***. Przekazywanie informacji za pomocą sieci nazywane są ruchem (telefonicznym, telegraficznym). Symboliczny podział telekomunikacji ze względu na omówione kryteria przedstawia rysunek 2.1.



Rys.2.1 *Symboliczny podział telekomunikacji*

Poglądowe przedstawienie sieci telekomunikacyjnej, czyli połączenia urządzeń końcowych (terminali), urządzeń teletransmisyjnych, urządzeń komutacyjnych i węzłów przedstawia rysunek 2.2.



Rys.2.2. *Sieć telekomunikacyjna*

2.3. Media transmisyjne

W telekomunikacji stosuje się kanały przestrzenne, częstotliwościowe, czasowe oraz kanały kombinowane przestrzenno – częstotliwościowe i przestrzenno – czasowe.

Kanały przestrzenne – są tworzone za pomocą torów telekomunikacyjnych przewodowych symetrycznych (napowietrznych lub kablowych, falowodowych lub radiowych).

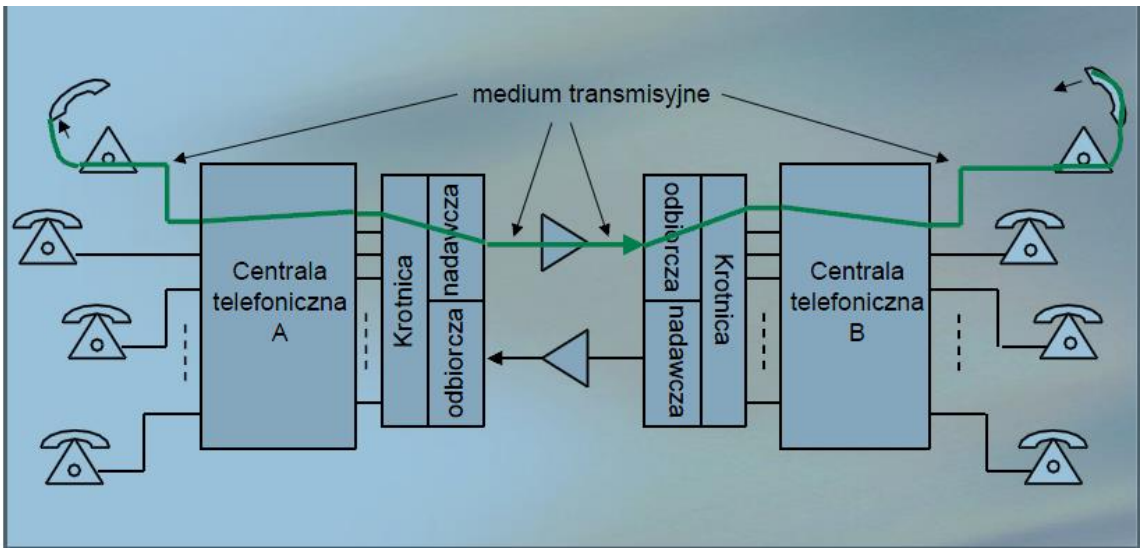
Kanałem telekomunikacyjnym częstotliwościowym nazywa się kanał telekomunikacyjny, w którym energia sygnału jest zawarta wewnątrz ograniczonego pasma częstotliwości.

Kanałem telekomunikacyjnym czasowym – nazywa się kanał ograniczony pod względem czasu do określonych przedziałów czasowych. Istnieją dwa odmienne sposoby przesyłania dowolnej informacji przez łącza telekomunikacyjne

- ***transmisja analogowa,***
- ***transmisja cyfrowa.***

Transmisja analogowa oznacza, że są przesyłane sygnały o ciągłym widmie częstotliwościowym, takim jak głos, dźwięk lub światło.

Transmisja cyfrowa oznacza, że przesyłany jest sygnał w postaci ciągu impulsów o ustalonej liczbie stanów. ***Sygnał*** **-** wielkość fizyczna, której pewne parametry są nośnikami informacji.



Rys.2.3. *Przykład kanału telekomunikacyjnego*

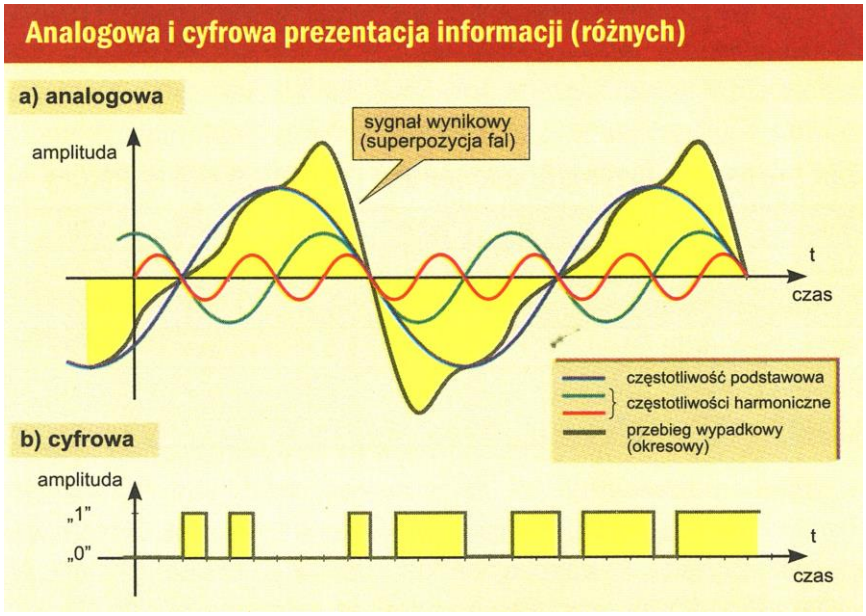
W telekomunikacji stosujemy sygnały ***analogowe*** lub ***cyfrowe***.

Sygnał analogowy, sygnał jako element ciągłego zbioru sygnału, w którym parametr informacji może w dowolnym czasie przyjmować dowolne wartości z dozwolonego przedziału zmian wartości.

Sygnał dyskretny (ziarnisty, cyfrowy), sygnał jako element dyskretnego zbioru sygnałów, w którym parametr informacji może przyjmować ograniczoną liczbę wartości, czyli w dowolnym czasie może przyjąć jedną i tylko jedną wartość z ściśle zdefiniowanego zbioru wartości. Sygnały dyskretne dzielimy na próbkowane, kwantowane i kodowane, czyli cyfrowe. Przepływność torów teletransmisyjnych (do niedawna oznaczana jako przepustowość kanału) zależy od typu łączy.

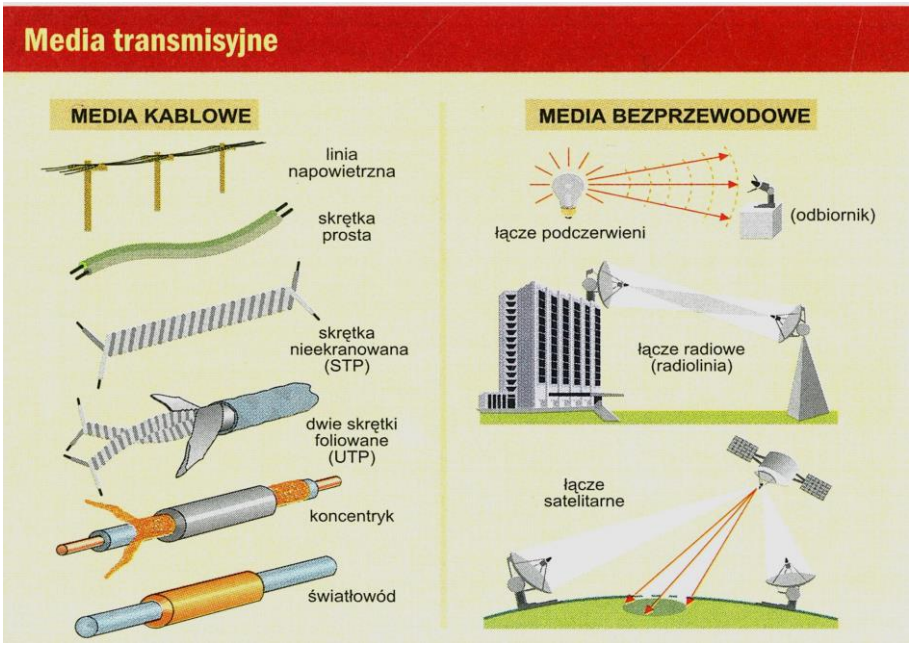
Łącza do transmisji cyfrowej są projektowane na określoną ***szybkość*** przesyłania wyrażoną w bitach na sekundę (b/s). ***Przepływność kanału*** (przepływność binarna) - zdolność kanału do przenoszenia informacji binarnej (ile bitów danych można przesłać w ciągu jednej sekundy) przez konkretne medium transmisyjne.

Przydatność łącza analogowego do pracy z różnymi szybkościami jest charakteryzowana szerokością pasma kanału. ***Szerokość pasma*** jest to różnica między górną a dolną częstotliwością pasma, które kanał jest zdolny przenieść z nierównomiernością nie gorszą niż 3 dB. Szerokość pasma jest wyrażona w hercach (Hz, kHz, MHz, GHz, THz), dla linii telefonicznej wynosi około 3,1 kHz w naturalnym paśmie częstotliwości od 300 do 3400 Hz (od 200 do 3500 Hz w niektórych aplikacjach).



Rys.2.4. *Prezentacja informacji sygnałami a) analogowymi b) dyskretnymi*

Generalnie media transmisyjne dzielimy na dwie grupy; kablowe i bezprzewodowe. Do mediów kablowych należą: linie napowietrzne, skrętki proste, skrętki nieekranowane (STP), skrętki ekranowane (UTP), kable koncentryczne i kable światłowodowe. Do mediów bezprzewodowych zaliczmy: łącza podczerwieni (IrDA), łącza radiowe (radioliniowe) i łącza satelitarne.



Rys.2.5. *Różne rodzaje mediów transmisyjnych*

Linia telefoniczna. Jest to najstarsze i najprostsze medium transportowe. Składa się ona z przewodów miedzianych w izolacji (kabel prosty), linii kablowych (skrętka) i linii napowietrznych. Pomimo wielu wad nadal są stosowane w telekomunikacji kable proste w postaci dwóch przewodów, wiązek lub płaskich taśm, najczęściej używanych do połączenia urządzeń peryferyjnych z interfejsem szeregowym (do 15 – 25 m) lub prostym równoległym na odległość do 2 m. Podstawowy, zasadniczy wpływ na maksymalną długość kabla telekomunikacyjnego i częstotliwość graniczną pracy łącza mają: średnica przewodów miedzianych, odległość między przewodami, rodzaj dielektryka, technologia skręcania przewodów, wzajemna symetria przewodów, jednorodność wykonania kabla, przyjęta asymetria w stosunku do ziemi oraz metoda nadawania i odbioru (napięciowa, prądowa, symetryczna, różnicowa czy inna).

Skrętka nieekranowana. Kabel typu skrętka UTP *(Unshielded Twisted Pair),* wykonany ze skręconych nieekranowanych przewodów, tworzy linię zrównoważoną (symetryczną). Skręcenie przewodów ze splotem 1 zwój na 6 – 10 cm chroni transmisję przed oddziaływaniem (interferencją) otoczenia. Skrętka jest powszechnie stosowana w sieciach telefonicznych i komputerowych – przy czym istnieją różne technologie

splotu przewodów, a poszczególne skrętki w kablu mogą mieć inny skręt (minimalizacja przesłuchów). Technologie te są opatentowane lub są tajemnicą producentów kabli. Przy przesyłaniu sygnałów cyfrowych za pomocą skrętki UTP uzyskuje się przepływności do 100 Mb/s (kategoria 5) a w najnowszej technologii Gigabit Ethernet 1000 Mb/s.

Skrętka foliowana FTP. Skrętka foliowana FTP *(Foiled Twisted Pair)* jest skrętką ekranowaną za pomocą folii, z przewodem uziemiającym i przeznaczoną głównie do budowy sieci komputerowych (Ethernet, Token Ring) o długości nawet kilka kilometrów.

Skrętka ekranowana STP. Skrętka ekranowana STP *(Shielded Twisted Pair)* różni się od skrętki FTP ekranem wykonanym w postaci oplotu i zewnętrznej koszulki ochronnej. Znaczenie skrętki ekranowanej wzrasta w świetle nowych europejskich norm kompatybilności elektromagnetycznej w zakresie emisji EMI *(ElectroMagnetic Interference)* – ograniczających promieniowanie dla nieekranowanych kabli telekomunikacyjnych przy wyższych częstotliwościach pracy.

Kable telekomunikacyjne. W kablach miedzianych wyróżnia się łącza niesymetryczne (co najmniej 1 biegun połączony z ziemią) i symetryczne, w których prąd w obu przewodach powinien być taki sam, lecz płynący w przeciwnych kierunkach (symetrycznie). Tak skręcona para daje dużą odporność na zakłócenia zewnętrzne. Pierwsze kable telekomunikacyjne miały papierowo – powietrzną izolację żył miedzianych, a powłokę zewnętrzną wykonaną z ołowiu. Takie kable obecnie nie są już produkowane, ale wciąż licznie jeszcze używane. Obecnie jako izolacji żył przewodzących używamy polichlorku winylu (PCW) lub polietylenu. Zasadniczym elementem kabla miedzianego jest para izolowanych przewodów skręconych ze sobą w celu uzyskania symetrii w stosunku do innych par i potencjału ziemi (eliminacja przesłuchów). Kable miedziane w specyfikacji EIA/TIA zostały podzielone na kilka grup (kategorii), w których przydatność do transmisji określa się w MHz:

- kategoria 1 – tradycyjna nieekranowana skrętka telefoniczna przeznaczona do transmisji głosu, nie przystosowana do transmisji danych;
- kategoria 2 – skrętka nieekranowana, szybkość transmisji do 4 MHz. Kabel ma 2 pary skręconych przewodów;
- kategoria 3 – skrętka o szybkości transmisji do 10 MHz, stosowana w sieciach Token Ring (4 Mb/s) oraz Ethernet 10BaseT (10 Mb/s). Kabel zawiera zwykle 4 pary skręconych przewodów;

- kategoria 4 – skrętka działająca z szybkością do 16 MHz, najniższa kategoria kabli nadających się do sieci Token Ring. Kabel jest zbudowany z 4 par przewodów.
- kategoria 5 – (klasa D) – skrętka z dopasowaniem rezystancyjnym 100 W, pozwalająca na transmisję danych z szybkością 100 Mb/s (pod warunkiem poprawnie wykonanej instalacji kabla, zgodnie z wymaganiami okablowania strukturalnego) na odległość 100 metrów. Przy zastosowaniu komponentów kategorii 5 i długości kabla 160 m uzyskuje się połączenie klasy C (16 MHz), na odległość do 250 m są to połączenia klasy B (1 MHz), natomiast w zasięgu do 3 km uzyskuje się transmisje klasy A (100 kHz). Kable tej kategorii są stale ulepszane (materiały, złącza, technologie wykonania, nowe metody dostępu), dzięki czemu jest już osiągana przepływność 1 Gb/s na odległość do 100 metrów (Gigabit Ethernet 1000 Mb/s). Niedawno organizacje standaryzacyjne ISO/IEC wprowadziły dwie nowe kategorie, w międzynarodowej normie okablowania strukturalnego ISO 11801, obejmują następujące klasy kabli miedzianych i osprzętu przyłączeniowego: klasa E (kategoria 6) umożliwiająca transmisję z częstotliwością w zakresie do 200 MHz oraz klasa F (kategoria 7) z transmisją o szybkości do 600 MHz.

Kabel współosiowy. Kabel koncentryczny (współosiowy), stosowany początkowo głównie do tworzenia niewielkich sieci LAN *(Local Area Network),* jest teraz najchętniej stosowanym medium w sieciach hybrydowych, związanych ze środowiskiem telewizji kablowej CATV. Składa się z dwu przewodów koncentrycznie umieszczonych jeden wewnątrz drugiego, co zapewnia większą odporność na zakłócenia – tym samą wyższą jakość transmisji. Powszechnie stosuje się dwa rodzaje kabli koncentrycznych: kable o oporności falowej 50 Ω (elektronika, radiokomunikacja profesjonalna) i 75 Ω (elektroniczny sprzęt powszechnego użytku). Częstotliwość graniczna współczesnych „grubych" kabli 50-omowych o przekrojach powyżej 10 mm sięga nawet 1000 MHz (przepływność binarna do 2 Gb/s). Kable 75-omowe o przekrojach 4-6 mm są wykorzystywane zarówno w transmisji cyfrowej jak i analogowej, a sygnały można przesyłać z przepływnością do 600 Mb/s. (pasmo 200 MHz użytkowane w telewizji kablowej CATV). Parametry transmisyjne kabli koncentrycznych pozwalają na ogół uzyskiwać wyższe przepływności, lecz o mniejszym zasięgu niż za pomocą skrętek.

Kabel światłowodowy. Transmisja światłowodowa polega na prowadzeniu przez włókno szklane promieni optycznych generowanych przez laserowe źródła światła. Ze względu na znikome zjawisko tłumienia, a także odporności na zewnętrzne pola

elektromagnetyczne, przy braku emisji energii poza tor światłowodowy, światłowód stanowi obecnie najlepsze medium transportowe stosowane w telekomunikacji.

Budowa światłowodu. Medium transmisyjne światłowodu stanowi czyste szklane włókno kwarcowe wykonane z dwutlenku krzemu (o kołowym przekroju), w którym światło jest zamknięte przez otoczenie nieprzezroczystym płaszczem centralnie położonego rdzenia. Dla promieni świetlnych o częstotliwości w zakresie bliskim podczerwieni współczynnik odbicia światła w płaszczu jest mniejszy niż w rdzeniu, co powoduje całkowite wewnętrzne odbicie promienia i prowadzenia go wzdłuż osi włókna. Najczęściej spotykana, znormalizowana średnica zewnętrzna płaszcza światłowodu wynosi 125 μm, a średnica płaszcza z pokryciem lakierowym – 250 μm.

Okna światłowodowe. Niejednorodna tłumienność jednostkowa światłowodu w funkcji częstotliwości (wyrażana w dB/km) określa wielkość strat absorpcyjnych medium transmisyjnego i wyróżnia się trzy podstawowe okna przydatne do prowadzenia transmisji

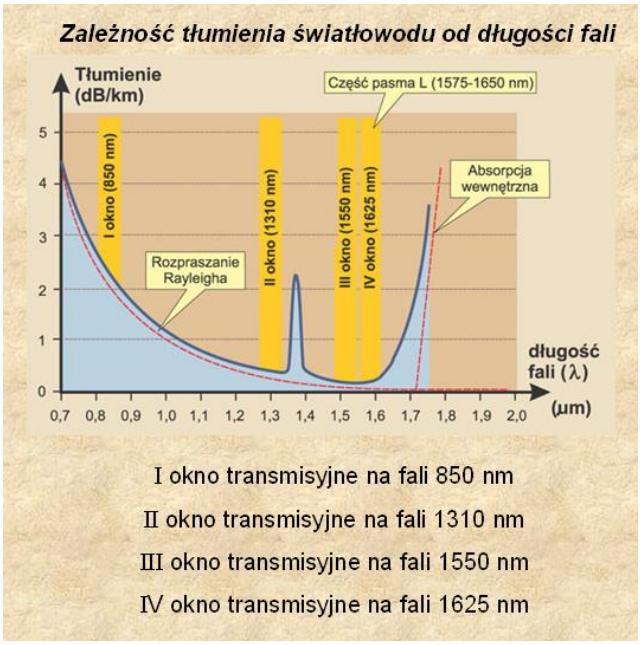
o obniżonej tłumienności. W najlepszych seryjnie produkowanych światłowodach jednomodowych tłumienność w kolejnych oknach optycznych wynosi w przybliżeniu: I okno (850 nm) – 0,7 dB/km, II okno (1300 nm) – 0,4 dB/km i III okno (1550 nm) – 0,2 dB/km.

Generacje światłowodowe. Obecnie wyróżnia się pięć generacji światłowodowych:

- Pierwsza (okno 850 nm) wiąże się z uzyskaniem włókna światłowodowego przez amerykańską firmę *Corning Glass* w roku 1972, włókna wielomodowego o tłumienności około 4 dB/km przy długości fali λ = **850** nm oraz pojemności transmisyjnej BL poniżej 50 (Mb/s)km i skokowej charakterystyce załamania wiązki świetlnej. Pojemność transmisyjna BL (*Bitrate x Length*) charakteryzuje przydatność torów światłowodowych do tworzenia gigabajtowych sieci optycznych. Pojemność BL jest wyrażona za pomocą iloczynu dwóch wzajemnie zależnych parametrów światłowodowych: przepływności binarnej B (określanej w Mb/s, Gb/s, Tb/s) i maksymalnej odległości L (w km) między regeneratorami sygnału. Pojemność transmisyjna BL we współczesnych traktach światłowodowych osiąga wartości od 200 (Gb/s)km do 360 (Tb/s)km w zależności od stosowanej technologii włókna, jego tłumienności, wzmacniaczy optycznych EDFA i jakości połączeń torów światłowodowych.

- Druga (okno 1300 nm) charakteryzuje się zastosowaniem (od 1987r. światłowodów jednomodowych o prawie zerowej dyspersji dla fali o długości λ = 1300 nm i zmniejszeniu tłumienia jednostkowego do około 0,4 dB/km.
- Trzecia (okno 1550 nm) kolejne okno światłowodowe λ = 1550 nm, o najmniejszej do tej pory uzyskanej tłumienności jednostkowej, od 0,16 do 0,20 dB/km, co pozwala na zwiększenie odległości międzyregeneratorowych do 200 kilometrów.

Kolejne generacje w technologii optycznej nie powstają już w wyniku dalszego udoskonalenia medium transmisyjnego, lecz przez jakościowe zwiększanie przepływności B lub pojemności transmisyjnej BL, operujących w oknach o najmniejszej tłumienności: 1300 nm i 1550 nm. I tak, czwarta generacja jest związana z wprowadzeniem szerokopasmowych wzmacniaczy optycznych EDFA *(Erbium-Dopped Fibre Amplifier)* oraz zwielokrotnienia falowego WDM *(Wavelenght Division Multiplexing)* w torach optycznych. Najnowsze osiągnięcia w zakresie transmisji solitonowej, umożliwiające prawie nieograniczony wzrost pojemności transmisyjnej BL, tworzą zręby nowej, piątej generacji przezroczystych systemów światłowodowych.



Rys.2.6. *Okna transmisyjne w światłowodach.*

Media bezprzewodowe. W telekomunikacji wykorzystuje się dwa rodzaje bezprzewodowego medium transmisyjnego WLAN (*Wireless Local Area Network*): fale z zakresu podczerwieni i fale radiowe. Zakres częstotliwości radiowych, ograniczony wieloma aspektami technicznymi, pozwala realizować systemy bezprzewodowej łączności radiowej RLAN (Radio LAN) z przepływnościami zwykle nie przekraczającymi 2 Mb/s dla pojedynczego abonenta systemu. Alternatywą dla

mikrofalowych kanałów radiowych jest transmisja bezprzewodowa oparta na promieniowaniu elektroenergetycznym o długościach fali 700 - 1500 nm, to znaczy fal radiowych z zakresu podczerwieni – praktycznie bez ograniczenia maksymalnej przepływności transmisji. Uzyskiwane w ten sposób przekazy mają obecnie standardowo przepływność 155 Mb/s (ATM), najnowsze zaś rozwiązania osiągają szybkość 622 Mb/s (ATM). Oczekiwania użytkowników mobilnych sięgające przepływności 1 Gb/s są w zasięgu tej technologii przekazu, jednak tylko na niewielkim obszarze – głównie w sieciach lokalnych LAN (bezprzewodowy Gigabajt Ethernet).

Łącza podczerwone. Kanały transmisyjne z zakresu podczerwieni, emitowane w otwartej przestrzeni lub w pomieszczeniach budynków, pomimo ich podobieństwa do kanałów radiowych wyróżniają się następującymi cechami:

- szeroki użytkowy zakres widma, wynoszący nawet 200 THz, może być wykorzystywany wielokrotnie w obrębie tego samego budynku, co jest związane z brakiem przenikalności fal przez ściany pomieszczeń (odbicie 40 – 90% energii fal od ścian wewnętrznych budynków);
- niewielkie lub żadne zaniki sygnałów wynikające z wielodrogowości transmisji;
- stosunkowo duża wrażliwość na zakłócenia pochodzące ze źródeł promieniowania widzialnego, co wymaga używania specjalnych konstrukcji urządzeń nadawczo – odbiorczych.

Fale radiowe. Przyjmuje się, że przekazy niskich częstotliwości widma elektromagnetycznego od 3 kHz do 300 GHz są traktowane jako transmisje na falach radiowych. Typowym zastosowaniem fal radiowych jest radiodyfuzja programów radiowych (z modulacją amplitudy AM i częstotliwości FM) i telewizyjnych oraz radiokomunikacja. Zasięg fal radiowych o wysokich częstotliwościach jest ograniczony linią widnokręgu, chociaż istnieje wiele zjawisk rozszerzających ten zasięg.

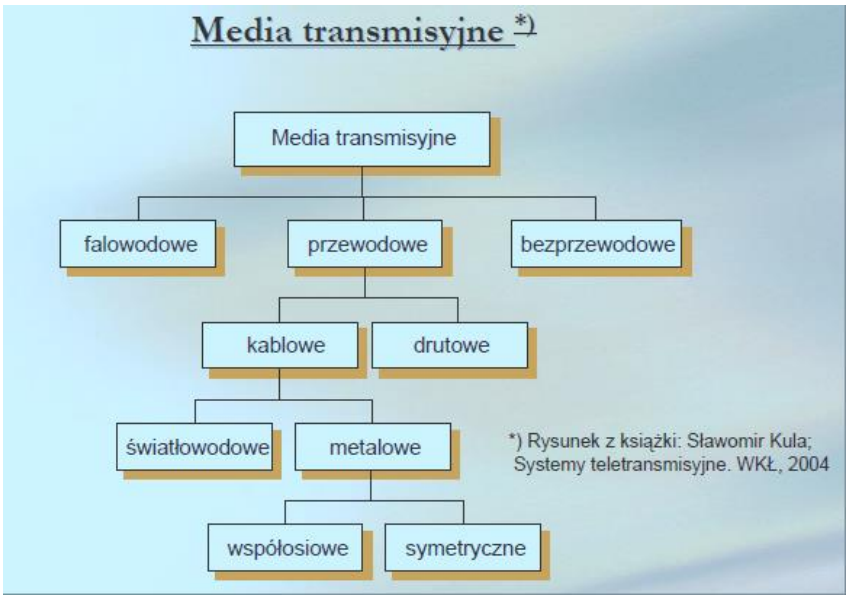
Transmisje mikrofalowe. Transmisja za pomocą mikrofal (o częstotliwości powyżej 1 GHz) może być zrealizowana pod warunkiem wzajemnej widoczności anten nadawcy i odbiorcy. Odstępstwem od tej zasady jest wykorzystanie zjawiska ugięcia i rozproszenia; wolny od przeszkód obszar pierwszej sfery Fresnela (elipsoida obrotowa), co umożliwia komunikacje w obszarze poza bezpośrednią widocznością anten. Maksymalna odległość miedzy kolejnymi węzłami naziemnej radiolinii mikrofalowej zwykle nie przekracza 60 km; aby uzyskać większy zasięg stosuje się stacje przekaźnikowe (przemienniki pasma). Stosowane częstotliwości radiowe znajdują się w zakresie 1 - 30 GHz, przy czym wyższe częstotliwości są używane do transmisji

prywatnych na krótszych dystansach, o większych możliwościach skupiania kierunkowego – podobnie jak promieniowanie optyczne. Transmisje mikrofalowe są stosowane w celu:

- łączności między dwoma budynkami w mieście;
- komunikacji na terenach otwartych, gdzie położenie kabla nie jest opłacalne (pustynie, bagna obszary wodne);
- zapewnienia połączeń naziemnych dublujących inne rodzaje komunikacji publicznej;
- zapewnienia łączności satelitarnej za stacjami naziemnymi.

Rozróżnia się dwa rodzaje łączy mikrofalowych: typowe łącza dwupunktowe klasy P - P (Point to Point) do komunikacji radioliniowej, także stosowane w sieciach komórkowych oraz klasy P- MP (Point to Multipoint), z przeznaczeniem do tworzenia dwukierunkowej sieci komunikacyjnej z koncentracja ruchu.

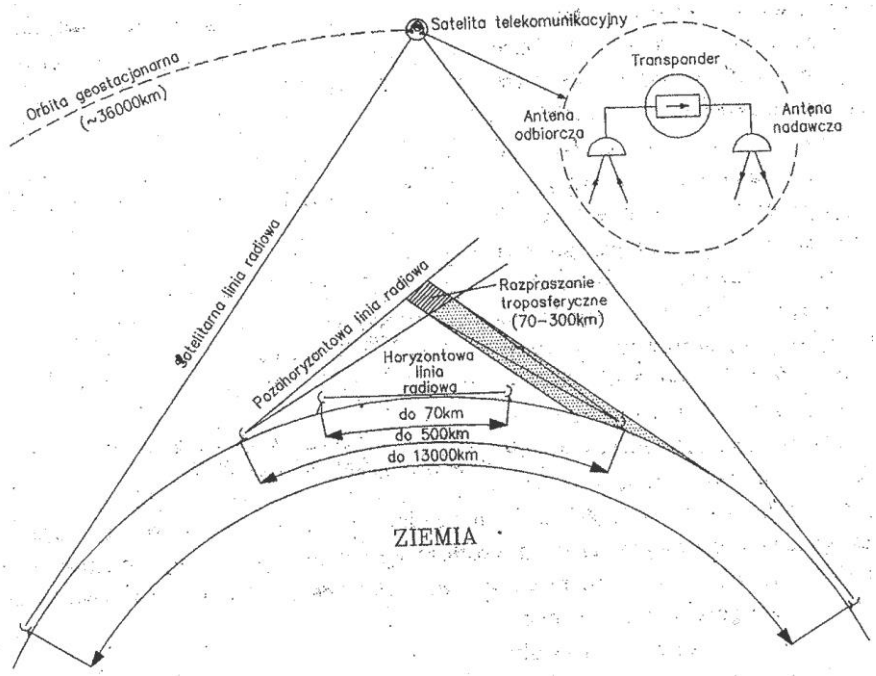
Łącze mikrofalowe. Zakres częstotliwości, na których działają naziemne łącza mikrofalowe na potrzeby telekomunikacji, jest różnie definiowany. Najczęściej stosowane długości fali radiowej w zakresie centymetrowym, od 1 m do 1mm, odpowiadają częstotliwościom od 0,3 GHz do 30 GHz, niekiedy nawet 300 GHz (0,1 mm).



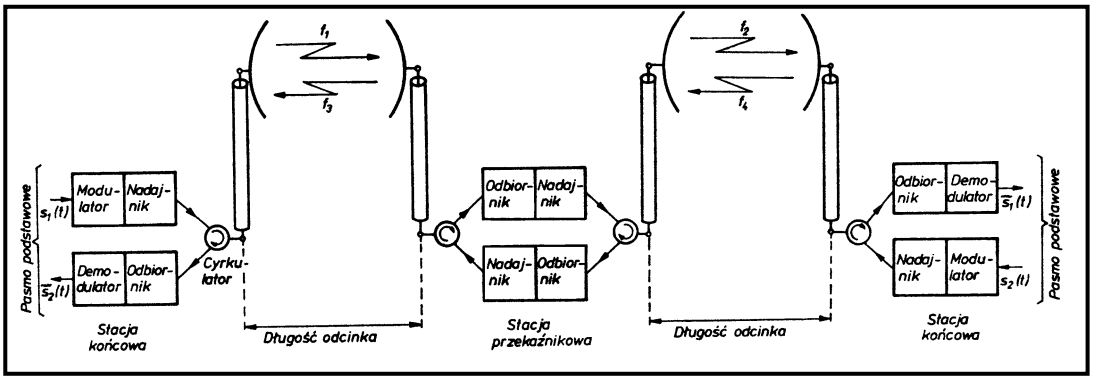
Rys.2.7. *Klasyfikacja (podział) mediów transmisyjnych.*

W radiokomunikacji najczęściej wykorzystuje się systemy radiowe jako połączenia radioliniowe (o ukierunkowanej charakterystyce promieniowania

zmodulowanej fali elektromagnetycznej). W praktyce stosuje się trzy typy systemów radiolinowych: horyzontowe – zasięg ograniczony krzywizną Ziemi, pozahoryzontowe wykorzystujące do propagacji fal zjawisko rozproszenia troposferycznego (troposfera jest niejednorodna, „smog" nad miastem, opady, różna koncentracja pary wodnej tzw. „globole" powoduje rozproszenie energii wielkiej częstotliwości emitowanej z nadajnika i niewielka część tej energii wraca do stacji odbiorczej) pozwalające na osiągnięcie większych zasięgów oraz radiolinii satelitarnych gdy potrzebujemy zasięgów bardzo dużych. Podział systemów linii radiowych przedstawia rys. 2.8, a schemat przykładowej linii radiowej rysunek 2.9.



Rys.2.8. *Podział linii radiowych.*



Rys.2.9. *Przykładowa linia radiowa.*

Łącza satelitarne. Łącza satelitarne, działające w szerokim zakresie częstotliwości radiowych od 0,3 GHz (pasmo UHF) do ponad 40 GHz (pasmo V) są wykorzystywane zarówno w komunikacji satelitarnej, jak i kosmicznej.

Do typowych zastosowań należą:

- komunikacja z naziemnymi obiektami ruchomymi (lądowa, lotnicza, morska, osobista i specjalna);
- komunikacja satelitarna ISL *(Inter Satellite Link)* między orbitującymi obiektami;
- naziemna komunikacja rozsiewcza (radiowa i telewizyjna);
- globalna radiolokacja i radionawigacja;
- badanie przestrzeni kosmicznej;
- aplikacje przyszłościowe (przesyłanie energii, łączność kosmiczna).

Podobnie jak w telekomunikacji tradycyjnej, tak i w komunikacji naziemnej za pomocą łączy satelitarnych mamy trzy sposoby jej realizacji:

- dwupunktowe połączenia porozumiewawcze P - P (*Point to Point)* zapewniające dwukierunkową łączność między dwiema stacjami naziemnymi (poprzez sieci kratowe) – zwykle dla transmisji ciągłych bez pośrednictwa stacji centralnej;
- komunikacja rozsiewcza typu P – MP *(Point to Multipoint)*, w której jedna stacja rozsyła jednokierunkowo sygnały do praktycznie nieograniczonej liczby odbiorców;
- interakcyjna komunikacja typu MP – P *(Multipoint to Point)*, w której zdalne terminale komunikują się ze sobą przez centralną stację pośredniczącą.

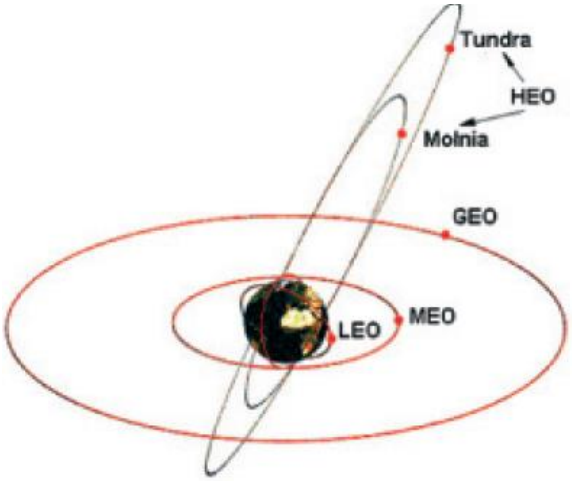
W systemach łączności satelitarnej wykorzystuje się satelity orbitujące na orbitach:
- **GEO** *(Geostationary Earth Orbit)* orbita geostacjonarna - satelity rozmieszczone w płaszczyźnie równikowej na wysokości 35786 km. Orbitę na tej wysokości nazywa się orbitą geostacjonarną, gdyż dla obserwatora na Ziemi prędkość kątowa obiegu Ziemi przez satelitę jest równa prędkości kątowej obrotu Ziemi wokół własnej osi. Aby zapewnić łączność wokół kuli ziemskiej, do szerokości geograficznej 75° potrzeba 3 do 4 satelitów. Duża odległość od powierzchni Ziemi wprowadza duże opóźnienia wynoszące około 500 ms (250 ms ziemia – satelita + 250 ms satelita - ziemia + czas niezbędny na obróbkę sygnału na pokładzie satelity). Aby satelity przetransportować na wymaganą w tych systemach wysokość orbity, potrzebne są kosztowne systemy rakietowe. W systemach GEO stosowane są duże moce sygnałów, ze względu na znaczną wysokość, przez co niemożliwe jest stosowanie na Ziemi terminali ręcznych. Systemy GEO nie obejmują swoim zasięgiem obszarów podbiegunowych, co jest ich

mankamentem, więc aby zapewnić łączność na terenach podbiegunowych (Kanada, Norwegia, Rosja) skonstruowano systemy o wydłużonych orbitach eliptycznych.

- **HEO** *(Helical Earth Orbit* lub *Higly Eliptical Orbit)* wydłużona orbita eliptyczna nachylona pod pewnym kątem do osi obrotu Ziemi. Parametry orbity; apogeum – punkt najdalszy od Ziemi – 40 do 50 tys. km a perigeum – punkt najbliższy Ziemi rzędu 5 tys. km. Dzięki takim parametrom satelita jest widoczny pod dużym kątem elewacji i może zapewnić łączność w terenach górzystych i silnie zurbanizowanych. System HEO wymaga anten śledzących na Ziemi i potrzeba od 3 do 10 satelitów aby zbudować system o właściwościach podobnych do GEO ale o zasięgu regionalnym.

- **MEO** ***(****Medium Earth Orbit****)*** - określane są także jako ICO *(Intermediate Circular Orbit)* - systemy o średniej wielkości orbit. Orbity dla satelitów wchodzących w skład tych systemów znajdują się na wysokości od 8000 km do 12000 km a nawet do 20 tysięcy kilometrów nad powierzchnią Ziemi. Taka, a nie inna wysokość wynika z istnienia poniżej, jak i powyżej, odpowiednio pierwszej i drugiej strefy Van Allena, składających się z cząsteczek niebezpiecznych dla elementów elektronicznych satelitów. Wysokość ta wpływa korzystnie na liczbę potrzebnych satelitów do pokrycia swoim zasięgiem całej ziemi, wystarcza od 10 do 15 satelitów (GPS – 24 satelity). Opóźnienie sygnału wynosi ok 150 ms, a orbity mogą być kołowe lub eliptyczne.

- **LEO** *(Low Earth Orbit)* systemy o niskich orbitach kołowych znajdujących się na wysokości teoretycznie od 200 do 2000 km, praktycznie 500 do 2000 km nad powierzchnią Ziemi. Umiejscowienie satelity właśnie na takiej wysokości wynika z faktu, że do 500 km atmosfera jest zbyt gęsta i występowałoby zbyt duże tarcie, natomiast powyżej 2000 km znajduje się pierwsza strefa Van Allena, w której występują liczne protony i elektrony mogące uszkodzić elektroniczne elementy satelity. Ze względu na niewielką wysokość, aby pokryć zasięgiem całą kulę ziemską potrzebna jest dość znaczna liczba satelitów około 40. Dlatego bardzo ważną kwestią jest zapewnienie skutecznego przełączania *(handover)*. Satelity te mają także dużą prędkość przez co znajdują się krótko w zasięgu naziemnej stacji abonenckiej lub bazowej. Zaletą systemów LEO jest niewielka wartość opóźnienia propagacyjnego rzędu 50 ms, dzięki czemu można bardzo łatwo i z dobrym rezultatem transmitować głos. Minusem systemów LEO jest duża liczba wymaganych satelitów. Istotne znaczenie ma tutaj także efekt Dopplera. Orbity LEO są najczęściej kołowe, czasami eliptyczne.



Rys.2.10. *Orbity sztucznych satelitów Ziemi: LEO – orbita niska, MEO – orbita średnia,HEO – wydłużona orbita eliptyczna, GEO – orbita geostacjonarna.*

Stacje satelitarne. Od chwili oddzielenia się satelity od ostatniego członu rakiety wynoszącej, kontrolę nad dalszym lotem satelity i jego funkcjonowania przez cały czas trwania misji (np. 10 – 15 lat) przejmuje **naziemna stacja kontrolna TTAC** *(Tracking, Telemetry and Command),* która nawiązuje łączność, stabilizuje lot, sprawdza na bieżąco wszystkie parametry transpondera, łącznie z korektą jego orbity oraz kierunkowością anten i poprawnością działania kanałów komunikacyjnych. Operatorzy stacji TTAC prowadzą stały nadzór stanu technicznego satelity telekomunikacyjnego, a w przypadku awarii elementów napędowych lub komunikacyjnych przeprowadzają zamianę uszkodzonych elementów na zapasowe układy redundancyjne (technika zdalnej redundancji układów transponderów jest jedną istotnych funkcji satelity). Nad właściwym wykorzystaniem łączy komunikacyjnych przekaźnika lub kilku równocześnie orbitujących przekaźników czuwa wydzielona **stacja centralnego sterowania satelitami SCC** *(Satelite Control Center).* Centrum to, oprócz kontroli i zarządzania połączeniami satelitarnymi z siecią PSTN *(Public Swiching Telephone Network)* przez huby i rutery, ma możliwość nadrzędnego przejęcia wszystkich funkcji sterujących z podległej mu stacji kontroli TTAC. Usługi oferowane przez współczesne systemy satelitarne to: FSS *(Fixed Satellite Sevices)* - np. sieci VSAT, MSS *(Mobile Satellite Services)* - systemy Inmartsat, BSS *(Broadcasting Satellite Services)* – TV, DVB …, RDSS *(Radiodetermination Satellite Services)* – GPS.

Z omówionych powyżej charakterystyk mediów transmisyjnych wynika, że zbudowanie pełnej infrastruktury łączy transmisyjnych, wymaga bardzo dużych nakładów finansowych. Z tego powodu obecnie nie stosuje się transmisji w paśmie

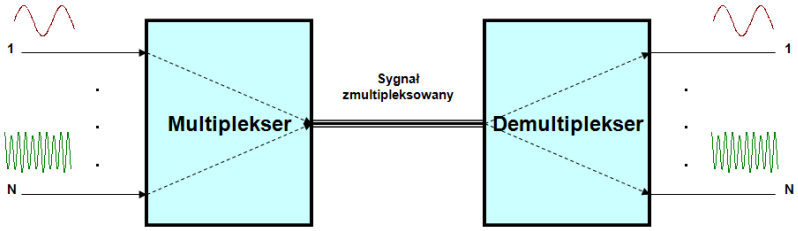
naturalnym (bezpośrednie połączenie dwu terminali kablem, jak w polowych systemach telefonicznych) lecz stosujemy systemy zwielokrotniania łączy. Poprawia to warunki amortyzacji inwestycji w systemy teletransmisyjne.

2.4. Zwielokrotnienie (multipleksacja) łączy.

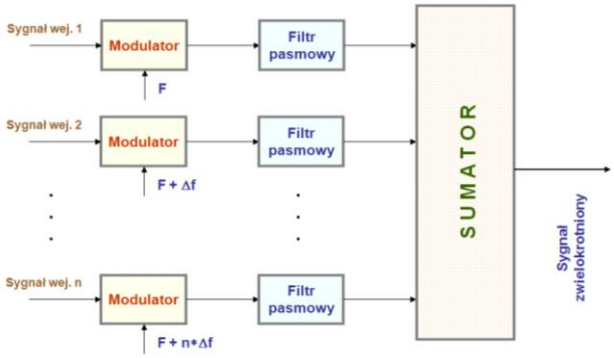
Multipleksacja kanałów. Proces multipleksacji kanałów (zwielokrotnienia) polega na transmisji wielu sygnałów analogowych lub cyfrowych o niższej przepływności przez pojedynczy kanał komunikacyjny o dużej przepływności binarnej. Po drugiej stronie łącza zachodzi proces odwrotny, zwany demultipleksacją, odtwarzający pierwotne strumienie sygnałów. Do najczęściej spotykanych metod zwielokrotnienia pojedynczych kanałów informacyjnych (w traktach przewodowych, światłowodowych, radiowych i satelitarnych) należą: częstotliwościowe **FDM** *(Frequency Division Multiplexing)*, czasowe **TDM** *(Time Division Multiplexing)*, kodowe **CDM** *(Code Division Multiplexing)*, falowe **WDM** *(Wavelenght Division Multiplexing)*, kierunkowe **DDM** *(Direction Division Multiplexing)* i przestrzenne **SDM** *(Space Divisin Multiplexing)*. Dla torów miedzianych największe znaczenie mają zwielokrotnienia częstotliwościowe FDM i czasowe TDM, dla torów światłowodowych zwielokrotnienia falowe WDM a dla torów radiowych zwielokrotnienia kodowe CDM. Multipleksacja (zwielokrotnienie) jest więc techniką transmisyjną pozwalającą na współużytkowanie medium transmisyjnego przez wielu użytkowników. Wykorzystywana do współużytkowania torów telekomunikacyjnych lub dostępu do wspólnego medium transmisyjnego. Multipleksacja może następować w zakresie jednego z trzech parametrów – czasie, częstotliwości i mocy.

Zwielokrotnienie częstotliwościowe FDM, jest zwielokrotnieniem sygnałów, które polega na umieszczaniu widma sygnałów wejściowych w kolejnych przedziałach częstotliwości o szerokości pasma sygnału podstawowego. Dla przesyłania N sygnałów wejściowych o paśmie widma Δf wymagane jest zarezerwowanie pasma równego $N * \Delta f$. Jest to taki sposób przesyłania analogowych lub cyfrowych sygnałów z wykorzystaniem oddzielnej częstotliwości nośnej dla każdego kanału użytkownika i każdego kierunku transmisji. Dla tego multipleksowania stosuje się najczęściej metodę dostępu do kanału z podziałem częstotliwości FDMA (*FDM Access*), w którym każdy udział użytkownika może być wprowadzany, wydzielany i wykorzystywany oddzielnie. Współużytkowanie toru przedstawiają rysunki, poglądowo 2.12 i „technicznie” 2.13 a zasadę zwielokrotnienia 2.14 i przykład takiego zwielokrotnienia 2.15.

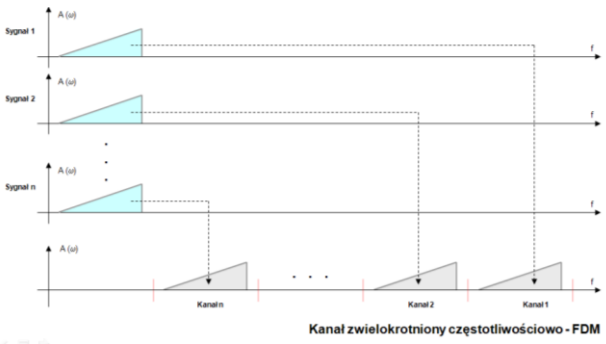
Rys.2.12. *Współużytkowanie toru*



Rys.2.13. *Współużytkowanie toru*

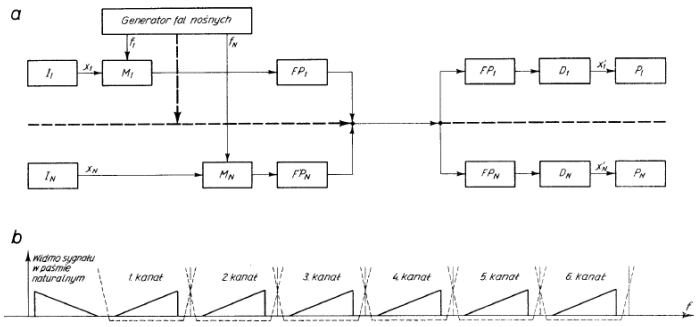


Rys.2.14. *Zasada zwielokrotnienia FDM*



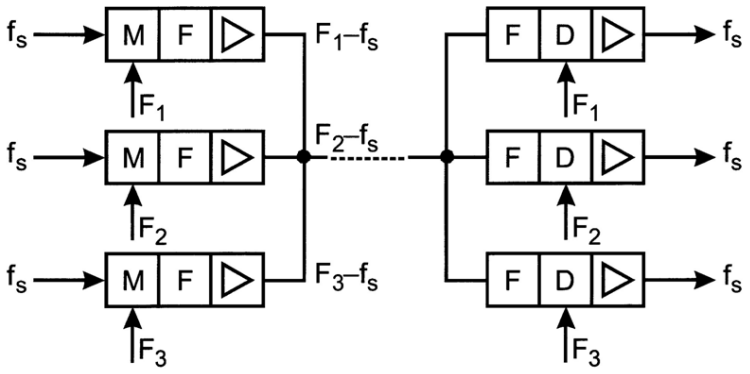
Rys.2.15. *Przykład zwielokrotnienia FDM*

Zwielokrotnienie częstotliwościowe polega więc na przeniesieniu pasm abonenckich w inne (wyższe) zakresy częstotliwości drogą wielokrotnej modulacji amplitudy i wydzieleniu poprzez filtrację górnej wstęgi bocznej widma sygnału zmodulowanego (po stronie nadawczej) i „włożenie sumy" tych sygnałów na wspólny tor transmisyjny. Po stronie odbiorczej filtrami wydzielamy fragmenty widma, przypisane konkretnym abonentom, demodulujemy i odtwarzamy odebrany sygnał. Schemat takiego systemu przedstawia rysunek 2.16.

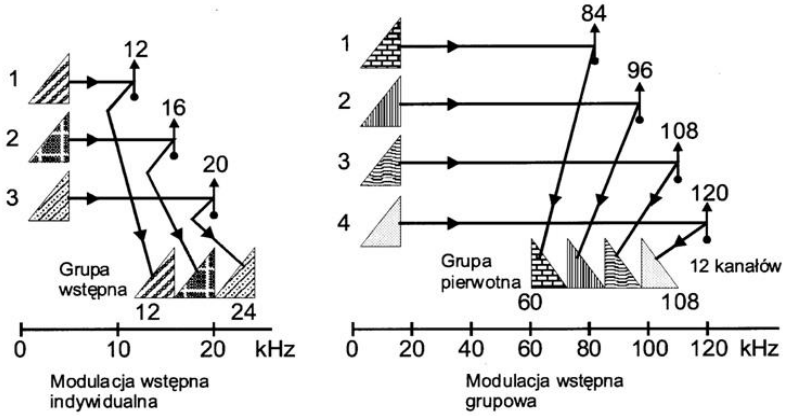


Rys.2.16. *Schemat systemu wielokrotnego z podziałem częstotliwościowym (a) i widmo sygnału grupowego (b).*

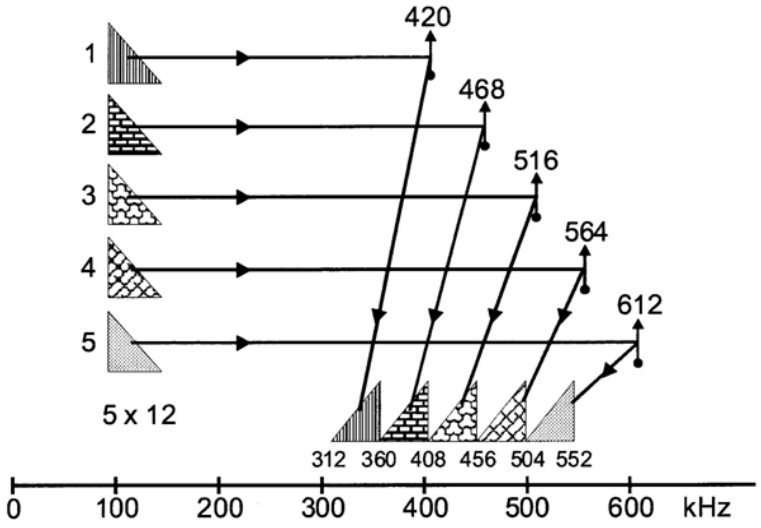
Dojście do założonej krotności systemu realizuje się poprzez kilka etapów; modulację wstępną – rys. 2.17; tworzenie grupy pierwotnej – rys. 2.18 (bierzemy 3 abonentów, każdy pracuje w paśmie 0,3 ÷ 3,4 kHz więc „włożenie" ich na wspólny kabel dałoby efekt „telefonu towarzyskiego", wszyscy słyszą rozmowy pozostałych. Każdemu z abonentów przydzielamy inną częstotliwość nośną 12, 16, 20 kHz modulujemy wyławiamy wstęgę górną i mamy przeniesienie pasm abonenckich w inny zakres częstotliwości 12 ÷ 24 kHz. Ponieważ każdy z abonentów ma dostęp do swojego „kawałka" widma to wyeliminowany został efekt „telefonu towarzyskiego". Podobnie postępujemy dalej, cztery grupy wstępne – każdą traktujemy jak poprzednio abonenta – dobieramy odpowiednie częstotliwości nośne, modulujemy, wyławiamy górną wstęgę i w paśmie 60 ÷ 108 kHz mamy 12 abonentów którzy jednocześnie mogą rozmawiać na jednej parze przewodów); tworzenie grupy wtórnej – na tej samej zasadzie – rys. 2.19; tworzenie grupy trójnej i grup o wyższych krotnościach, aż do założonej opłacalnej dla operatora krotności. Stosowane zwielokrotnienia częstotliwościowe zawiera tabela 7.



Rys.2.17. *Modulacja wstępna*



Rys.2.18. *FDM – grupa pierwotna*



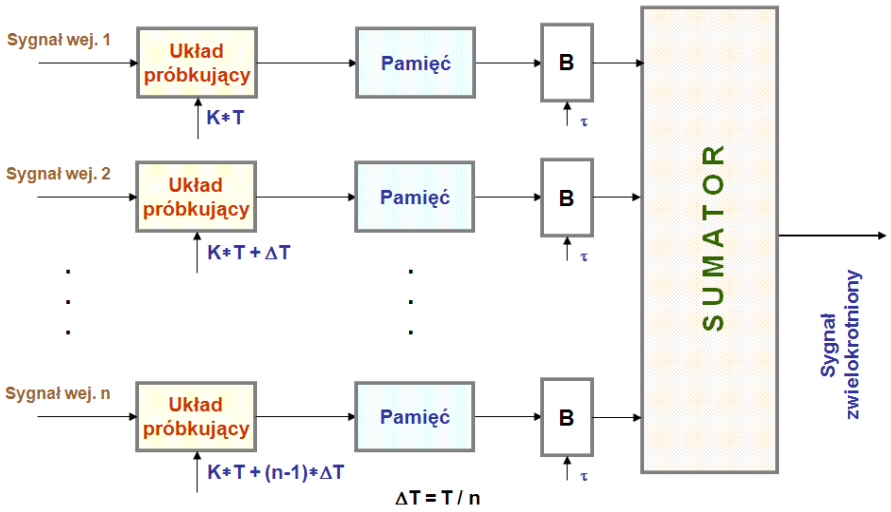
Rys.2.19. *FDM – grupa wtórna*

Tablica 7. *Wielokrotne systemy analogowe*

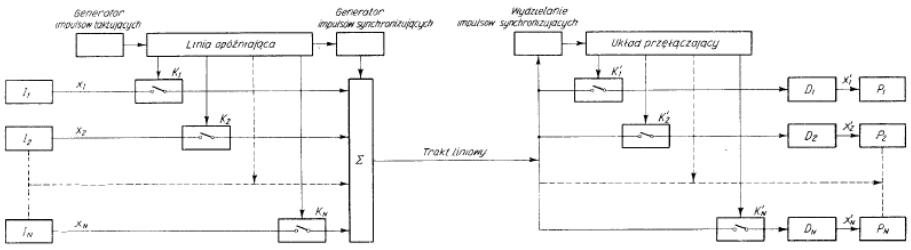
Krotność systemu	Liczba i rodzaj grup podstawowych składających się na system	Pasmo [kHz]	Określenie systemu
12	1 grupa podstawowa	60 ÷ 108	Grupa pierowotna
60	5 grup podstawowych 1 grupa wtórna	312 ÷ 552	Grupa wtórna
300	5 grup podstawowych lub 1 grupa trójna	60 ÷ 1300 64 ÷ 1296	1, 3 MHz
600	10 grup wtórynych	60 ÷ 2540	2,6 MHz
900	3 grupy trójne	64 ÷ 4024 lub 316 ÷ 4188	4 MHz
960	16 grup wtórnych	60 ÷ 4028	4 MHz
1200	4 grupy potrójne	316 ÷ 5564	6 MHz
1260	21 grup wtórnych	60 ÷ 5564	6 MHz
2700	3 grupy czwórne	316 ÷ 12388	12 MHz
2700	2 grupy czwórne + 1 zestaw 15 grup wtórnych	312÷12388	12 MHz
2700	3 zestawy 15 grup wtórnych	312 ÷ 12336	12 MHz
7200	8 grup czwórnych	4332 ÷ 39884 lub 4404 ÷ 39780	40 MHz
10800	12 grup czwórnych	4332 ÷ 59684 lub 4404 ÷ 59580	60 MHz

Zwielokrotnienie w dziedzinie czasu TDM. Zwielokrotnienie w dziedzinie czasu polega na ustaleniu stałego odcinka czasu nazwanego ramką, która jest synchronicznie przesyłana w kanale. Ramkę dzieli się na mniejsze odcinki zwane szczelinami, w których przesyła się wartości chwilowe przenoszonego sygnału. Jest to więc sposób przesyłania analogowych lub cyfrowych sygnałów z wykorzystaniem jednego kanału (częstotliwościowego) do transmisji informacji do wielu użytkowników, przez podział kanału na odcinki czasu, zwane szczelinami czasowymi, skojarzone z różnymi użytkownikami. Dla takiego multipleksowania stosuje się metodę dostępu do kanałów z podziałem czasu TDMA (*TDMA Access*). Typowym przykładem zwielokrotnienia TDM jest łącze 2 Mb/s, które może przenosić 30 kanałów 64 kb/s i kanały sygnalizacyjne. Zwielokrotnienie TDM jest często mylone z metodą czasowego dostępu

wielokrotnego TDMA (*Time Division Multiplexing Access*), stosowaną wtedy, gdy wielu użytkowników chce jednocześnie przesłać informację do jednego odbiornika, np. do stacji bazowej. Czasową multipleksację kanałów można również zastosować do realizacji łącza dupleksowego. Mamy wtedy tzw. dupleks czasowy TDD (*Time Division Duplex*), w którym część szczelin czasowych służy do przesyłania danych w jednym kierunku, pozostałe szczeliny w drugim kierunku (np. system DECT). Zasadę zwielokrotnienia TDM przedstawia rysunek 2.20 a schemat systemu wielokrotnego z podziałem czasowym rysunek 2.21.



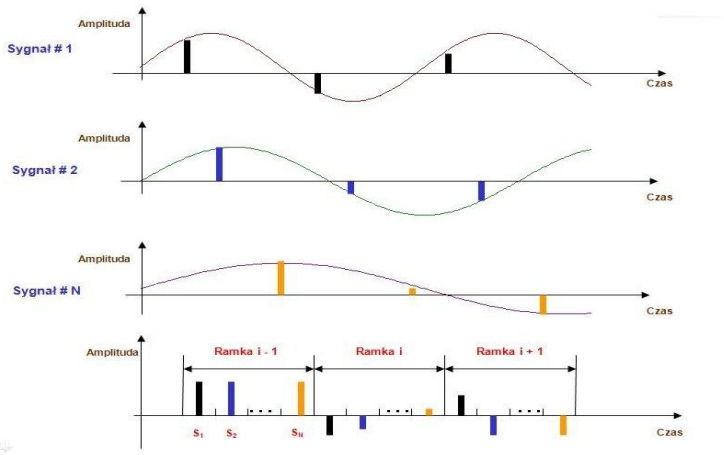
Rys. 2.20. *Zasada zwielokrotnienia TDM.*



Rys.2.21. *System wielokrotny z podziałem czasowym.*

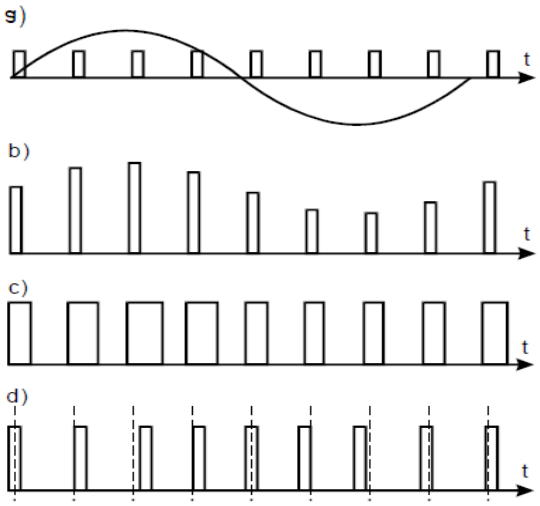
Zwielokrotnienie czasowe jest to więc taki sposób przesyłania analogowych lub cyfrowych sygnałów z wykorzystaniem jednego kanału (częstotliwościowego) do transmisji informacji do wielu użytkowników, przez podział kanału na odcinki czasu, zwane szczelinami czasowymi, skojarzone z różnymi użytkownikami. Zasada pracy takiego systemu sprowadza się do tego, że bierzemy pewną ilość sygnałów abonenckich (np. w GSM osiem, w ISDN amerykańsko japońskim **24**, w europejskim

ISDN **32**) próbkujemy każdy i pomiędzy próbki jednego kanału „wkładamy" próbki innych kanałów. Przebiegi czasowe w systemie TDM przedstawia rysunek 2.22.



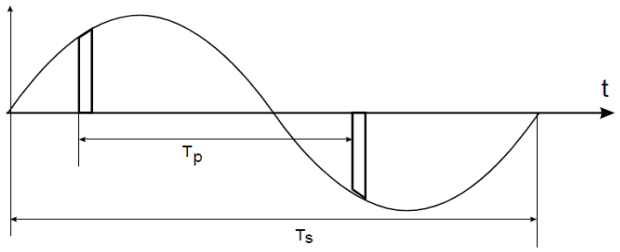
Rys.2.22. *Przebiegi czasowe w zwielokrotnieniu TDM*

Przejście od sygnału analogowego (np. sygnał mowy) do sygnału cyfrowego (dyskretnego, ziarnistego) można zrealizować na kila sposobów. Historycznie najwcześniej stosowane były analogowe modulacje impulsowe **PAM** *(Pulse Amplitude Modulation)* - informacja o chwilowej wartości przebiegu próbkowanego zapisana wielkością amplitudy impulsu, **PWM** *(Pulse Width Modulation)* – informacja o chwilowej wartości przebiegu próbkowanego zapisana czasem trwania impulsu oraz **PPM** *(Pulse Position Modulation)* – informacja o chwilowej wartości przebiegu próbkowanego zapisana w odchyleniu rzeczywistego położenia próbki od położenia nominalnego, rysunek 2.23.



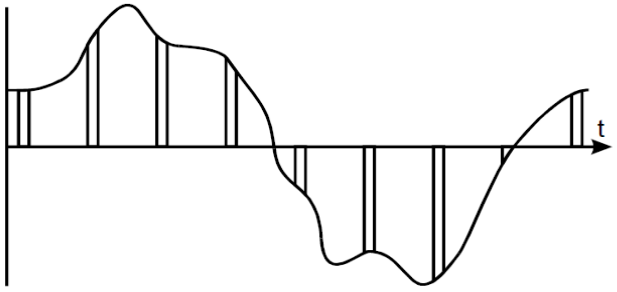
Rys.2.23. *Analogowe modulacje impulsowe. a) przebieg analogowy i ciąg impulsów próbkujących b) modulacja amplitudy impulsów – PAM c) modulacja szerokości impulsów PWM d) modulacja położenia impulsów PPM.*

Istotnym problemem jest dobór właściwej częstości próbkowania. Zgodnie z teorią Kotielnikowa – Shannona (twierdzenie o próbkowaniu) w przypadku przekształcania analogowego sygnału pasmowego, częstotliwość próbkowania musi być większa lub co najwyżej równa dwukrotnej częstotliwości maksymalnej sygnału próbkowanego $f_p \geq 2\ f_m$



Twierdzenie o próbkowaniu:

$T_p \leq 0{,}5\ T_s$ lub $f_p \geq 2\ f_g$



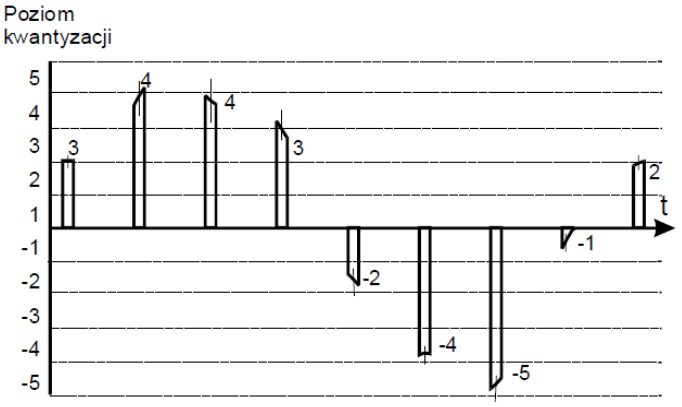
Rys.2.24. *Próbkowanie*

W sygnale mowy f_{max} wynosi 3400 Hz a z uwzględnieniem „pewnego zapasu" (pasma ochronnego przyjęto f_{max} = 4000 Hz więc należy próbkować 8000 razy/sek czyli co 125 μs. Dla cyfrowego zapisu dźwięku na płycie kompaktowej przyjęto częstotliwość próbkowania f_p = 44,1 kHz. Żadna z w/w impulsowych modulacji analogowych nie znalazła szerszego praktycznego zastosowania (PPM zastosowano w systemach wojskowych) pojawił się pomysł aby zakodować wartość każdej konkretnej próbki pewną paczka impulsów. To doprowadziło do powstania modulacji PCM *(Pulse Code Modulation – modulacja impulsowo - kodowa).* Pozwala to zapewnienie poprawnego przekazania sygnału cyfrowego poprzez trakt z zakłóceniami. Przekształcenie sygnału analogowego np. mowy w sygnał cyfrowy PCM wymaga czterech etapów (kroków):

- określenie dozwolonego zakresu zmian sygnału analogowego ± A (+A maksymalna amplituda dodatnia, – A maksymalna amplituda ujemna),

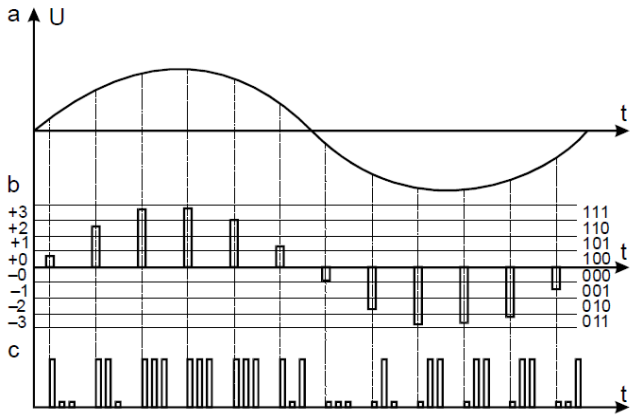
- kwantyzacja,
- próbkowanie,
- kodowanie.

Kwantyzacja polega na zakwalifikowaniu wartości amplitudy próbki z ciągłego przedziału wartości do jednego ze skończonej liczby przedziałów np. 128 w systemie amerykańsko – japońskim lub 256 w systemie europejskim. Rysunek 2.25.



Rys.2.25. *Kwantyzacja*

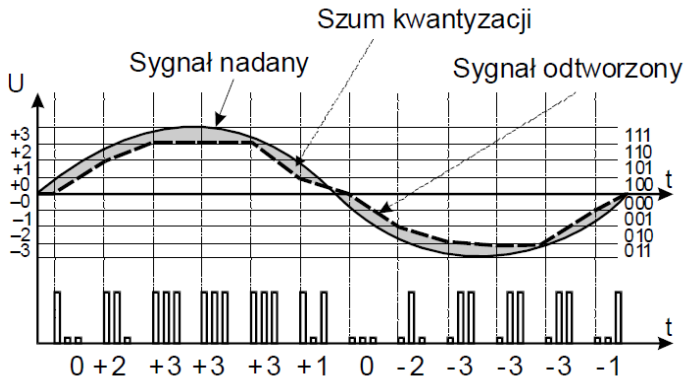
Każdemu poziomowi kwantyzacji przyporządkowujemy pewną liczbę binarną 7 - bitową w systemie stosowanym w USA i Japoni lub 8 – bitową w systemie europejskim. Wiedząc jaka jest konkretna wartość próbki (w którym pasku jest wierzchołek) kodujemy tę wielkość poprzez podanie liczby binarnej odpowiadający danemu poziomowi kwantyzacji.



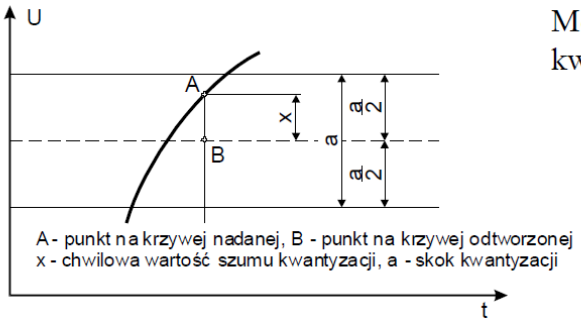
Rys.2.26. *Kodowanie symetryczne*

Taki ciąg bitów przesyłamy przez łącze telekomunikacyjne, po wcześniejszym dodatkowym kodowaniu transmisyjnym np. kodem AMI *(Alternate Mark Inverion)* eliminującym składową stałą w łączu. Ponieważ odstęp między paczkami impulsów przypisanych dla konkretnego sygnału wynosi 125 μs to możemy podobnie jak w przypadku modulacji PAM zwielokrotnić łącze, wstawiając w tę lukę paczki bitów

innych sygnałów. W systemie amerykańsko – japońskim mamy zwielokrotnienie czasowe 24 razy a w europejskim 32 razy. Problemem jest poprawne odtworzenie sygnału po stronie odbiorczej. Odbiornik „zakłada", że wierzchołek próbki jest zawsze w środku przedziału kwantyzacji a po stronie nadawczej przebieg próbkowany może przyjmować wartości z całego przedziału kwantyzacji (rys. 2.27 i 2.28). Stąd pojawia się różnica pomiędzy sygnałem nadanym a odtworzonym. Różnicę tę nazywamy szumem kwantyzacji. Mimo nazwy „szum" nie jest to zakłócenie lecz zniekształcenie związane z przyjętym sposobem modulacji.



Rys.2.27. *Odtworzenie sygnału*

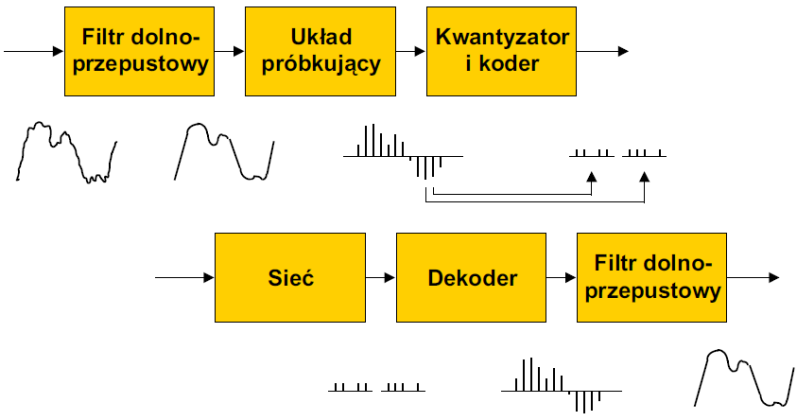


Moc szumu kwantyzacji:

$$S_k^2 = \frac{a^2}{12}$$

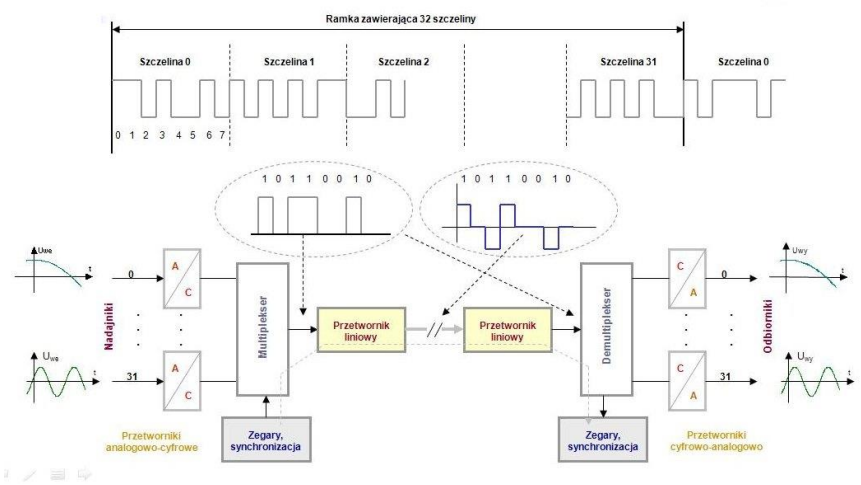
Rys.2.28. *Szum kwantyzacji*

Moc szumu kwantyzacji zależy wyłącznie od wartości skoku kwantyzacji a nie od wielkości próbki, stąd w europejskim systemie PCM jest on mniejszy niż w systemie amerykańsko – japońskim (dwukrotnie większe poziomy kwantyzacji). Blokowy schemat modulacji PCM przedstawia rysunek 2.29.

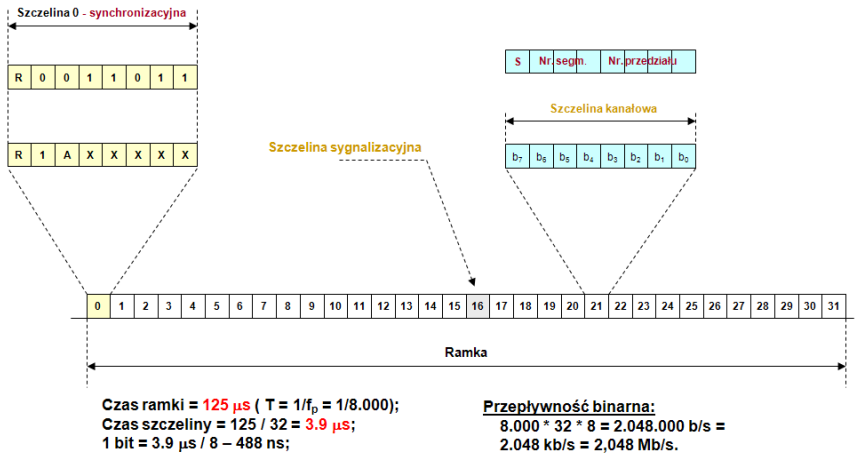


Rys.2.29. *Schemat blokowy modulacji PCM*

Zwielokrotniony system PCM przedstawia rysunek 2.30, ramkę takiego systemu rys. 2.31 a dane techniczne sytemu tabela 8.



Rys.2.30. *Zwielokrotniony system PCM*

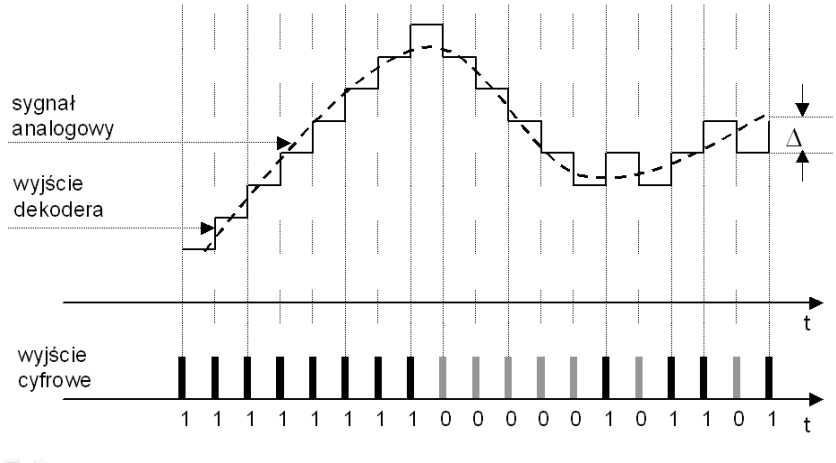


Rys.2.31. *Ramka systemu PCM 32/30*

Tabela 2.8. *Parametry systemu PCM 32/30*

Paramter	Wielkość
Przepływność binarna	2 048 kb/s
Długość ramki	125 µs
Liczba szczelin kanałowych	32
Liczba bitów w szczelinie	8
Liczba kanałów rozmównych	30
Długość szczeliny kanałowej	3,9 µs
Liczba bitów w ramce	256
Długość wieloramki	2 ms
Liczba ramek w wieloramce	16
Liczba stopni kwantyzacji	256
Liczba szczelin sygnalizacyjnych	1
Częstotliwość próbkowania	8 kHz
Prawo kompresji	A = 87,6
Pasmo kanału rozmównego	300 - 3400 Hz

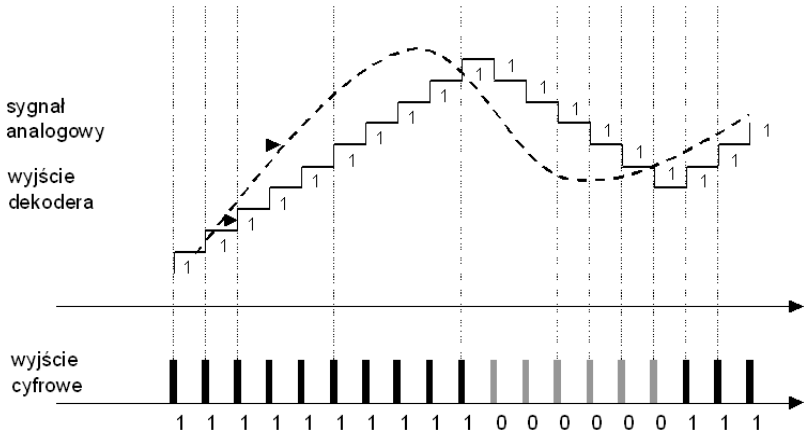
Wraz z rozwojem technologii pojawił się nowy typ modulacji cyfrowej tak zwana „1 – bitowa PCM" inaczej nazywana modulacją delta (Δ). W tym przypadku wartości próbki nie kodujemy 8 bitami lecz tylko jednym bitem, na zasadzie, czy bieżąca próbka jest większa od poprzedniej - wartość bitu 1 lub nie – wartość bitu równa 0. W ten sposób zmniejszamy przepływność binarną w torze w stosunku do przepływności w systemach PCM. Modulacja Δ jest więc przykładem kodowania różnicowego które polega na kwantyzacji i kodowaniu różnic występujących pomiędzy kolejnymi próbkami. Ponieważ wartość tej różnicy jest zwykle mniejsza od wartości próbek, to taką samą, jak w przypadku kodowania „całych" próbek, jakość odtwarzania można uzyskać przy zredukowanej ilości przesyłanej informacji w efekcie zmniejszenia liczby poziomów kwantyzacji równoważnej długości słowa kodowego.



Rys.2.32. *Zasada modulacji delta (Δ), (czasem DM – Delta Modulation)*

Modulacja delta jest więc najprostszą i najstarsza wersją kodowania różnicowego.

W tym rodzaju modulacji sygnał analogowy jest aproksymowany funkcją schodkową, którą charakteryzuje to, że zmiana wartości funkcji w kolejnych dwu szczelinach czasowych jest zawsze zmianą o jeden ustalony poziom kwantyzacji: - Δ lub + Δ a którym odpowiadają zero i jedynka. W tej sytuacji, podobnie jak w PCM szum kwantyzacji, mamy błąd poprawnego odtworzenia po stronie odbiorczej sygnału próbkowanego, rysunek 2.33.

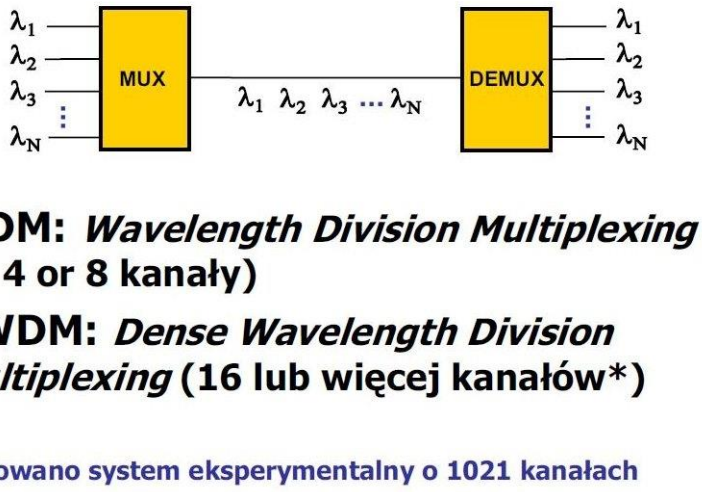


Rys.2.33. *Klasyczna modulacja delta.*

Jak widać na rysunku 2.33 odtworzony czas narastania zbocza przebiego próbkowanego (krzywa schodkowa) nie odpowiada rzeczywistemu czasowi narastania sygnału analogowego (linia przertwana). Aby poprawnie odwzorować przebieg próbkowany w systemach z modulacją delta dwukrotnie zwiększono, w porównaniu do PCM, częstotliwość próbkowania f_p = 16 kHz zamiast 8 kHz w PCM. Z tego wynika,

że przepływność binarna wynosi 16 kb/s. Taki rodzaj modulacji stosowany jest w systemach polowych np. w radiostacjach wojskowych. Pojawia się więc problem jak wprowadzić trakty cyfrowe 16 kb/s w trakt PCM o przeplywności 64 kb/s. Pierwszy pomysł to wtórne zwielokrotnienie np. 4 sygnaly 16 kb/s w jeden trakt 64 kilobitowy. Oczywistym jest, że takiego rozwiązania nie można zastosować ze względu na synchroniczną pracę systemów PCM. Można więc w jeden trakt PCM wprowadzić co najwyżej 3 trakty 16 kb/s z uzupełnieniem do przepływności 64 kb/s niedrukowalnymi znakami np. DLE i SYN z międzynarodowego kodu nr 5.

Zwielokrotnienie falowe WDM (*Wavelength Division Multiplexing*) – multipleksacja z podziałem długości fal, polegająca na równoległej i równoczesnej transmisji wielu fal o różnych długościach. Metoda ta pozwala na zwielokrotnienie przepływności w istniejących i instalowanych połączeniach, głównie światłowodowych, przez wykorzystanie szerokich pasm w drugim (pasmo 12 THz) i w trzecim oknie (pasmo 15 THz) włókna światłowodowego, do jednoczesnej transmisji wielu (kilkudziesięciu) odrębnych kanałów, każdy o szybkości np. 2,5 Gb/s czy 10 Gb/s. Dzięki temu łączna przepływność w jednym włóknie światłowodu sięga obecnie 1 Tb/s. Zasadę tego zwielokrotnienia przedstawia rysunek 2.34.



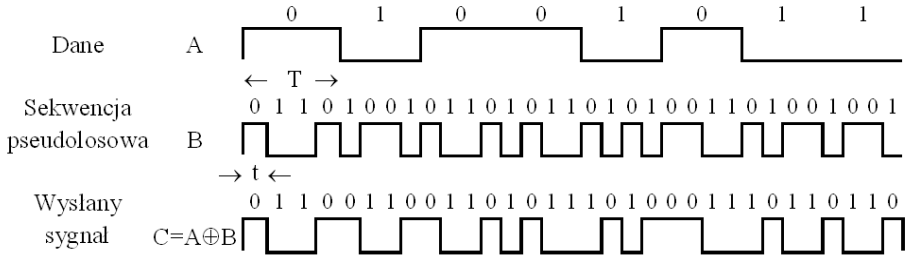
Rys.2.34. *Zasada zwielokrotnienia falowego*

Zwielokrotnienie kodowe CDM *(Code Division Multiplexing)* – sposób polegający na niezależnym kodowaniu każdego z sygnałów kodem (sekwencja) rozpraszającym. Wszystkie tak zakodowane sygnały są przesyłane w tym samym paśmie transmisyjnym. Ze względu na ortogonalność stosowanych kodów rozpraszających odbiornik jest w stanie zdekodować wysłany do niego sygnał. W tej samej technologii można zrealizować również dostęp wielokrotny oznaczony skrótem CDMA (*CDMA Access*).

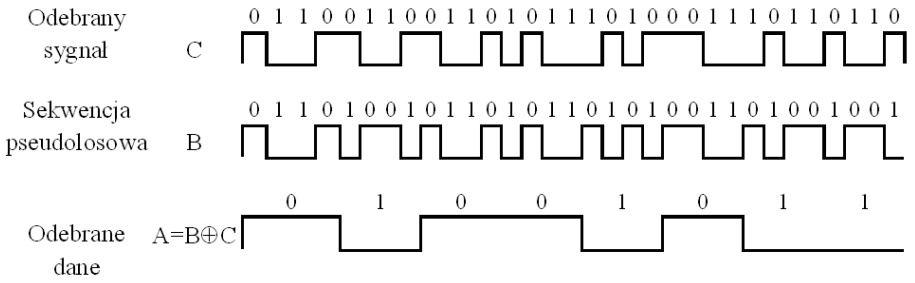
Każdy z użytkowników ma do dyspozycji przez cały czas transmisji pełne pasmo medium transmisyjnego. Jedynym warunkiem jest to, aby stosowany przez terminal kod rozpoznający był unikatowy i ortogonalny w stosunku do pozostałych kodów stosowanych w tym samym czasie. Metoda ta, oprócz uodporniania transmitowanego sygnału na zakłócenia wąskopasmowe, utrudnia nieupoważniony dostęp do sygnału. Zwielokrotnienie kodowe CDM wykorzystuje systemy z rozpraszaniem widma. Dla rozproszenia widma wykorzystuje się dwa podstawowe rodzaje systemów SS *(Spread Spectrum)*:

- DS/SS *(Direct Sequence SS)* – jest to metoda z kluczowaniem bezpośrednim wykorzystująca rozpraszanie widma przez szybkozmienne kluczowanie,
- FH/SS *(Frequency Hopping SS)* – jest to metoda skakania po częstotliwościach, czyli losowo zmieniające się częstotliwości nośne sygnału modulującego.

Idea techniki rozpraszania bezpośredniego DS./SS polegającą na kluczowaniu sygnału danych szybkozmienną sekwencją pseudolosową, generowaną przez specjalny układ nadajnika przedstawia rysunek 2.35. Po stronie odbiorczej systemu DS/SS odbiornik odbiera sygnał, demoduluje go i poddaje kluczowaniu używając tej samej sekwencji co nadajnik. Przedstawia to rysunek 2.36.



Rys.2.35. *Modulacja DS/SS*

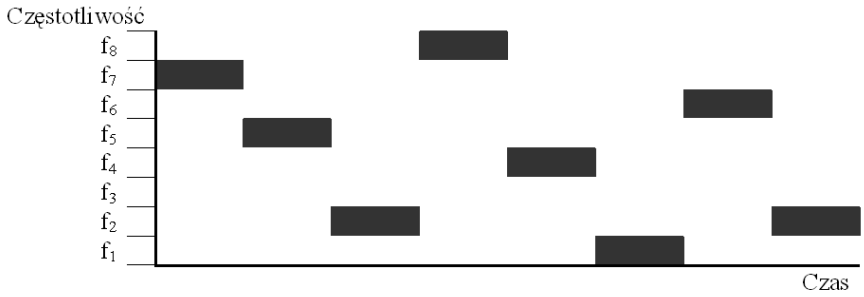


Rys.2.36. *Demodulacja DS/SS*

Najczęstrze zastosowania systemu DS/SS to system nawigacji satelitarnej GPS, telefony bezprzewodowe pracujące w paśmie 2,4 GHz, sieci WLAN w technologo WiFi zgodne

ze standardami IEEE 802.11 i IEEE 802.11b oraz sieci sensorowe ZigBee standardu IEEE 802.15.4.

Idea techniki FH/SS polega na tym, że pasmo dzielone jest na określoną liczbę kanałów. Nadajnik zmienia kanał zgodnie z założoną sekwencją pseudolosową co przedstawia rysunek 2.37.



Rys.2.37. *Modulacja FH/SS.*

Po stronie odbiorczej, aby poprawnie zdemodulować sygnał używana jest ta sama sekwencja pseudolosowa. Modulacja FH/SS umożliwia redundacyjne pokrycie wielu punktów dostępu i jest odporna na zakłócenia ale wymaga poprawnej synchronizacji odbiornika i nadajnika. W przypadku interferencji na jednej częstotliwości wymagane jest powtórzenie transmisji pakietu. Najczęstrze zastosowania to BlueTooth standard IEEE 802.15.1 sieci bezprzewodowe standardu IEEE 802.11 oraz systemy wojskowe.

Podsumowując, sygnały z rozproszonym (poszerzonym) widmem są to sygnały, w których oprócz przekształcenia za pomocą modulacji wąskopasmowej dokonuje się dodatkowego przekształcenia się tego sygnału wykorzystując ciąg pseudolosowy w celu N – krotnego poszerzenia widma sygnału (i tym samym zmniejszenia mocy w tym paśmie). N przyjmuje się typowo: z zakresu 100 do 10 000.

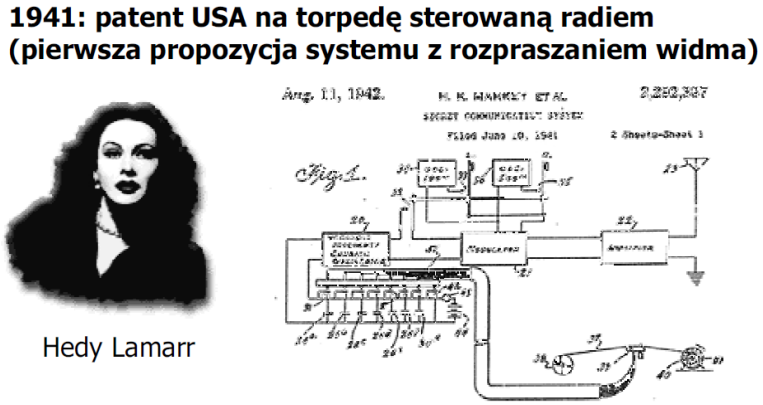
Zaletą tych systemów są ich właściwości:

- przesyłane wiadomości są trudne do przechwycenia
- niski poziom mocy i charakter przesyłanych sygnałów powoduje, że są one łatwe do ukrycia,
- sygnały są odporne na zakłócenia celowe i propagację wielodrożną,
- w jednym kanale częstotliwościowym mogą być przesyłane sygnały wielu użytkowników.

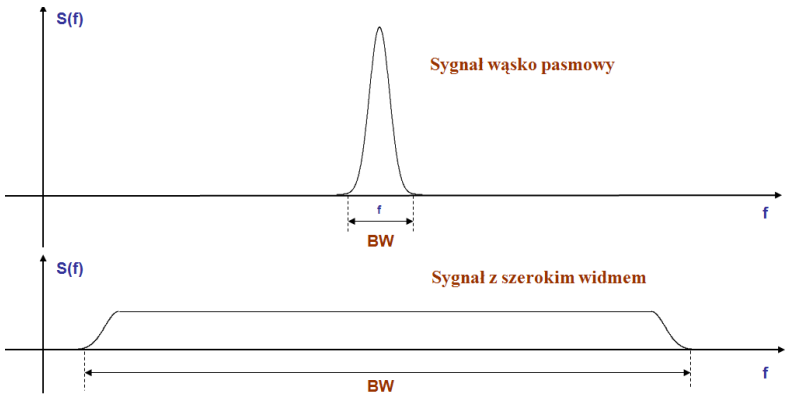
System CDMA w porównaniu do systemów FDMA i TDMA nie ma ściśle określonej liczby użytkowników wykorzystujących jednocześnie system – ze wzrostem

liczby użytkowników korzystających jednocześnie z systemu rośnie poziom zakłóceń, automatycznie, w łagodny sposób ograniczając ich liczbę.

Ciekawostką systemów z rozproszonym widmem jest fakt, że pierwszy patent dla takiego systemu wykorzystywanego do radiowego sterowania torpedą „Secret Communication System" – patent numer 2292387, system FH/SS, uzyskali gwiazda filmu aktorka Hedy Lamarr i pianista George Antheil. Rysunek 2.38 przedstawia projekt rozwiązania systemu z rozpraszaniem widma zgłoszonego w Urzędzie Patentowym USA a rysunek 2.39 przedstawia widmo sygnału CDMA.



Rys.2.38. *Systemy z rozproszonym widmem.*

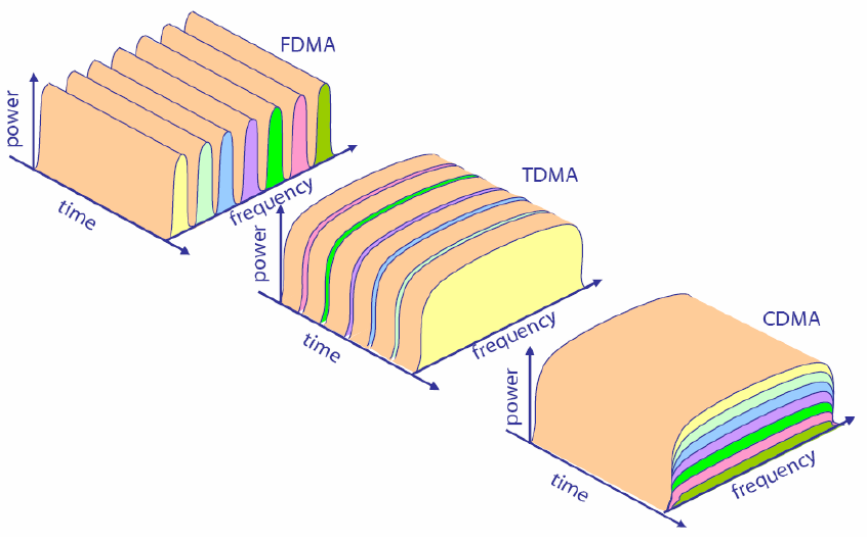


Rys.2.39. *Widmo sygnału CDMA*

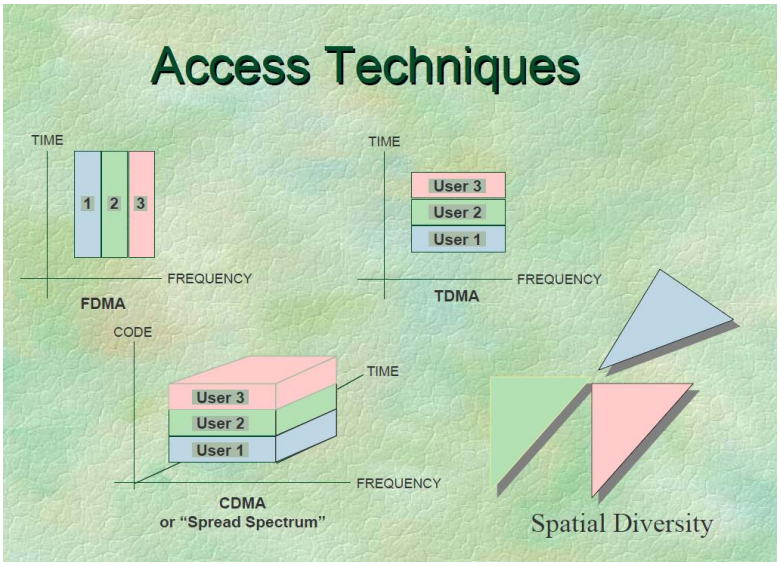
Podsumowując, należy stwierdzić, że do najczęściej spotykanych metod zwielokrotnienia pojedynczych kanałów informacyjnych w traktach przewodowych, światłowodowych, radiowych i satelitarnych należą:

– częstotliwościowe FDM,
– czasowe TDM,
– kodowe CDM,
– przestrzenne SDM.

Podział ten przedstawiono na rysunku 2.40 a na rysunku 2.41 pokazano wymienione wyżej techniki zwielokrotnienia łącznie z SDM.



Rys.2.40. *Zasady dostępów FDMA, TDMA i CDMA.*

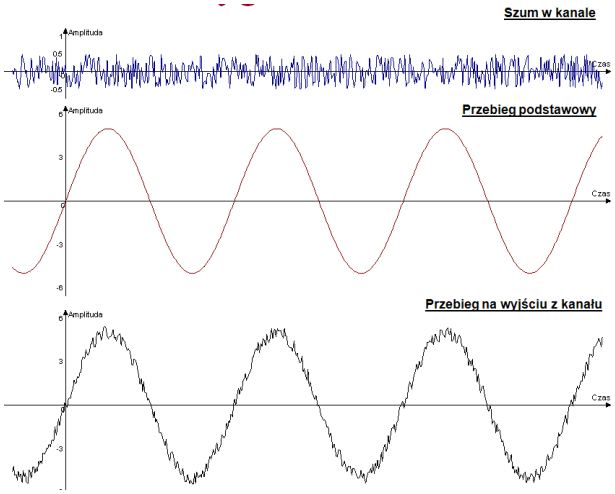


Rys.2.41. *Podstawowe techniki dostępu do medium transmisyjnego.*

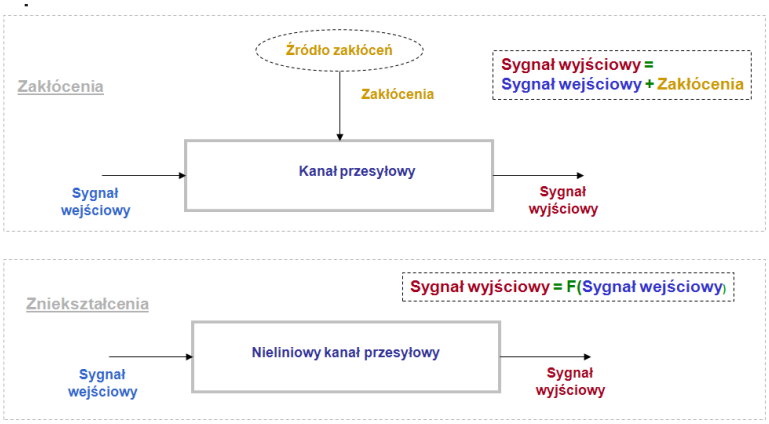
Zwielokrotnienie przestrzenne SDM *(Space Division Multiplexing)* – sposób umożliwiający powielanie toru transmisyjnego, łącznie z urządzeniami wejścia i wyjścia, często stosowane w łączach satelitarnych, w systemach GSM – celem podniesienia redundancji przekazu. W wielu obecnie stosowanych systemach multipleksacji sygnałów zwykle są łączone dwie różne metody zwielokrotnienia, dając złożony obraz sygnału wyjściowego o dużej przepływności binarnej.

2.5. Zakłócenia transmisji.

Jedną z głównych przyczyn powstawania błędów w torach telekomunikacyjnych są zakłócenia sygnału w torze telefonicznym. W linii telefonicznej występują dwa rodzaje zakłóceń: **addytywne**, związane z szumem cieplnym, zakłóceniami przemysłowymi, atmosferycznymi i przesłuchami od innych kanałów oraz **multiplikatywne**, wynikające ze zmiany parametrów kanału. Inaczej niż w zakłóceniach addytywnych zwiększenie mocy sygnału użytecznego nie zmniejsza wpływu zakłóceń multiplikatywnych. Więc, zakłócenia sygnału telekomunikacyjnego są to niepożądane przebiegi (sygnały) występujące razem z przebiegiem (sygnałem) użytecznym pochodzące z innych źródeł niż sygnał. Ze względu na źródło zakłóceń dzielą się na: zakłócenia atmosferyczne powstałe w wyniku wyładowań; zakłócenia energetyczne powstałe w wyniku pracy urządzeń elektrycznych (np. silniki komutatorowe); zakłócenia przenikowe związane z przenikiem energii pomiędzy różnymi drogami przesyłowymi. Ze względu na miejsce powstania zakłócenia dzielą się na: zakłócenia własne (np. szum cieplny, zakłócenia komutacyjne); zakłócenia obce (np. zakłócenia atmosferyczne, energetyczne, przenikowi, szum otoczenia). Ze względu na czas trwania zakłócenia dzielą się na: trwałe (np. energetyczne); impulsowe (nietrwałe – przemijające np. zakłócenia atmosferyczne). Innym problemem związanym z transmisją sygnału są **zniekształcenia sygnału.** Zniekształcenie sygnału telekomunikacyjnego jest to niezamierzone odchylenie kształtu (przebiegu) sygnału od jego pierwotnej postaci wywołane niepożądanymi właściwościami drogi przesyłowej (np. za wąskie pasmo), na którą nie oddziałuje żadne inne źródło energii poza źródłem sygnału. Zniekształcenia sygnału dzielą się na: zniekształcenia linearne – tłumieniowe i fazowe (opóźnieniowe); zniekształcenia nielinearne – powodujące powstanie nowych składowych (harmonicznych) widma sygnału. Oczywistym jest, że ze wzrostem krotności systemów zwielokrotniania, wydłużania toru zwiększa się jego tłumienność. **Tłumienność toru** charakteryzuje tor telekomunikacyjny pod względem jego przydatności do transmisji długodystansowej i zdolności do przekazywania mocy pozornej. Tłumienie (wzmocnienie) jest wyrażane logarytmem stosunku dwu mocy pozornych: doprowadzonej do toru i wydzielonej na impedancji obciążenia. Jednostką w jakich to wyrażamy jest decybel (dB) czyli 1/10 jednostki podstawowej znanej jako Bell [B]. Wpływ szumu w kanale na sygnał analogowy przedstawia rysunek 2.43.

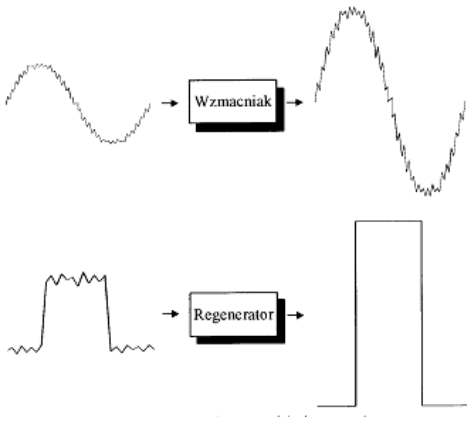


Rys.2.43. *Zakłócenia sygnału w kanale.*



Rys.2.44. *Zakłócenia i zniekształcenia sygnału*

Aby wyeliminować negatywny wpływ tłumienności na przesyłany sygnał pomiędzy stacją nadawczą i odbiorczą musimy „włożyć" urządzenia które będą przywracały właściwy poziom sygnału. Takimi urządzeniami w systemach analogowych są **wzmacniaki**, a w traktach cyfrowych **regeneratory**. Porównanie efektów ich działania przedstawia rysunek 2.45.



Rys.2.45. *Porównanie efektów działania wzmacniaka i regeneratora.*

Z powyższego rysunku wynika podstawowa zaleta systemów cyfrowych w porównaniu do systemów analogowych. W systemach analogowych wzmacniak przywraca właściwy poziom sygnału zakłóconego (wzmacnia sygnał użyteczny i zakłócający) czyli jeśli zakłócenie „wpadło" w trakt to już go nie można wyeliminować. W systemach cyfrowych zakłócenie zmienia kształt impulsu a regenerator może przywrócić właściwy kształt impulsu i go wzmocnić.

3. Zintegrowane systemy łączności.

3.1. Wprowadzenie

Sieci telekomunikacyjne stanowią część infrastruktury państwa. Zasadniczą i największą częścią tych sieci jest publiczna sieć telekomunikacyjna, świadcząca powszechne usługi dla dowolnego abonenta. Abonenci sieci publicznej są bardzo zróżnicowani: od najprostszego abonenta jakim jest abonent telefoniczny domowy do bardziej skomplikowanego technicznie i usługowo jakim jest centrala telefoniczna należąca do przedsiębiorstwa. Poza publiczną siecią telekomunikacyjną istnieją telekomunikacyjne sieci wydzielone, nazwane również prywatnymi. Oczywiście, sieci wydzielone współpracują z publiczną siecią telekomunikacyjną. Z wielkości i powszechności publicznych sieci telekomunikacyjnych państwa oraz międzynarodowej współpracy sieci publicznych wynika, że podstawowe standardy techniczne i usługowe na sieci telekomunikacyjne są narzucane przez sieć publiczną. W publicznych sieciach telekomunikacyjnych wyróżnia się ze względów technicznych i eksploatacyjnych sieci telefoniczne, telegraficzne, teleinformatyczne, sieci radiokomunikacji ruchomej, sieci łączy radiofonicznych i telewizyjnych. W wyżej wymienionych usługowo - autonomicznych sieciach, instalowane są różne podsystemy usługowe, np. systemy teletekstowe i telefaksowe w sieciach telefonicznych. Sieci i systemy są usługowo niezależne, chociaż wykorzystują wspólne zasoby transmisyjne i komutacyjne.

Podstawową funkcją klasycznej telekomunikacji jest transport informacji na drodze elektromagnetycznej. Z dotychczas przedstawionych materiałów wynika, że w współczesnych systemach informacyjnych, znacząco wzrasta rola przetwarzania informacji. Różnorodność usług niefonicznych wynikająca z zapotrzebowania na szybką komunikację w systemie „człowiek-maszyna", wymaga ścisłego współdziałania na poziomie procedur między źródłami; generacji informacji, punktami odbioru i systemami transportu informacji. Powoduje to zwiększenie zakresu usług

współczesnej telekomunikacji i jej ścisłego powiązania z systemami komputerowymi – głównymi elementami źródeł i ujść informacji.

Sprostanie takim zadaniom jest możliwe tylko w przypadku utworzenia jednolitej sieci telekomunikacyjnej świadczącej wszystkie rodzaje usług telekomunikacyjnych.

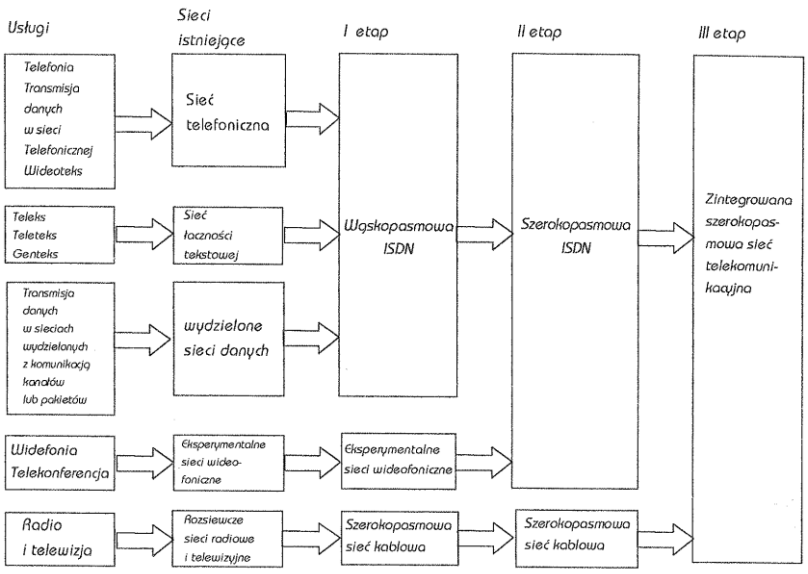
Taką sieć można było zrealizować dopiero przy odpowiednim poziomie rozwoju metod cyfrowego przesyłania mowy. Obecnie telekomunikacja zmierza do jednolitej sieci cyfrowej z integracją usług tzw. sieci wąskopasmowej N - ISDN *(Narrow Integrated Services Digital Network)* i sieci szerokopasmowych B - ISDN *(Broadband ISDN)*, informatyka rozwija metody rozproszonego przetwarzania, obie te dziedziny *(teleinformatyka)* zmierzają do oprogramowania opartego na językach postprocedualnych i systemach ekspertowych.

W ostatnich latach rozważane są koncepcje telekomunikacyjnych sieci inteligentnych drugiej generacji IN/2 *(Intelligent Network)* budowane z wykorzystaniem technicznych sieci ISDN.

3.2. Sieci cyfrowe

Rozwój cyfrowych sieci telekomunikacyjnych dokonuje się poprzez wykorzystanie techniki półprzewodnikowej, światłowodów i optyki zintegrowanej dla transmisji i komutacji. Wybór strategii rozwoju sieci cyfrowych sprowadza się do wyboru właściwych metod komutacji i związanych z nimi metod transmisji i sygnalizacji, Każda strategia musi w pierwszym rzędzie uwzględniać obecny stan sieci telekomunikacyjnej, a w szczególności interesy właścicieli sieci. Z tego punktu widzenia jest oczywiste, że dochodzenie do sieci zintegrowanej usługowo będzie musiało się odbywać na drodze ewolucji dostatecznie długotrwałej, aby zamortyzowały się olbrzymie nakłady zainwestowane w istniejące sieci.

Proces przejścia od stanu obecnego do sieci docelowej przedstawiony jest na rys. 3.1.



Rys.3.1. *Etapy integracji sieci telekomunikacyjnej.*

Dotychczasowy rozwój publicznej sieci telekomunikacyjnej jest zdominowany przez telefonię. Z tej dominującej roli telefonii wynika główne założenie dla koncepcji CCITT dotyczące sieci IDN, w której za podstawę przyjęto komutację synchronicznych, dwukierunkowych kanałów cyfrowych o przepustowości 64 kb/s.

Nowe usługi telekomunikacyjne z punktu widzenia planowania cyfrowych sieci zintegrowanych charakteryzują się następującymi właściwościami:

- przyszły "abonent zintegrowany" będzie posługiwał się terminalami pracującymi z bardzo rożnymi szybkościami transmisji;
- należy się liczyć z różnymi formatami sygnałów w poszczególnych usługach;
- w obecnej sieci telekomunikacyjnej przeważają połączenia "punkt-punkt" pomiędzy dwoma abonentami charakteryzujące się wymianą informacji w obu kierunkach o zbliżonej objętości. Nowe usługi mają odmienne cechy ruchowe. Objętość informacji wymieniona w obu kierunkach połączenia jest bardzo różna. Coraz więcej będzie połączeń "punkt-wiele punktów", oraz "wiele punktów - punkt".

Obecna, powszechna komutowana sieć telefoniczna PSTN przekształcana jest w sieć cyfrową z kanałami PCM o przepływności 64 kbit/s dla transmisji i komutacji. Cyfryzacja sieci prowadzi do cyfrowej sieci zintegrowanej technicznie (pod względem techniki) IDN *(Intergreated Digital Network)*. Zastosowanie cyfrowej techniki transmisyjnej i komutacyjnej powoduje zasadnicze zmiany w strukturze hierarchicznej sieci i metodach jej eksploatacji. Zmiany te dotyczą nie tylko zasad komutacji, ale również organizacji systemu węzłów komutacyjnych i systemów teletransmisyjnych. W systemie sieci telekomunikacyjnych w pierwszej kolejności cyfrowe centrale są

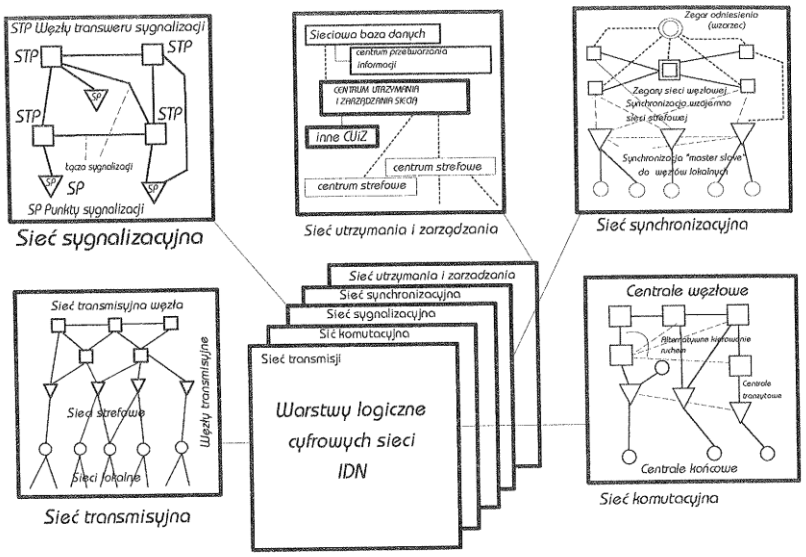
stosowane na wyższych poziomach hierachii sieci: w centralach tranzytowych i międzymiastowych. Centrale końcowe są instalowane w drugiej kolejności. Wynika to ze względów technicznych i ekonomicznych. Strategia przejścia z dotychczasowej sieci telefonicznej na sieć cyfrową nie polega jedynie na zastosowaniu nowego sprzętu komutacyjnego i transmisyjnego. Tworzenie telekomunikacyjnej sieci cyfrowej powoduje istotne zmiany w strukturze sieci, planie numeracji, technicznych zasadach taryfikacji oraz metodach utrzymania i zarządzania siecią. Aby ewolucyjnie dokonać tego przejścia, uzasadnione jest wykonanie w pierwszej kolejności zmian na poziomie central tranzytowych. Komputerowe sterowanie w tych węzłach umożliwia ruchową reorganizację sieci magistralnej oraz implementację komputerowych, scentralizowanych systemów utrzymania i zarządzania siecią. Ucyfrowienie sieci lokalnej i central końcowych wiąże się z innymi trudnościami. Najwięcej jest central końcowych, a analogowe doprowadzenia abonenckie stanowią bardzo duży majątek sieci. W sieciach IDN zakłada się pozostawienie dotychczasowych analogowych doprowadzeń abonenckich. Wobec tego, elektroniczne centrale końcowe różnią się znacznie od central tranzytowych. W centralach tranzytowych "abonentem" jest wielokrotny strumień cyfrowy, dość łatwo sprzężony z cyfrowym polem komutacyjnym.

W centralach końcowych, sprzężenie z cyfrowym polem komutacyjnym musi być poprzedzone zastosowaniem koncentratorów, które mają dwa podstawowe zadania:

- konwersję analogowych sygnałów z linii abonenckich na sygnały cyfrowe z modulacją PCM;
- koncentrację łączy abonenckich na cyfrowe wielokrotne strumienie do pola komutacyjnego.

W wyniku zastosowania:

- cyfrowej międzycentralowej sieci transmisyjnej,
- węzłów komutacyjnych z cyfrowymi polami komutacyjnymi, sterowanymi programowo,
- scentralizowanego systemu sygnalizacji CCITT Nr 7,
- zmian strukturalnych sieci telekomunikacyjnej ukształtowała się logiczna struktura sieci cyfrowych jak na rys. 3.2.



Rys.3.2. *Logiczna struktura sieci cyfrowych.*

W cyfrowej sieci typu IDN można wyróżnić następujące warstwy logiczne:

1. Międzycentralową sieć transmisyjną odpowiedzialną za tworzenie dróg transportu informacji i użytkowników w kanałach podstawowych o przepływności 64 kb/s. Sieci teletransmisyjne mogą być samodzielnie rekonfigurowane bez udziału central komutacyjnych.
2. Sieć węzłów komutacyjnych, sterowanych programowo, dla komutacji cyfrowych kanałów o przepustowości 64 kb/s.
3. Autonomiczną sieć sygnalizacyjną. Dla sieci cyfrowych przewidziany jest scentralizowany system sygnalizacji CCITT Nr 7. Kanał sygnalizacyjny ma przepustowość 64 kb/s; fizycznie tworzony jest w szczelinach sygnalizacyjnych (szczelina 16) cyfrowych traktów PCM o przepływności 2 Mb/s.
4. Autonomiczna sieć synchronizacji węzłów. Integracja techniczna sieci z zastosowaniem techniki cyfrowej dla transmisji i komutacji wymaga zastosowania synchronizacji nie stosowanej w klasycznych sieciach analogowych z przestrzennymi polami komutacyjnymi. Cyfrowe pola komutacyjne central muszą pracować synchronicznie. Dla realizacji tych wymagań zegary węzłów sieci są wzajemnie powiązane w sieć synchroniczną.
5. Sieć utrzymania i zarządzania. Rozproszona struktura central końcowych oraz wprowadzenie metod alternatywnego sterowania ruchem w sieci uzasadnia centralizację zarządzania i utrzymania sieci, tworzone są centra eksploatacji technicznej (CET – *Centrum Eksploatacji Technicznej*) obejmujące co najmniej kilka central. Centra CET są ze sobą powiązane w sieć zarządzania i utrzymania.

Komunikacja między węzłami CET tworzona jest zwykle na kanałach sygnalizacyjnych sieci sygnalizacyjnej, jednak logicznie jest to sieć wydzielona.

Opisany sposób przebudowy sieci telekomunikacyjnej w sieć IDN jest uzasadniony ekonomicznie nawet przy założeniu wyłącznie usług telefonicznych. Dokładniejsza analiza możliwości takiej sieci: szybka komutacja porównywalna z komutacją w sieciach pakietowych, efektywny system sygnalizacji wywołują uzasadnione pytania, dlaczego tak zbudowana sieć ma przenosić wyłącznie ruch telefoniczny. Sieć IDN daje techniczne uzasadnienie dla integracji usług dla ewolucyjnego przejścia do sieci ISDN.

3.3. Sieci ISDN.

Zgodnie z koncepcją zintegrowanej usługowo, cyfrowej sieci telekomunikacyjnej ISDN *(Integrated Services Digital Network)* określoną przez CCITT jest to wielousługowa sieć rozwinięta z cyfrowej sieci telefonicznej typu IDN, zapewniająca cyfrowe połączenia od terminala do terminala 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.

Podstawowe cechy określające ISDN to:

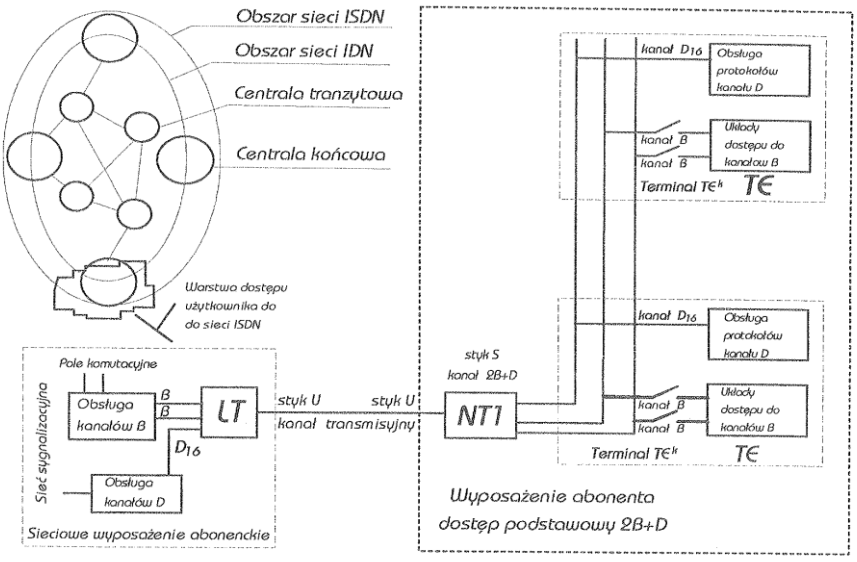
1. Sieć uniwersalna podkładowa, integrująca usługi z pasma telefonicznego i pozatelefonicznego. Zakłada się ograniczony zbiór interfejsów ,,użytkownik-sieć" i ograniczony zbiór usług podstawowych transportu informacji (np. komutacja kanałów, komutacja pakietów).
2. Powinny być realizowane połączenia komutowane i niekomutowane dla różnorodnych usług telekomunikacyjnych. Połączenia mogą być komutowane metodą komutacji kanałów i komutacji pakietów; należy preferować połączenia komutowane;

   z przepływnością 64 kb/s.
3. ISDN będzie naturalną ewolucją sieci telefonicznej zintegrowanej technicznie IDN poprzez wprowadzenie nowych usług np. realizowanych w sieciach wydzielonych oraz poprzez standaryzację cyfrowego dostępu użytkownika do sieci. Ewo1ucyjne przejścia od sieci IDN do sieci ISDN przedstawia rys. 3.3. Zewnętrzna warstwa sieci ISDN stanowi rozwinięcie możliwości usługowych sieci IDN. Fizycznie, rozwinięcie to polega na budowie cyfrowych standardowych łączy informacyjnych

do użytkowników; użytkownikami będą zarówno terminale abonenckie jak i inne wydzielone sieci (np. sieci pakietowe). Realizacja funkcyjna sieci wielousługowej wymaga stworzenia standardowych metod programowanego dostępu do sieci w łączu informacyjnym użytkownika i odpowiednio rozszerzonego oprogramowania w węzłach końcowych i tranzytowych. Sieć IDN, tworzona obecnie w wielu krajach, jest etapem pośrednim między PSTN *(Public Switched Telephone Network - powszechna komutowana sieć telefoniczna)* a przyszłą siecią ISDN, rozumianą jako wąskopasmowa sieć wielofunkcyjna. Przez wąskopasmową sieć rozumie się sieć o podstawowym kanale 64 kb/s w odróżnieniu od sieci szerokopasmowych B-ISDN o kanałach rzędu Mb/s. Dla jednolitej analizy koncepcji i protokołów ISDN przyjęto model odniesienia RM *(Reference Model)* oparty na koncepcji i zasadach modelu odniesienia ISO/CCITT OSI. Podstawowe cechą modelu RM-ISDN jest rekursywne zastosowanie siedmiowarstwowej struktury systemów otwartych OSI w modelowaniu dwóch rodzajów przepływu informacji:

- użytkownika U (user)
- sterujących C (control)

Pojęcie "użytkownik" jest szerokie i obejmuje zarówno prosty terminal abonencki, inne sieci (sieci wydzielone, centrale PBX, sieci LAN), jak również wyposażenia utrzymaniowe
i zarządzające sieci ISDN.

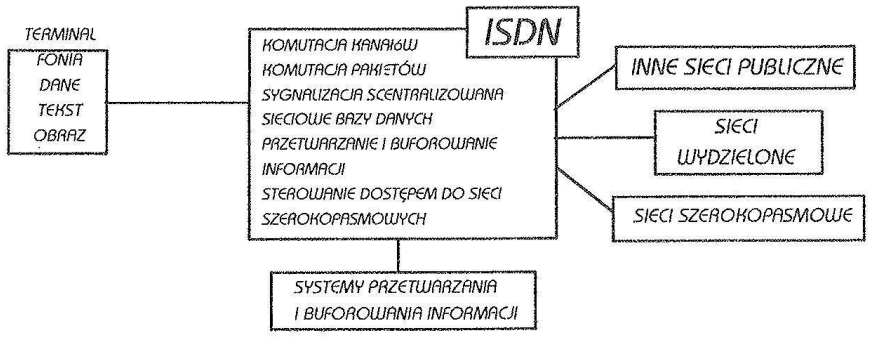


Rys.3.3. *Przejście od sieci IDN do ISDN.*

Charakterystyczne dla sieci ISDN są następujące zagadnienia:

1. Komutacja kanałów. Podstawową szybkością w kanale będzie 64 kb/s, chociaż są przewidziane inne szybkości, wielokrotne z szybkością podstawową. Komutacja kanałów jest uznana za efektywną metodę komutacji dla usług w czasie rzeczywistym (fonia) oraz dla przekazywania dużych porcji informacji. W ISDN, sterowanie komutacją kanałów odbywać się będzie przy użyciu sygnalizacji scentralizowanej.
2. Komutacja pakietów. Zakłada się szybkość transmisji 64 kb/s z możliwością wykorzystania większych szybkości. Komutację pakietów stosować się będzie do pracy interakcyjnej jest to usługa komplementarna do komutacji kanałów.
3. Svgnalizacja scentralizowana. Będzie używana do ustanawiania, nadzorowania i rozłączania połączeń w systemie komutacji kanałów w usługach fonicznych i niefonicznych.
4. Zarządzanie bazami danych. Sieciowe bazy danych będą niezbędne dla efektywnego i zunifikowanego zarządzania usługami fonicznymi i niefonicznymi oraz sprzętem dla tych usług.
5. Przetwarzanie i buforowanie informacji. Integralną częścią ISDN są wyposażenia dla przetwarzania i buforowania informacji, np. wyposażenia dla takich usług telematycznych, jak: teletekst, videotex, poczta elektroniczna, systemy dystrybucji wiadomości MHS *(Message Handling System)*, telefaks.
6. Sterowanie dostępem do sieci szerokopasmowych. Powszechnie uznaje się, że analogowe sieci szerokopasmowe o pasmach rzędu 6 do 10 MHz lub cyfrowe o przepływnościach kilkadziesiąt lub kilkaset Mb/s stosowane w wideokomunikacji ruchomych obrazów i szybkiej komunikacji międzykomputerowej pozostaną przez bardzo długi czas jako wydzielone z ISDN, drogi transportu informacji użytkowych, jednakże procesy sterujące (dostęp użytkowników do tych sieci) mogą być implementowane w jednolity sposób w sieci ISDN.

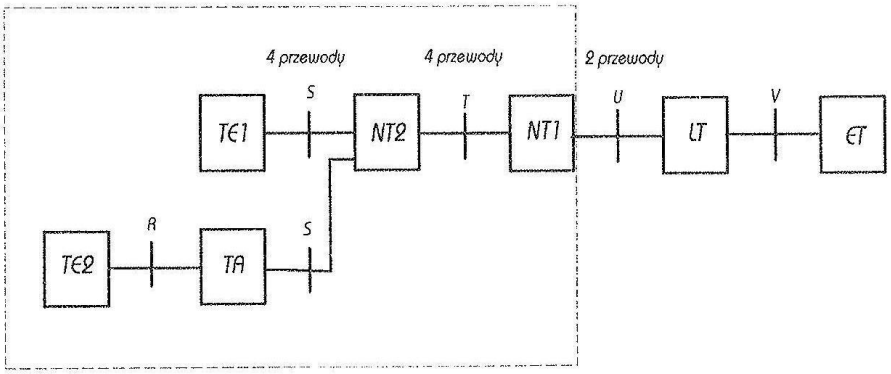
Opisane środowisko ISDN przedstawione jest na rys. 3.4.



Rys.3.4. *Środowisko sieci ISDN*

Styk użytkownika z siecią.

Aby umożliwić przyłączanie do sieci zintegrowanej różnych urządzeń końcowych, wytworzonych przez rożnych producentów, w rożnych. krajach, CCITT znormalizowało ograniczoną liczbę styków użytkownika z siecią. Styki te określają zarówno punkty dostępu do sieci, jak i funkcje realizowane przez urządzenia stykowe. Schemat dostępu użytkowników do sieci ISDN przedstawia rys. 3.5. Linią przerywaną obwiedziono przekroje znormalizowane przez CCITT. Przekrój U, przez łącze cyfrowe między wyposażeniem liniowym centrali ISDN a użytkownikiem, nie jest znormalizowany międzynarodowo, podobnie jak tradycyjne analogowe łącze telefoniczne.



Rys.3.5. *Struktura styków użytkownika z siecią ISDN.*

ET – zakończenie centralowe,

LT – zakończenie liniowe,

NT – zakończenie sieciowe,

TA – adapter terminalowy,

TE – urządzenie końcowe.

Adapter sieciowy NTl *(Network Termination)* spełnia następujące funkcje związane z fizycznym i elektromagnetycznym stykiem z siecią:

- zakończenie transmisyjne łącza,
- liniowe funkcje utrzymaniowe i nadzór,
- synchronizacja i ramkowanie,
- przekazywanie zasilania łącza abonenckiego,
- konwersja struktury ramkowej liniowej na standardową,
- zakończenie od strony styku.

Adapter sieciowy NT2 może pełnić funkcje multipleksowania, komutacji, sterowania urządzeniami końcowymi. Realizuje także funkcje utrzymaniowe. Przykładami adaptera NT2 mogą być: centrala abonencka, sieć lokalna LAN, sterownik urządzeń końcowych.

TE 1 *(Terminal Equipment)* jest typowym urządzeniem końcowym ISDN, a TE2 urządzeniem końcowym nie mającym styku zgodnego z zaleceniami dotyczącymi ISDN. TE2 jest przyłączony do sieci ISDN za pośrednictwem adaptera TA *(Terminal Adapter)* dokonującego konwersji odpowiednich protokołów.

Między opisanymi jednostkami funkcjonalnymi znajdują się przekroje T, S oraz R. Niektóre jednostki funkcjonalne mogą być połączone razem w jedną całość. Na przykład połączenie NT 1 i NT 2 powoduje wyeliminowanie styku T, a połączenie TE z NT 2 lub TA z NT 2 wyeliminowanie styku S. TE 1 lub TA mogą być bezpośrednio przyłączone do NT 1 - w takim przypadku styki S i T pokrywają się.

Fizyczny styk w przekrojach S lub T może mieć jedną z następujących struktur:

- struktura dostępu podstawowego *(Basic Rate Acces)*; zawiera dwa kanały B o przepływności 64 kb/s i jeden kanał D (2 B + D), przy czym kanał D ma przepływność 16 kb/s;
- struktury dostępu pierwotnego *(Primary Rate Acces)*, zawierają 23 (USA i Japonia) lub 30 kanałów B i jeden kanał D o przepływności 64 kb/s (23B + D) lub (30D + D);
- struktury dostępu pierwotnego częściowego nPRA (n x B + D) czyli n kanałów B o przepływności 64 kb/s i kanał D również o przepływności 64 kb/s.

W przypadku użycia struktury 2B + D z kanałów B można korzystać niezależnie tzn. rożne urządzenia końcowe użytkownika mogą pracować jednocześnie. W sytuacjach gdy dostęp 2B + D nie zezwala na zorganizowanie konkretnego systemu

wspomagania zarządzania np. Gminne Centrum Zarządzania Kryzysowego (za mała przepływność) a zastosowanie dostępu 30B + D (PRA) są nieracjonalne (zbyt duże koszty eksploatacji) można zastosować dostęp pierwotny częściowy nPRA (dostęp pierwotny częściowy) czyli nB + D (n razy 64 kb/s + 64 kb/s). Koszty takiego dostępu są dużo niższe niż dostępu PRA. Przykładem takiego rozwiązania jest dostęp 6B + D stosowany dla transmisji sygnału programu pierwszego Polskiego Radia z studiów nagraniowych w Warszawie do Centrum Nadawczego w Solcu Kujawskim tzw. „kanał H0" zapewniający przepływność 384 kb/s + 64 kb/s.

W rzeczywistości sumaryczna przepływność kombinacji kanałów B, D oraz H jest większa niż by to wynikało z sumowania wartości podanych wyżej, ponieważ należy uwzględnić bity synchronizacyjne.

Sieci szerokopasmowe.

1. Najważniejsze cechy sieci B-ISDN

Skrót B-ISDN *(Broadband Integrate Services Digita1 Networks)* oznacza szerokopasmową sieć cyfrową z integracją usług, w której informacje przesyłane są z dużą szybkością w postaci komutowanych pakietów danych, mowy, obrazów ruchomych

i nieruchomych. Sieci B-ISDN udostępniają użytkownikowi (abonentowi) transmisyjny styk cyfrowy o bardzo dużej przepływności (155 Mb/s i większej), pozwalający na realizację wielorakich usług (telefonicznych, teledacyjnych oraz video) za pośrednictwem jednego tylko kanału. Przykładem szerokopasmowych usług teledacyjnych może być transfer dużych zbiorów między komputerami oraz połączenia między sieciami lokalnymi (LAN). W zakresie usług związanych z przetwarzaniem obrazów i usług video należy się liczyć, w przyszłości z dużym zapotrzebowaniem na takie zlecenia, jak: przesyłanie filmów i danych z bibliotek video, zdalne nabywanie towarów, zdalne gry video, video konferencje itp. Dla zapewnienia tego typu usług muszą być tworzone w sieci drogi przesyłowe o bardzo dużych przepływnościach. Tworzenie takich dróg zapewnia synchroniczna hierarchia systemów cyfrowych SDH *(Synchronous Digital Hierarchy)*.

Wielość usług oferowanych abonentowi wymaga różnych przepływności występujących w tym samym punkcie dostępu do sieci. Zaistniała zatem potrzeba opracowania metody komutacji informacji zawartych w strumieniach o różnej przepływności.

W sieci B-ISDN zastosowano niekonwencjonalną metodę komutacji, opartą na technice zwanej asynchronicznym trybem transferu ATM *(Asynchronous Transfer Mode)*, w założeniu której jest ujednolicenie postaci komutowanej informacji dla wszystkich usług.

Różnice między siecią zintegrowaną (ISDN) wąskopasmową i szerokopasmową (B-ISDN) dotyczą zarówno punktów dostępu użytkownika do sieci jak też dróg transportu informacji i metod łączenia.

Różnice te można określić następująco:

a) wąskopasmowa sieć ISDN umożliwia użytkownikowi dostęp do kanałów o z góry określonej przepływności, np. 64 kb/s (kanał B) i 16 kb/s (kanał D); w B-ISDN przepływność punktu styku użytkownik - sieć jest bardzo duża (155 Mb/s lub 622 Mb/s) i tworzone są kanały wirtualne w zależności od zapotrzebowania na usługę bez konieczności wcześniejszego wyboru przepływności kanału;
b) w wąskopasmowej ISDN wykorzystuje się istniejące abonenckie łącza jednotorowe oparte na kablach miedzianych symetrycznych, zaś w B-ISDN stosuje się wyłącznie kable światłowodowe;
c) w wąskopasmowej ISDN są stosowane systemy komutacyjne z komutacją kanałów telefonicznych, a tylko w przypadku kanałów używanych dla sygnalizacji stosuje się komutację pakietów, natomiast w B-ISDN wyłącznie komutację pakietów.

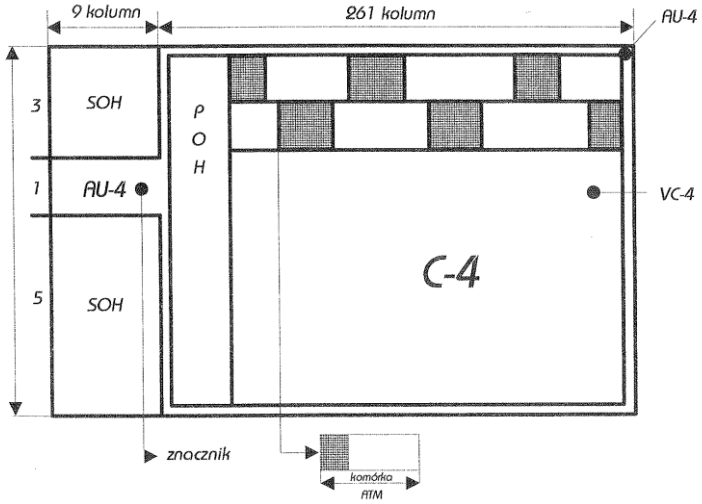
2. Technika transmisji w sieciach B-ISDN

Przesyłanie komórek ATM w sieci odbywa się w sposób ciągły, komórki są przesyłane jedna za drugą. Między komórkami informacyjnymi przesyła się komórki dla potrzeb zarządzania i utrzymania (OAM). Są one wtrącane do strumienia ATM co 26 komórkę. Przepływność użyteczna takiego sygnału jest równa 149,760 Mb/s.

Jak już wspomniano, do realizacji dróg transportu komórek ATM CCITT preferuje synchroniczną hierarchię systemów cyfrowych. Pierwszy człon tej rodziny stanowi synchroniczny moduł transportowy STM-1 o przepływności liniowej 155,520 kb/s. Moduł ten może być zwielokrotniany w sposób synchroniczny do modułu STM-4 o przepływności 622 Mb/s, a ten zaś do modułu STM-16 o przepływności 2,56 Gb/s. Parametry i struktura tej rodziny systemów zostały określone w zaleceniach CCITT: G.707-G. 709, G.781-G. 784 oraz G.957 i G.958.

Ramka modułu STM-1 stanowi ramkę bazową dla całej hierarchii, dzięki czemu możliwy jest prosty dostęp do sygnałów przenoszonych przez system oraz prosta

operacja multipleksacji i demultipleksacji. Sygnałami wejściowymi (pierwotnymi) dla modułu STM-1 mogą być również sygnały systemów plezjochronicznych o przepływnościach 2, 34 oraz 140 Mb/s. Strukturę ramki modułu STM-1 pokazano na rysunku 3.9. Jest ona przedstawiona w postaci tablicy bajtów zawierającej 9 rzędów i 270 kolumn. Pierwsze 9 kolumn tworzy nagłówek sekcji i zwielokrotnienia (SOH) oraz znacznik tzw. jednostki administracyjnej AU-4, natomiast kolumna dziesiąta zawiera bajty nagłówka drogi przesyłowej (POH). Pozostałe 260 kolumn (stanowiące tzw. kontener C4) zawierają bajty przeznaczone do transferu informacji użytkowej.



Rys.3.9. *Struktura ramki modułu STM – 1.*

Należy zaznaczyć, że struktura ramki STM-1 jest identyczna zarówno w przypadku transmisji strumieni ATM, jak i transmisji konwencjonalnych strumieni plezjochronicznych. Jedyną różnicą jest to, że kontener C-4 zawiera w pierwszym przypadku komórki ATM, natomiast w drugim przypadku – bajty sygnałów plezjochronicznych. Daje to możliwość stosowania tego samego systemu transmisyjnego w obecnej sieci plezjochronicznej jak i w przyszłej sieci B-ISDN.

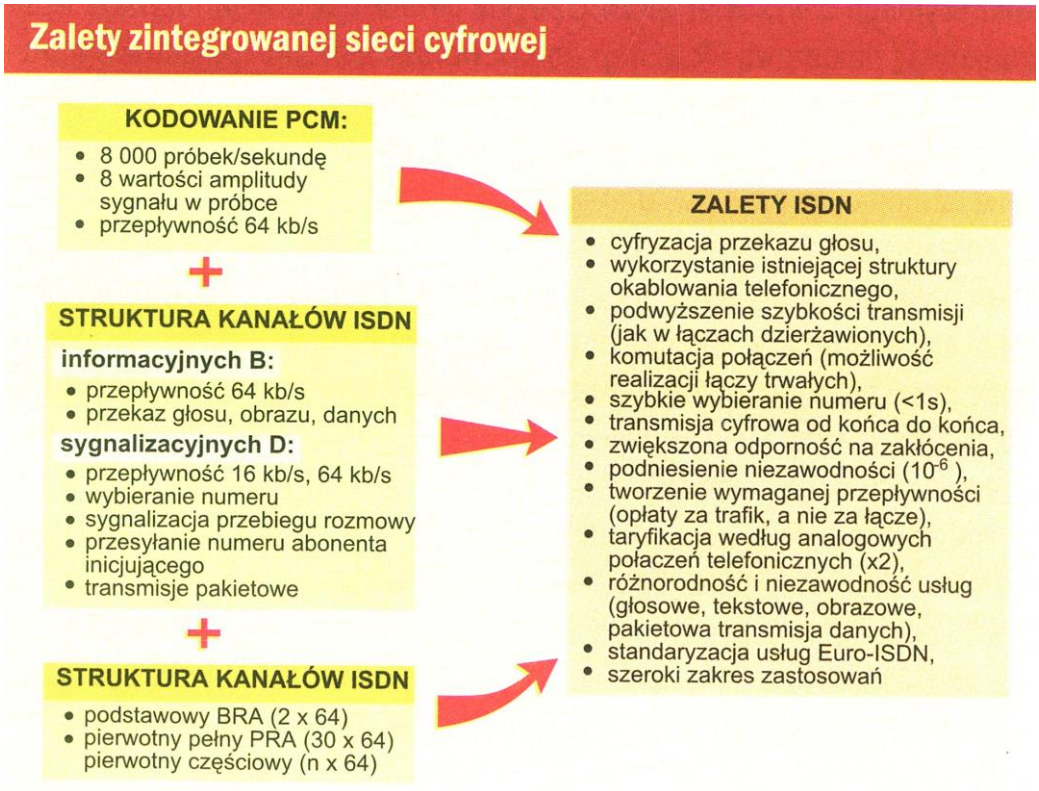
Transmisja dużej liczby sygnałów szerokopasmowych wymaga przepływności znacznie większych niż 155 Mb/s. W obecnym stadium rozwoju SDH są znormalizowane przez CCITT, jak już wspomniano, moduły transmisyjne o przepływnościach 622 Mb/s (STM-4) i 2,5 Gb/s (STM-16).

Rozwój technologii optoelektronicznej oraz nowych technik transferu informacji dał podstawę do ujednolicenia sieci telekomunikacyjnej zapewniającej wszystkie usługi, tj. budowę sieci B-ISDN.

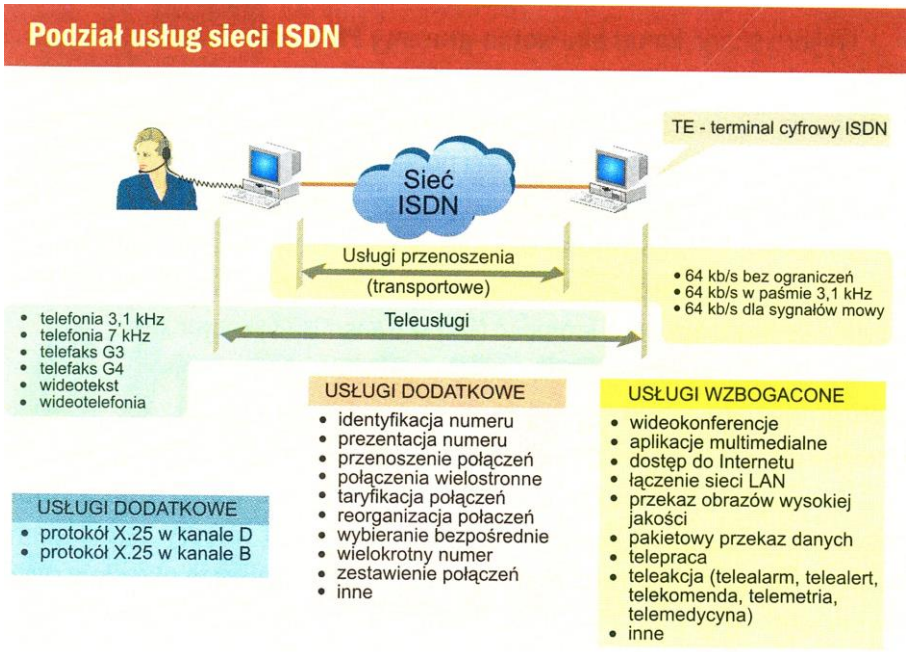
Sieci B-ISDN są tworzone na podstawie asynchronicznej zasady transferu (ATM) i systemów transmisyjnych o zwielokrotnieniu synchronicznym (SDH). ATM zapewnia efektywne wykorzystanie całkowitej przepustowości kanału transmisyjnego. Systemy SDH pozwalają budować elastyczne sieci z możliwością przełączania dróg transportu informacji.

Zastosowanie kabli światłowodowych w łączach abonenckich umożliwia dostęp abonentów do sieci szerokopasmowej. Dokonana przez CCITT standaryzacja punktu styku abonenta z węzłem sieci zapewnia ogólnoświatową jednolitość sprzętu.

Zalety zintegrowanej sieci cyfrowej przedstawiono na rysunku 3.11 a dostępne w systemie usługi z podziałem na grupy: przenoszenia (bazowe), teleusługi, usługi dodatkowe i wzbogacone przedstawia rysunek 3.12.



Rys.3.11. *Zalety zintegrowanej sieci cyfrowej*



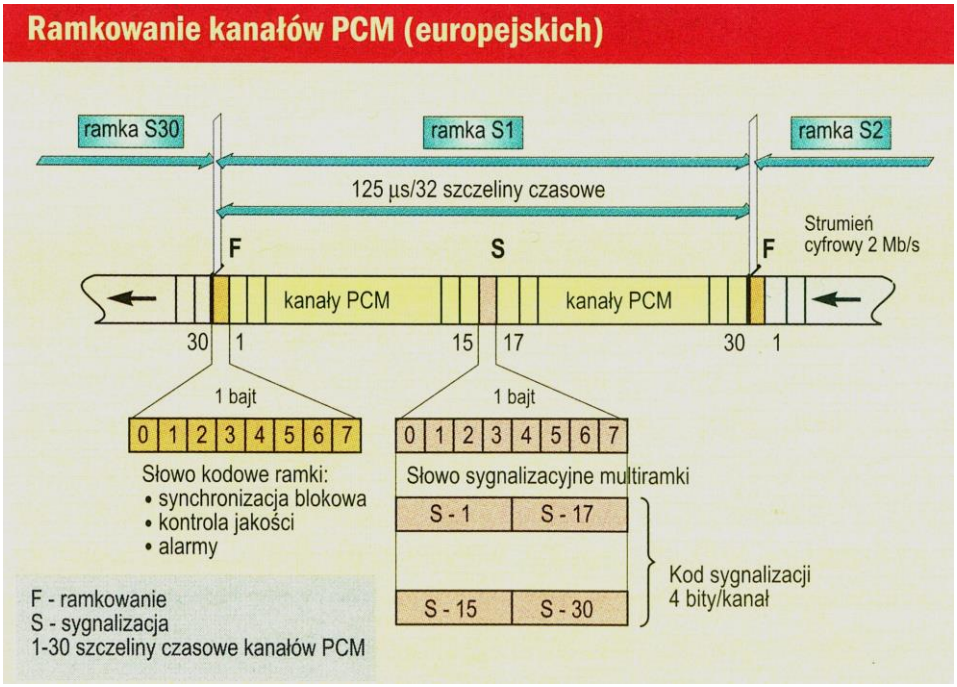
Rys.3.12. *Podział usług sieci ISDN*

Przykłady najczęściej stosowanych usług dodatkowych przedstawia rysunek 3.13.

Usługi dodatkowe ISDN

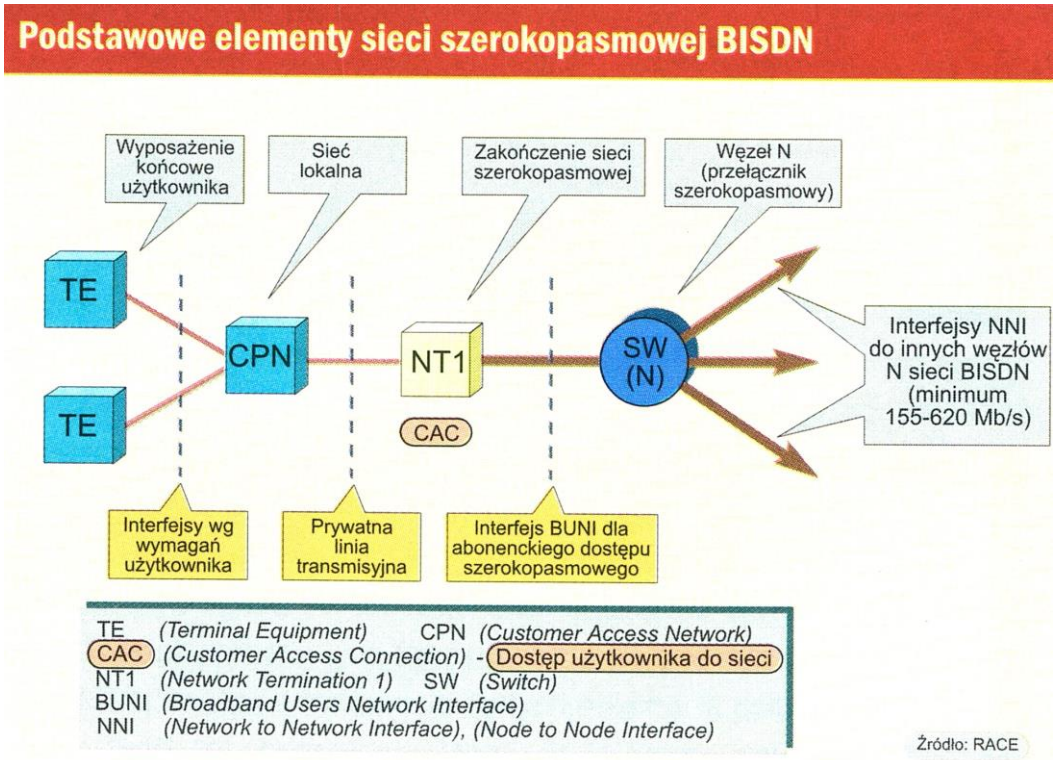
Skrót	Nazwa usługi	Opis
CLI	Calling Line Identification	identyfikacja numeru linii wywołującej
CLIP	Calling Line Identification Presentation	prezentacja numeru łącza wywołującego
CLIR	Calling Line Identification Restriction	blokada prezentacji numeru łącza wywołującego
CLIRO	Calling Line Identification Restriction Override	omijanie blokady prezentacji numeru łącza wywołującego
COL	Connected Line Identification	identyfikacja numeru łącza osiągniętego
COLP	Connected Line Identification Presentation	prezentacja numeru łącza osiągniętego
COLR	Connected Line Identification Restriction	blokada prezentacji numeru łącza osiągniętego
COLRO	Connected Line Identification Restriction Override	omijanie blokady prezentacji numeru abonenta przyłączonego
DDI	Direct Dialing In	wybieranie bezpośrednie. Łączy abonentów zewnętrznych z numerami wewnętrznymi bez pośrednictwa operatora
MSN	Multiple Subscribe Number	uwielokrotniony numer abonenta. Przypisuje różne numery urządzeniom dostępu podstawowego
MCI	Malicious Call Identification	identyfikacja złośliwych wywołań
SUB	Subadressing	subadresacja. Nadaje adresy urządzeniom podrzędnym
CD	Call Diversion	przenoszenie przychodzących wywołań na inny numer
CFB	Call Forwarding on Busy	przekierowanie połączenia w przypadku zajętości
CFNR	Call Forwarding No Replay	przekierowanie połączenia w przypadku braku odpowiedzi
CFU	Call Forwarding Unconditional	bezwarunkowe przekierowanie połączenia
CD	Call Deflection	przekierowanie przez terminal połączeń przychodzących
CH	Call Hold	podtrzymanie wywołania. Pozwala abonentowi zawiesić bieżące połączenie, wykonać inne i powrócić do pierwotnego
CW	Call Wait	informacja o połączeniu oczekującym. Informuje abonenta o nowym wywołaniu, podczas gdy oba kanały B są zajęte
CCBS	Call Completion to Busy Subscriber	automatyczne oddzwonienie do zajętego abonenta
CUG	Closed User Group	zamknięta grupa użytkowników. Umożliwia tworzenie grup z ograniczonym dostępem
AOC	Advice of Charge	automatyczna informacja o. opłatach
UUS	User-to-User Signalling	sygnalizacja użytkownik – użytkownik
TP	Terminal Portability	przenośność terminalu. Pozwala abonentowi zawiesić aktywne połączenie i wykonać inną czynność
OCB	Outgoing Call Barring	blokada wywołań wychodzących
IFC	Inhibition of Incoming Forwarded Calls	blokada dla wywołań przychodzących przekierowanych
CI	Call Interception	przechwytywanie wywołań. Pozwala operatorowi sieci przechwycić połączenie, które nie może być zrealizowane
CONF	Conference	połączenie konferencyjne

Rys.3.13. *Usługi dodatkowe ISDN*



Rys.3.14. *Europejskie ramkowanie kanałów PCM*

Rysunek 3.14 przedstawia europejskie ramkowanie kanałów PCM, rysunek 3.15 przedstawia podstawowe interfejsy sieci B-ISDN.



Rys.3.15. *Podstawowe interfejsy sieci szerokopasmowej B-ISDN*

Tabela 3.1 *Europejska hierarchia wielokrotnych systemów cyfrowych PCM*

Określenie systemu	Liczba kanałów 64 kb / s		Przepływność sygnału grupowego [kb/s]
	telefonicznych	synchronizacyjno - sygnalizacyjnych	
2 Mb/s	30	2	2048
8 Mb/s	120	4	8448
34 Mb/s	480	8	34368
140 Mb/s	1920	16	139264
560 Mb/s	7680	32	564922

4. Propagacja fal radiowych

4.1. Łączność radiowa

Zaletą kanału telefonicznego jest jego, w zasadzie nieograniczona długość, istotną zaś wadą – konieczność stosowania linii przewodowych. Wykorzystanie pewnych zjawisk towarzyszącym drganiom elektrycznym pozwala jednak na wysyłanie wiadomości zawartej w sygnałach elektrycznych w otwartą przestrzeń (filozoficzny XIX - wieczny „eter") pozbawioną przewodów łączących nadawcę z odbiorcą. Odbywa się to podobnie jak przy wytwarzaniu dźwięku, a więc przez spowodowanie falowego rozprzestrzeniania się zaburzeń w równowadze otaczającej przestrzeni, jednakże nie w mechanicznej równowadze cząstek powietrza, jak to miało miejsce przy przesyłaniu dźwięku, lecz w elektrycznej i magnetycznej równowadze przestrzeni. To jest właśnie istotą łączności radiowej.

Takie idealne stany równowagi w otaczającym nas świecie praktycznie nie istnieją, ale upraszczając zagadnienie można je sobie wyobrazić w ten sposób, że gdy na przykład cząstki powietrza znajdują się w bezruchu, to znaczy, że nie są poruszane żadnymi siłami, wówczas ciśnienie powietrza jest stałe (idealna cisza akustyczna). Analogicznie możemy sobie wyobrazić podobną „ciszę" elektromagnetyczną, która polega na tym, że na ładunki elektryczne lub ciała magnetyczne umieszczone gdzieś w przestrzeni nie działają żadne siły, dzięki czemu są one nieruchome.

Taką „ciszę" elektromagnetyczną można zakłócić za pomocą urządzenia przedstawionego w lewej części rysunku 4.1. Urządzenie to składa się ze źródła prądu zmiennego (nazwanego nadajnikiem) i dołączonych do niego dwóch przewodów (zwanych anteną nadawczą).

Dzięki działaniu nadajnika do obu części anteny dopływają na przemian ładunki elektryczne o przeciwnych znakach – dodatnie i ujemne. Inaczej mówiąc płynie w nich prąd elektryczny o zmiennym kierunku: w górę (na rys. 4.1 – strzałka ciągła) lub w dół (strzałka przerywana). W otoczeniu anteny powstają wtedy siły elektryczne i magnetyczne, wytwarzają się tzw. pola elektryczne i magnetyczne.

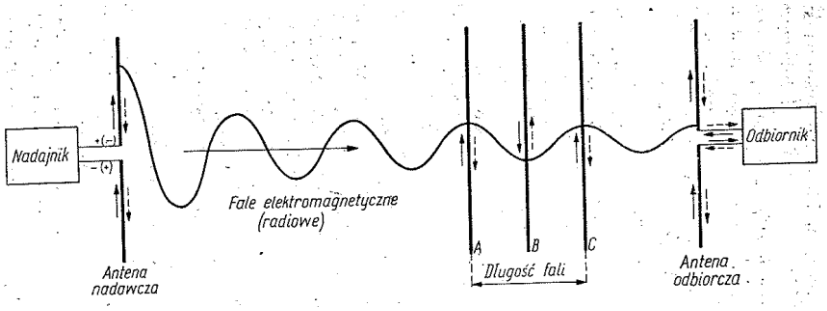
Takie połączone pola elektryczne i magnetyczne tworzą pole elektromagnetyczne o bardzo cennych właściwościach. Rozprzestrzenia się ono na bardzo duże odległości z szybkością światła (300 tysięcy kilometrów na sekundę) i może powodować ruchy ładunków elektrycznych, które napotyka na swej drodze. Zjawisko takie nazywamy falami radiowymi.

Jeżeli teraz w pewnej odległości od anteny nadawczej umieścimy przewód A (rys.4.1), w którym, jak wiadomo, ładunki elektryczne mogą się łatwo poruszać, to zaobserwujemy, że ruch ładunków w nim będzie miał taki sam charakter jak w antenie nadawczej, tj. w górę i w dół, a więc powstanie przepływ prądu zmiennego analogicznie jak w antenie nadawczej. Przesuwając wspomniany przewód nieco dalej można znaleźć miejsce **B**, w którym prądy płynące w nim będą miały w danej chwili przeciwny kierunek. Przesuwając z kolei jeszcze dalej omawiany przewód znajdziemy miejsce **C**, w którym będą znów takie same kierunki prądów. Ładunki elektryczne będą poruszały się w górę i w dół w przewodach **A**, **B** i **C**, podobnie jak trzy korki znajdujące się na powierzchni wody, wtedy gdy dojdą do nich fale spowodowane przez jakieś zakłócenie równowagi wody w pobliżu.

Ruch ten będzie się odbywał w pewnej chwili w punktach **A** i **C** równocześnie w górę, zaś w punkcie **B** w dół, następnie w punktach **A** i **C** w dół, a w punkcie **B** w górę. W przestrzeni rozchodzą się fale, powodujące ruchy ładunków elektrycznych, a odległość między miejscami, w których mają one taki sam kierunek nazywa się **długością fali.**

Jeżeli prąd płynący w antenie nadawczej ma stałą częstotliwość zmian kierunku, a więc płynie w danym kierunku zawsze co pewien okres czasu (okres drgań), to siły elektryczne i magnetyczne wytwarzane w otoczeniu przez antenę mają taki sam kierunek również po tym okresie. W miejscu, w którym znajduje się wspomniany przewód A, będą powstawały fale o zgodnych kierunkach również co pewien taki sam okres czasu. Fala, która działa w punkcie **C**, przed takim właśnie okresem czasu działała w punkcie **A**, a więc odcinek drogi równy „długości fali" przebyła ona w czasie równym okresowi drgań nadajnika.

Zatem częstotliwość drgań nadajnika określa, ile takich okresów mieści się w jednej sekundzie, a więc, ile takich odcinków przebyła fala w ciągu jednej sekundy. Ponieważ w ciągu jednej sekundy fala przebywa odległość 300 milionów metrów, więc dzieląc tę liczbę przez częstotliwość można obliczyć długość fali. Częstotliwość na ogół wygodniej jest określać w milionach okresów na sekundę (megahercach – **MHz**) i wtedy dzieląc 300 przez liczbę megaherców otrzymuje się długość fali w metrach. Na przykład częstotliwości 30 MHz odpowiada długość fali 10 m, zaś częstotliwości 100 MHz – długość fali 3 m.



Rys.4.1. *Wykres ilustrujący nadawanie i odbiór fal radiowych*

W prawej części rysunku 4.1 przedstawione jest praktyczne wykorzystanie zjawiska wytwarzania prądu w odcinku przewodu pod wpływem działania fal radiowych. Antena odbiorcza stanowi przewód przecięty w środku i połączony w miejscu przecięcia z odbirnikiem. Prądy płynące w obydwóch połówkach anteny przepływają również przez odbiornik, w którym mogą być wykorzystane do usprawnienia procesu informacyjnego.

Błędem byłoby jednak przypuszczać, że można w ten sposób przesyłać drogą radiową energię elektryczną stosowaną np. do oświetlenia. Fale radiowe słabną bowiem znacznie w miarę wzrostu odległości od nadajnika i jeśli odległość ta będzie zbyt duża nie odbierzemy żadnego sygnału. Słabe prądy wzbudzone w antenie odbiorczej mogą być wzmocnione za pomocą układów elektronicznych (lampowych bądź tranzystorowych) do takiej wartości, że można rozpoznać treść wiadomości przesyłanych z nadajnika.

Aby jednak fale radiowe przenosiły jakąś wiadomość, np. mowę, muszą być od niej w pewien sposób uzależnione, podobnie jak np. prąd płynący w obwodzie telefonicznym od mikrofonu do słuchawki. Najprostszym rozwiązaniem wydawałoby się doprowadzenie do anteny nadawczej drgań elektrycznych bezpośrednio z mikrofonu. (Prąd płynący w antenie odbiorczej zmieniałby się wtedy tak samo i po wzmocnieniu przepływając przez słuchawkę mógłby wytwarzać dźwięk. Trudność

w zrealizowaniu takiej łączności radiowej wynika z własności anten nadawczych i odbiorczych.

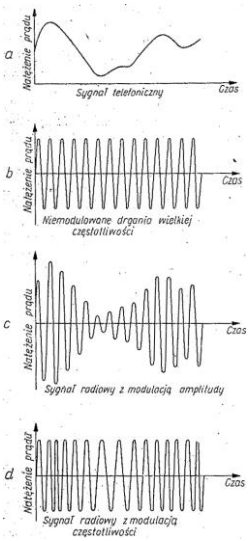
Anteny takiego typu, jak przedstawione na rys. 4.1, powinny mieć całkowitą długość obu połówek równą połowie długości fali. Są to tzw. dipole półfalowe. Wtedy drgania elektryczne wytwarzają się w nich łatwo i mają dużą moc. Dla fal o innej długości, które odpowiadają drganiom o innej częstotliwości, wzbudzenie drgań w antenie jest znacznie trudniejsze.

W antenie występuje więc rezonans dla pewnej częstotliwości drgań elektrycznych, podobny do rezonansu struny instrumentu muzycznego, która drgając wytwarza dźwięki o pewnej częstotliwości (wysokości tonu), zależnej od długości struny, a trudno poddaje się drganiom o innej częstotliwości. Często spotyka się anteny, w których zamiast dolnej połówki dołącza się uziemienie, metalową obudowę radiostacji (radiotelefonu), nadwozie samochodu lub kilka poziomych prętów metalowych. Antena taka zwana anteną ćwierćfalową działa zupełnie podobnie jak antena półfalowa, a jest często wygodniejsza do zamocowania.

Gdybyśmy chcieli wykonać antenę ćwierćfalową dla częstotliwości odpowiadającej mowie, np. 1000 Hz, to łatwo obliczyć, że musiałaby ona mieć wysokość 75 kilometrów, ponieważ długość fali dla drgań o takiej częstotliwości wynosi 300 km. Jest to, oczywiście, niemożliwe i dlatego drogą radiową możemy przekazywać tylko drgania o znacznie większych częstotliwościach, co odpowiada falom krótszym.

Na rysunku 4.2 przedstawiono w postaci wykreślnej sposób, w jaki można wykorzystać drgania elektryczne o wielkiej częstotliwości do przekazywania drgań mowy, tj. drgań o małej częstotliwości. Rys. 4.2a (przedstawia znane już zmiany natężenia prądu w mikrofonie, zaś rys. 4.2b - natężenie prądu zmiennego wielkiej częstotliwości wytwarzanego w nadajniku.

Drgania elektryczne przedstawione na rys. 4.2b nie reprezentują jeszcze żadnej wiadomości, ale po pewnym przekształceniu, zwanym modulacją, mogą ją przenosić. Nazywamy je drganiami nośnymi (lub drganiami o częstotliwości nośnej), zaś falę radiową, która z nich powstaje, nazywamy falą nośną.



Rys.4.2. *Różne rodzaje sygnałów elektrycznych.*

Przed doprowadzeniem drgań nośnych do anteny nadawczej można spowodować zmiany wielkości (amplitudy) drgań zgodnie ze zmianami prądu w mikrofonie, a więc zgodnie z dźwiękami działającymi na mikrofon (rys. 4.2c). Prąd wytworzony w antenie odbiorczej będzie się zmieniał wtedy tak samo, przy czym w odbiorniku będzie można na podstawie jego zmian odtworzyć przekazywane dźwięki. Takie prądy zmienne o wielkiej częstotliwości i zmiennej w takt mowy amplitudzie nazywamy sygnałami radiowymi z modulacją amplitudy.

Można jednak zastosować inną metodę, a mianowicie zmieniać w niewielkich granicach częstotliwość prądu doprowadzanego do anteny nadawczej. W ten sposób powstają sygnały radiowe z modulacją częstotliwości (rys. 4.2d), które również mogą być wykorzystane do przekazywania wiadomości.

Na rysunku 4.2d widać, że gdy natężenie prądu w mikrofonie wzrasta, wzrasta również częstotliwość zmian prądu (krótsze okresy drgań). Przeciwnie, gdy prąd w mikrofonie jest mniejszy, częstotliwość nadawanych sygnałów jest również mniejsza (dłuższe okresy). Zmiany częstotliwości przedstawione na rysunku 4.2d są przesadnie duże. W rzeczywistości dla przekazywania wiadomości wystarczy tylko nieznacznie zmieniać częstotliwość.

Sygnały z modulacją częstotliwości mają bardzo istotną zaletę w porównaniu z sygnałami z modulacją amplitudy, która polega na znacznie mniejszej wrażliwości transmisji radiowej (radiotelefonicznej) na zakłócenia. Najczęściej występujące zakłócenia w odbiorze radiowym objawiają się w postaci szumów i trzasków, słyszanych równocześnie z odbieranymi wiadomościami. Zakłócenia te są wynikiem odbierania przez antenę odbiornika fal radiowych pochodzących z ubocznych źródeł.

Różne zjawiska elektryczne powstające w otoczeniu, jak np. wyładowania atmosferyczne, iskrzenie w silnikach elektrycznych itp. są przyczynami powstawania fal radiowych. Są to pewnego rodzaju zupełnie nieużyteczne, szkodliwe sygnały radiowe o różnych częstotliwościach. W przypadku, gdy takie sygnały zakłócające dochodzą do anteny odbiorczej równocześnie z sygnałem pożądanym, powodują zazwyczaj dodatkowe zmiany natężenia prądu (amplitudy drgań elektrycznych) w antenie. Zmiany te są na ogół nieregularne, chaotyczne.

Odbiornik przystosowany do odbioru sygnałów z modulacją amplitudy wytwarza w słuchawce dźwięki odpowiadając wszystkim zmianom amplitudy sygnału, a więc odpowiadające zmianom dokonanym z wyniku modulacji (dźwięki mowy) oraz odpowiadające zmianom wynikłym na skutek działania zakłóceń (trzaski, szumy). Natomiast odbiornik przystosowany do odbioru sygnałów z modulacją częstotliwości nie reaguje na zmiany amplitudy sygnału spowodowane przez zakłócenia, a dźwięki w słuchawce wytwarzane są tylko na podstawie zmian częstotliwości drgań, dokonanych w nadajniku.

Zakłócenia w odbiorze sygnałów radiowych są najsilniej odczuwane przy odbiorze słabych sygnałów, ponieważ wtedy nawet słabe zakłócenia są słyszane równie dobrze jak sygnał pożądany. Nadajniki radiowe (radiotelefonów), które z racji swej istoty muszą być urządzeniami małymi i nieskomplikowanymi, wytwarzają sygnały o niezbyt dużej mocy, kilka tysięcy razy mniejszej niż np. sygnały przeciętnych stacji radiofonicznych. Odbiorniki radiowe (radiotelefonów) muszą więc odbierać bardzo słabe sygnały.

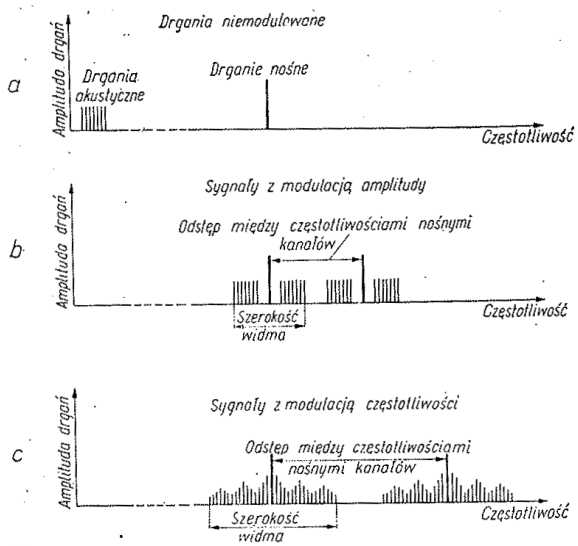
Dlatego modulacja częstotliwości w systemach radiokomunikacyjnych jest często stosowana. Dzięki niej odbiór jest na ogół wolny od zakłóceń, a zrozumienie przekazywanych wiadomości nie sprawia trudności użytkownikom, niemającym specjalnej wprawy w odbiorze radiowym.

Istotnym zagadnieniem, które wymaga z kolei wyjaśnienia, jest sposób skierowania wiadomości nadawanych przez radio do właściwego odbiorcy. Szybki rozwój zastosowań fal radiowych w ostatnich latach sprawił, że obecnie pracuje równocześnie ogromna liczba nadajników, nadających różnorodne sygnały radiowe przeznaczone do różnych celów. Duża liczba tych sygnałów radiowych dochodzi równocześnie do anteny odbiorczej, jednakże odbiorcę interesuje w danej chwili tylko jeden z nich, który jest przeznaczony dla niego.

Odbiornik musi więc odróżnić ten sygnał od innych i odtworzyć treść wiadomości, zawartą tylko w tym sygnale. Najistotniejszą cechą charakterystyczną sygnału radiowego, która pozwala na odróżnienie go od innych sygnałów, jest jego częstotliwość nośna. Jest to, jak już mówiliśmy, częstotliwość drgań wytworzonych w nadajniku, które następnie zostały zmodulowane drganiami małej częstotliwości otrzymanymi z mikrofonu.

Aby odebrać właściwy sygnał, trzeba więc znać jego częstotliwość nośną lub też długość fali, bo te dwie wielkości są ze sobą ściśle związane w znany już sposób. Fale radiowe o określonej częstotliwości nośnej, łączące między sobą nadajnik przystosowany do nadawania takich właśnie fal i odbiornik przystosowany do ich odbioru, tworzą kanał radiowy, za pomocą którego przekazywane wiadomości są kierowane do odbiorcy. Cechą rozpoznawczą kanału radiowego jest częstotliwość przekazywanych w nim sygnałów radiowych, która wymaga jednak pewnych dodatkowych wyjaśnień.

Wytworzone w nadajniku drgania o częstotliwości nośnej, jeszcze nie zmodulowane, przedstawione są na rys. 4.2b za pomocą wykresu o kształcie sinusoidy. Są to proste drgania o jednej, niezmiennej częstotliwości i stałej amplitudzie. Natomiast po dokonaniu modulacji nie mają one już przebiegu sinusoidalnego, lecz zmiany natężenia prądu są bardziej skomplikowane. Okazuje się, że mamy w tym przypadku do czynienia z sumarycznym działaniem większej liczby prostych drgań sinusoidalnych, o częstotliwościach nieco różniących się od częstotliwości nośnej.



Rys.4.3. *Szerokość widma częstotliwości sygnałów telefonicznych (niosących informację) i radiowych.*

Zjawisko to przedstawione jest na rys. 4.3 w postaci wykresów, na których w kierunku poziomym rozmieszczone są różne częstotliwości drgań, zaś w kierunku pionowym - ich amplitudy. Proste drgania sinusoidalne (niemodulowane) o pewnej częstotliwości nośnej zobrazowane są na rys. 4.3a pionową kreską, której wysokość jest proporcjonalna do ich amplitudy. W lewej części wykresu przedstawiona jest grupa drgań o małych częstotliwościach, reprezentujących różne dźwięki mowy.

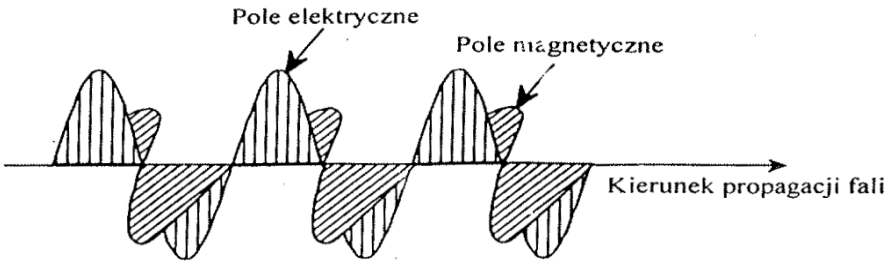
Drgania o częstotliwości nośnej po zmodulowaniu ich tymi drganiami akustycznymi „rozpadają" się jak gdyby na szereg drgań o mniejszych amplitudach i częstotliwościach, nieco większych lub nieco mniejszych od częstotliwości nośnej (rys. 4.3b,c). Cały ten zespół drgań nadawanych przez nadajnik nosi nazwę „widma" sygnału radiowego i ma pewną - „szerokość" w skali częstotliwości.

Sygnał radiowy zawierający jakąś wiadomość wniesioną do niego w wyniku modulacji składa się, jak widać, z większej liczby drgań o różnych częstotliwościach i wszystkie te drgania muszą być odebrane przez odbiornik, aby mógł on odtworzyć treść wiadomości. Odbiornik powinien więc odbierać nie tylko drgania o częstotliwości nośnej, ale również dodatkowo te drgania, których częstotliwości mieszczą się w pewnym paśmie w pobliżu częstotliwości nośnej.

Częstotliwości drgań wchodzących w skład innych sygnałów, które są przekazywane z innego nadajnika do innego odbiornika, muszą znajdować się poza tym pasmem. Częstotliwości nośne poszczególnych sygnałów muszą więc różnić się od siebie o pewną wartość częstotliwości, zwaną odstępem kanałów. Tylko wtedy odbiornik będzie mógł odróżnić te sygnały od siebie o nie będą się one mieszały ze sobą, a zatem różne nadajniki nie będą nawzajem przeszkadzały w odbiorze nadawanych przez nie wiadomości.

Na rys. 4.3b przedstawiono dwa widma sygnałów z modulacją amplitudy, zaś na rys. 4.3c dwa widma sygnałów z modulacją częstotliwości, obok siebie na skali częstotliwości. Na podstawie tego rysunku łatwo można dostrzec również pewną różnicę między tymi dwoma rodzajami modulacji. Różnica ta dotyczy szerokości widm sygnałów. Sygnały z modulacją częstotliwości mają z reguły widma szersze niż sygnały z modulacją amplitudy. W związku z tym odstępy częstotliwości między kanałami muszą być tu większe. Jest to wadą modulacji częstotliwości, ponieważ powoduje to trudności w rozdzieleniu kanałów radiowych między różne nadajniki pracujące równocześnie.

Reasumując, fala radiowa jest poprzeczną falą elektromagnetyczną *(TEM - Transverse Electro-Magnetic)* o dwóch wzajemnie do siebie prostopadłych składowych – elektrycznej **E** i magnetycznej **H**, a obie one są prostopadłe do kierunku rozchodzenia się (propagacji). W sensie praktycznym, większe znaczenie ma składowa elektryczna, łatwiejsze pomiary jej wielkości oraz od tego jak jest ona zorientowana w stosunku do powierzchni Ziemi mówimy o polaryzacji anteny (sygnału). Jeśli składowa **E** jest prostopadła do Ziemi to mamy polaryzację pionową, gdy równoległa to mówimy o polaryzacji poziomej. Są to dwa podstawowe typy polaryzacji anten co nie wyklucza innych rozwiązań np. stosowania polaryzacji kołowej w systemach satelitarnych. Aby te zagadnienia lepiej zrozumieć, trzeba jednak zapoznać się z niektórymi własnościami fal radiowych o różnych długościach, a więc różnych zakresach częstotliwości. Na szczęście literatura omawiająca te problemy jest bogata i łatwo dostępna.



Rys.4.4. *Poprzeczna fala elektromagnetyczna.*

4.2. Budowa atmosery

W otaczającej Ziemię atmosferze można wyróżnić kilka warstw o różnym stopniu zjonizowania powietrza. Są to:

- neutrosfera,
- jonosfera,
- egzosfera.

Neutrosfera zaczyna się od powierzchni Ziemi i rozciąga się do wysokości 60 km. Od powierzchni Ziemi do wysokości 10 ÷ 15 km rozciąga się troposfera. Warstwy zjonizowanego powietrza zaczynają występować na wysokości od 40 km do 60 km. Ten obszar jonosfery nazywany jest obszarem D. Podstawowa warstwa zjonizowanego powietrza występuje na wysokości powyżej 60 km. Jonosferę dzielimy na następujące obszary:

- obszar E (60 ÷ 200 km),
- obszar F (200 ÷ 500 km).

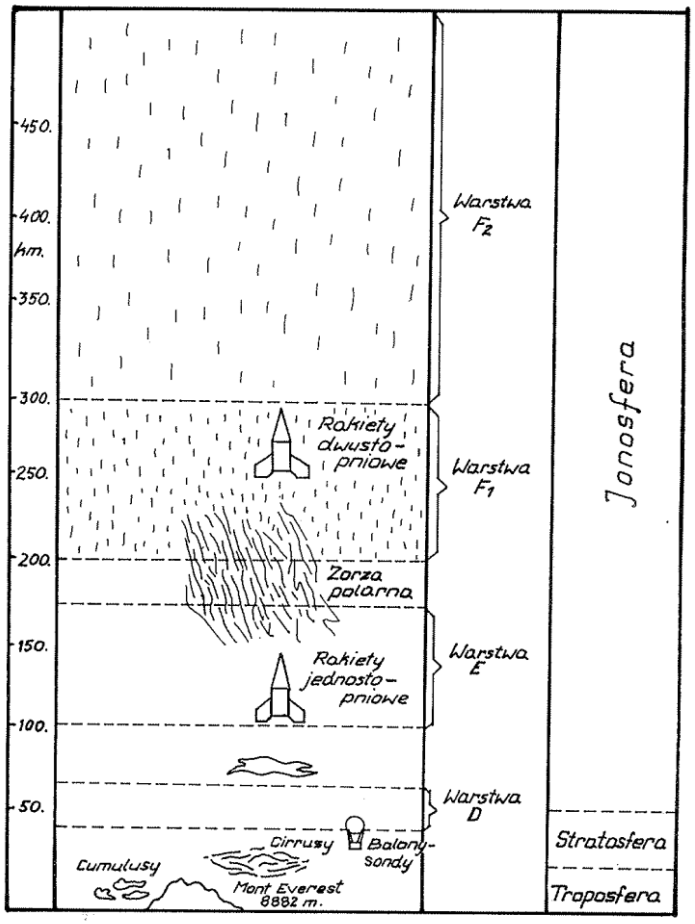
Obszar F dzieli się na:

- obszar F_1 (200 ÷ 300 km),
- obszar F_2 (300 ÷ 500 km).

Reasumując, z punktu widzenia łączności radiowej atmosferę ziemską dzielimy na trzy zasadnicze warstwy:

- troposferę.
- stratosferę,
- jonosferę.

Z punktu widzenia problemów propagacji najważniejsze z nich to warstwa najbliższa Ziemi – troposfera oraz jonosfera. Podział ten przestawia rysunek 4.5. a w tabeli 4.1 zawarto średnie wielkości stopnia jonizacji i okresów ich występowania.



Rys.4.5. *Atmosfera ziemska i jej podział.*

Tabela 4.1. *Regularne warstwy jonosfery*

Warstwa	Wysokość [km]	Max. gęst.elektr. [liczba elektronów/cm^3]	Uwagi
D	60 - 90	$2x10^2 – 7x10^2$	tylko w dzień
E	100 – 120	$4x10^4 – 12x10^4$ $5x10^3 – 1x10^4$	w dzień w nocy
F_1	150 – 180	$2,5x10^5 – 4x10^4$	w dzień – lato
F_2	250 – 400	10^6 $2x10^6$ $2x10^5$	w dzień – lato w dzień – zima w nocy

Z tabeli 4.1 wynika, że stopień jonizacji regularnych warstw jonosfery zmienia się zarówno ze względu na porę dnia, porę roku a również 11 – letniego okresu aktywności Słońca (zwiększona ilość plam słonecznych) zmieniających stopień jonizacji atmosfery ziemskiej (większy „wiatr" słoneczny. Problemy te muszą być uwzględnione w procesie projektowania systemu radiokomunikacyjnego.

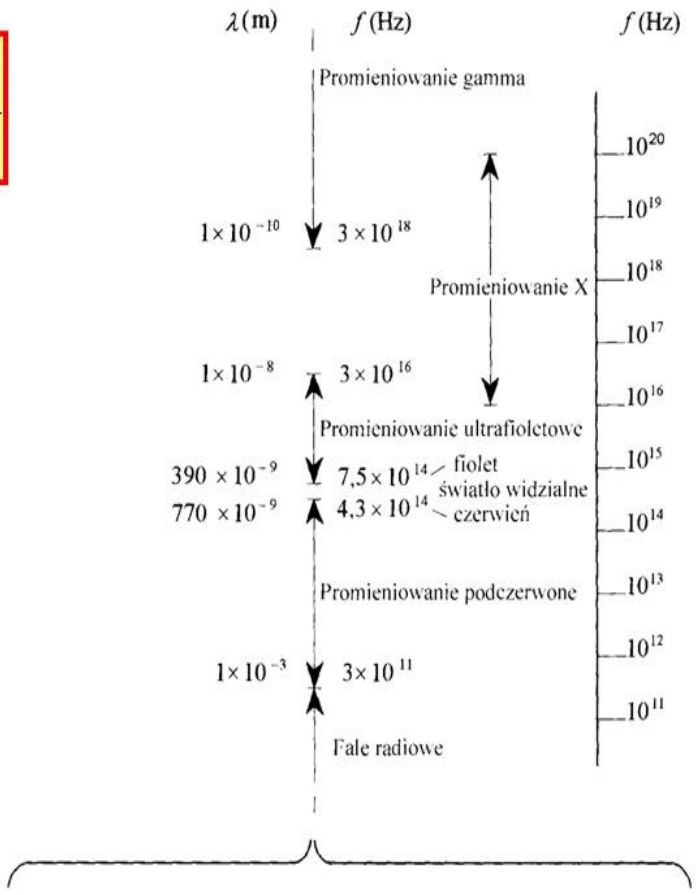
4.3. Podział widma częstotliwości radiowych na zakresy.

Cechą charakterystyczną każdego systemu radiokomunikacyjnego jest przekazywanie informacji przez ośrodek propagacji fal radiowych. W przeciwieństwie do urządzeń zarówno nadawczych jak i odbiorczych, droga przesyłania sygnałów w łączności radiowej jest w dużej mierze niezależna od człowieka. Przetwarzanie wiadomości i nadawanie sygnałów, a także ich odbiór i odtwarzanie zależą od układu i konstrukcji urządzeń przeznaczonych do tych celów; natomiast warunki propagacji fal radiowych są zależne od wielu czynników i okoliczności pozostających poza wpływem działania ludzkiego. W każdym miejscu, czasie i zakresie częstotliwości istnieją określone, w sensie statystycznym, warunki propagacyjne, których znajomość jest konieczna do optymalnego projektowania i wykorzystywania systemów radiokomunikacyjnych.

Zakres częstotliwości wykorzystywanych w systemach radiokomunikacyjnych jest bardzo szeroki i rozciąga się ods częstotliwości rzędu kilku kiloherców aż do częstotliwości optycznych. Stosunek największych do najmniejszuch częstotliwości wykorzystywanych obecnie w praktyce wynosi około 10^{10}. Konsekwencją bardzo dużej

szerokości względnej widma częstotliwości radiowych jest znaczne zróżnicowanie ich właściwości, zależnie od położenia w widmie.

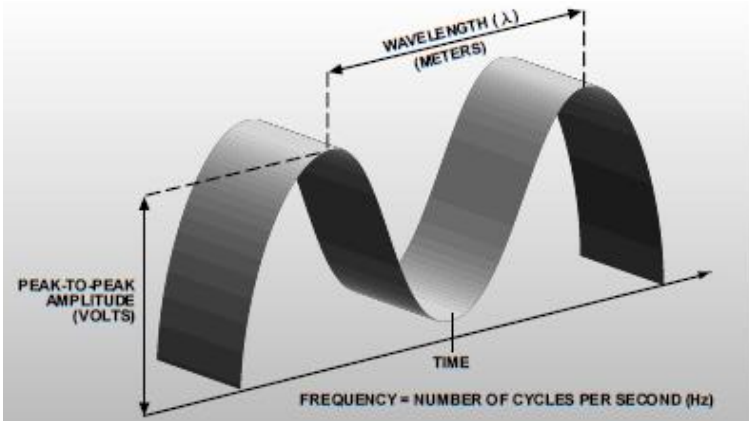
$$\lambda = \frac{c}{f}$$



Fale milimetrowe	EHF	30 - 300	GHz
Fale centymetrowe	SHF	3 - 30	GHz
Fale decymetrowe	UHF	0,3 - 3	GHz
Fale metrowe	VHF	30 - 300	MHz
Fale dekametrowe	HF	3 - 30	MHz
Fale hektometrowe	MF	0,3 - 3	MHz
Fale kilometrowe	LF	30 - 300	kHz
Fale myriametrowe	VLF	3 - 30	kHz

Rys.4.6. *Widmo promieniowania elektromagnetycznego.*

W podsumowaniu tego akapitu należy stwierdzić, że falę elektromagnetyczną jednoznacznie określają dwa parametry: c***zęstotliwość*** i ***długość fali***. Znajomość jednego z nich jednoznacznie określa konkretną falę.



Rys.4.7. *Parametry fali elektromagnetycznej*

Zgodnie z Międzynarodowym Regulaminem Radiokomunikacyjnym obecnie stosuje się dekadowy podział widma fal radiowych na zakresy. Podział ten przedstawia tabela 4.2.

Tabela 4.2. *Podział widma fal radiowych na zakresy (zgodnie z regulaminem radiokomunikacyjnym)*

Nr zakresu	Nazwa zakresu	Długość fali	Częstotliwość
4	fale myriametrowe, **VLF**	100 – 10 km	3 kHz – 30 kHz
5	fale kilometrowe, **LF**	10 – 1 km	30 kHz – 300 kHz
6	fale hektometrowe, **MF**	1000 – 100 m	300 kHz – 3 MHz
7	fale dekametrowe, **HF**	100 – 10 m	3 MHz – 30 MHz
8	fale metrowe, **VHF**	100 – 1 m	30 MHz – 300 MHz
9	fale decymetrowe, **UHF**	100 – 10 cm	300 MHz – 3 GHz
10	fale centymetrowe, **SHF**	10 – 1 cm	3 GHz – 30 GHz
11	fale milimetrowe, **EHF**	10 – 1 mm	30 GHz – 300 GHz
12	fale decymilimetrowe	1 -0,1 mm	300 GHz – 3 THz

1 THz = 1000 GHz.

Aktualnie częstotliwości powyżej 60 GHz są w stadium badań, na ogół jeszcze nie wykorzystywane w telekomunikacji. W kolumnie „Częstotliwość" dolna granica jest wyłączona, natomiast górna włączona do danego pasma.

Ze względu na rozszerzenie się widma użytecznych częstotliwości radiowych

organizacja CCIR *(Comite Consutatif International des Radiocommunicationns)*, poprzedniczka obecnej ITU–R *(International Telecommunication Union - Radiocommunication)* przyjęła numerację zakresów począwszy od 3 Hz, mimo że fale dłuższe od myrimetrowych nie mają obecnie praktycznego zastosowania jako fale radiowe. Przedstawiony w tablicy 4.2 podział jest zupełnie formalny, gdyż nie wynika z naturalnych właściwości fal różnych zakresów. W związku z tym równolegle stosowany jest również podział tradycyjny, dotyczący głównie systemów radiofonicznych (rozgłoszeniowych), przedstawiony w tabeli 4.3.

Tabela 4.3. *Tradycyjny podział widma częstotliwości radiowych na zakresy.*

Nazwa zakresu	**Długość fali**	**Częstotliwości**
Fale bardzo długie	powyżej 20 km	Poniżej 15 kHz
Fale długie	20 ÷ 3 km	15 ÷ 100 kHz
Fale średnie	3000 ÷ 200 m	100 ÷ 1500 kHz
Fale pośrednie	200 ÷ 100 m	1,5 ÷ 3 MHz
Fale krótkie	100 ÷ 10 m	3 ÷ 30 MHz
Fale ultrakrótkie	10 ÷ 1 m	30 ÷ 300 MHz
Mikrofale	Poniżej 1 m	Powyżej 300 MHz

Z rysunku 4.3 i tabeli 4.2 wynika, że szerokość pasma fal myriametrowych **VHF** wynosi tylko 27 kHz a zakresu fal milimetrowych **EHF** aż 270 GHz. Fakt ten spowodował konieczność podziału zakresów **SHF** i **EHF** na mniejsze podpasma z oznaczeniami literowymi. Problemem jest jednak to, że różne służby stosują inne podziały. W tabeli 4.4 przedstawiony jest podział stosowany w radiolokacji a w tabeli 4.5 w telekomunikacji (radiokomunikacji).

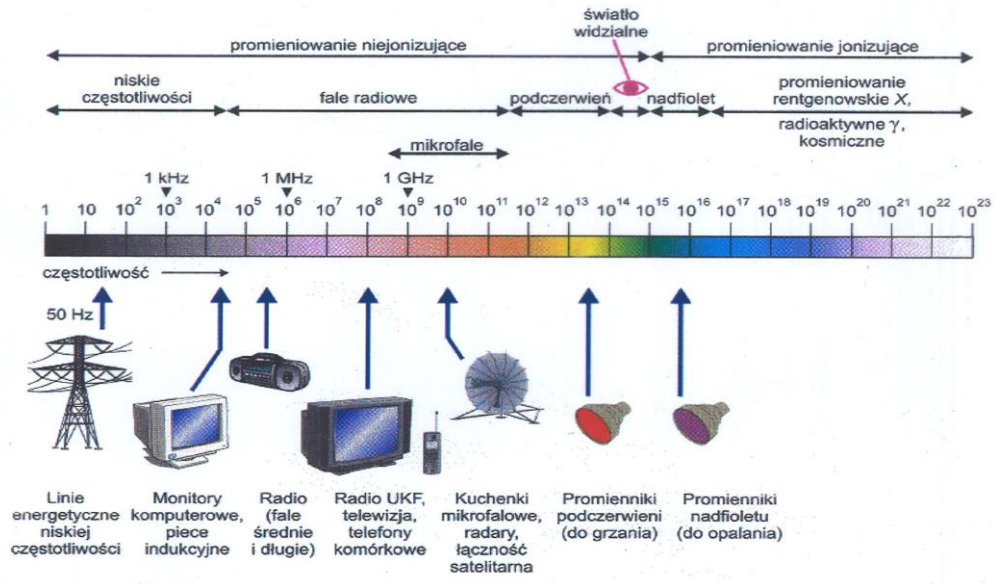
Tabela 4.4. *Pasma radiolokacyjne*

Pasmo	**Zakres częstotliwości [MHz]**	**Zakres długości fal [cm]**
P	225 – 390	133,3 – 76,9
L	390 – 1550	76,9 – 19,3
S	1550 – 5200	19,3 – 5,77
X	5200 – 10900	5,77 – 2,75
K	10900 – 36000	2,75 – 0,834
Q	36000 – 46000	0,834 – 0,652
V	46000 – 56000	0,652 – 0,536

Tabela 4.5. *Podpasma zakresów SHF i EHF wykorzystywane w radiokomunikacji.*

Oznaczenie podpasma	Zakres częstotliwości [GHz]
L	1 – 2
S	2 – 4
C	4 – 8
X	8 – 12
Ku	12 – 18
K	18 – 27
Ka	27 – 40
W	40 – 100

Wynika stąd konieczność opisowego omówienia konkretnych częstotliwości w sytuacji organizowania współpracy różnych służb. Ponadto z tabeli 4.5 wynika, że w systemach radiokomunikacyjnych maksymalna częstotliwość pracy to 100 GHz (praktycznie 60 GHz) mimo, że zakres EHF ma górną granicę równą 300 GHz. Poza tym telekomunikacja wykorzystuje jeszcze podczerwień i światło widzialne (w tych przypadkach wygodniej jest posługiwać się długością fali niż częstotliwością np. światło widzialne 390 ÷ 770 nm). Rysunek 4.8 przedstawia wykorzystanie różnych zakresów pól elektromagnetycznych w działalności gospodarczej człowieka.



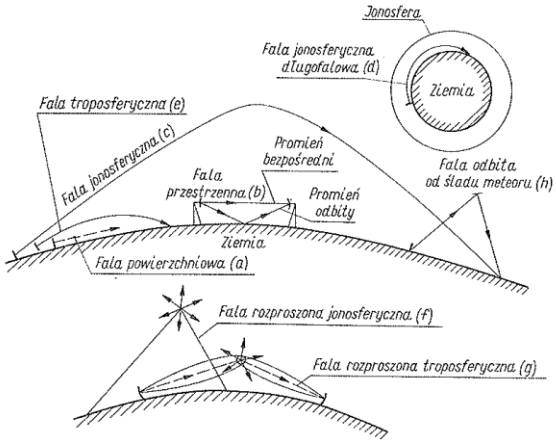
Rys.4.8. *Pola elektromagnetyczne w środowisku człowieka.*

4.4. Klasyfikacja sposobów propagacji fal radiowych.

Jednym z możliwych sposobów klasyfikacji fal radiowych może być charakter drogi, wzduż której docierają one z nadajnika do odbiornika. W zależności od położenia w przestrzeni dwóch punktów utrzymujących łączność między sobą można wyróżnić trzy zasadnicze przypadki:

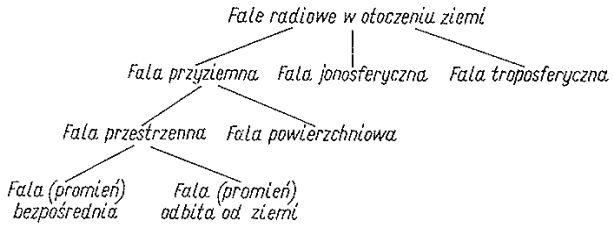
a) Ziemia – Ziemia, gdy oba punkty znajdują się na Ziemi,
b) Ziemia – Kosmos, gdy jeden z punktów znajduje się na Ziemi, a drugi w przestrzeni kosmicznej,
c) Kosmos – Kosmos, gdy oba punkty znajdują się w przestrzeni kosmicznej.

W pierwszym przypadku mamy do czynienia z rozchodzeniem się fal w otoczeniu Ziemi. Pozostałe dwa przypadki możemy w pierwszym przybliżeniu sprowadzić do propagacji fal w swobodnej przestrzeni. Należy jednak pamiętać, że fala wypromieniowana z Ziemi w przestrzeń kosmiczna przechodzi przez atmosferę ziemską,
a nawet przestrzeń międzyplanetarną ma raczej charakter plazmy niż iedealnej próżni.



Rys.4.9. *Różne sposoby rozchodzenia się fal radiowych w otoczeniu Ziemi.*

Na rysunku 4.9 przedstawiono schematycznie różne sposoby rozchodzenia się fal radiowych w otoczeniu Ziemi, a na rysunku 4.10 – klasyfikację tych fal.



Rys.4.10. *Schemat klasyfikacji różnych sposobów rozchodzenia się fal radiowych w otoczeniu Ziemii.*

Falę rozchodzącą się w bliskości Ziemi nazywamy ***falą przyziemną***. Fale przyziemne dzielimy na ***fale powierzchniowe*** i ***przestrzenne***. Fala powierzchniowa jest promieniowana przez antenę nadawczą, umieszczoną bezpośrednio na powierzchni Ziemi, i rozchodzi się wzdłuż tej powierzchni (rys. 4.9a). Fale przestrzenne (rys. 4.9b) występują głównie w zakresie fal ultrakrótkich gdy anteny są umieszczone ponad powierzchnią Ziemi, co jest możliwe dzięki małym rozmiarom anten. Przy falach dłuższych fale przestrzenne występują przy połączeniach między Ziemią a samolotem. Fala przestrzenna może mieć dwie składowe – ***falę bezpośrednią*** i ***falę odbitą*** od powierzchni Ziemi. Gdy anteny nadawcza i odbiorcza znajdują się na powierzchni Ziemi, wówczas obydwie składowe fali przestrzennej mają jednakowe amplitudy, lecz przeciwne fazy i znoszą się wzajemnie; fala powirzchniowa jest wtedy jedyną składową fali przyziemnej.

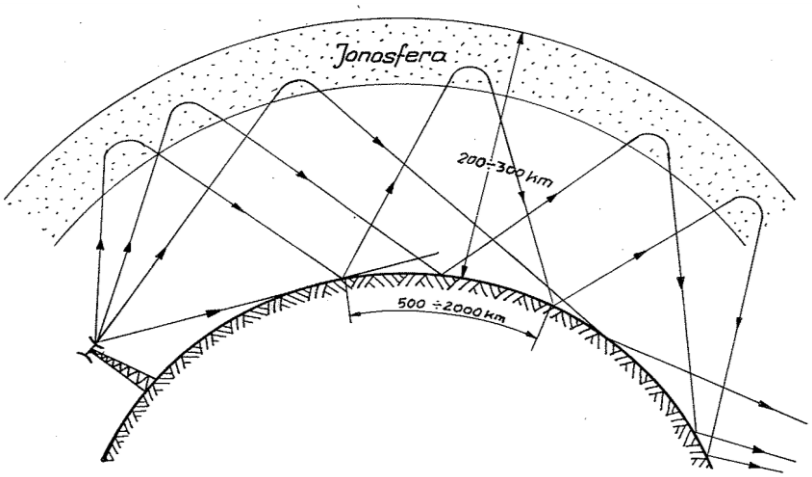
Falą jonosferyczną nazywamy falę, która dociera do odbiornika dzięki istnieniu jonosfery. Można tu rozróżnić dwa pokazane na rysunkach 4.9c i 4.9d. Na rysunku 4.9c promień padający na jonosferę ulega odbiciu i powraca na powierzchnię Ziemi. W taki sposób odbijają się od jonosfery fale krótkie i częściowo średnie, natomiast fale długie rozchodzą się w przestrzeni ograniczonej powierzchnią Ziemi i dolną granicą jonosery („falowód kulisty") w sposób przedstawiony na rys. 4.9d.

Falą troposferyczną nazywamy falę, która dociera do odbiornika dzięki refrakcji w troposferze.

Natężenie pola fali oraz jej faza i kierunek w miejscu odbioru są wynikiem nałożenia się promieni, które docierają do anteny odbiorczej różnymi drogami. Wypadkowe natężenie pola w miejscu odbioru zależy od amplitud, faz i polaryzacji promieni składowych. Może się na przykład zdarzyć, że do anteny odbiorczej docierają dwie fale o znacznych natężeniach pola, ale przesunięte w fazie o kąt bliski 180°, wobec czego wypadkowe natężenie pola jest bardzo małe. Może ono ponadto ulegać dużym zmianom w czasie, jeśli jedna ze składowych zmienia swą amplitudę, fazę lub polaryzację.

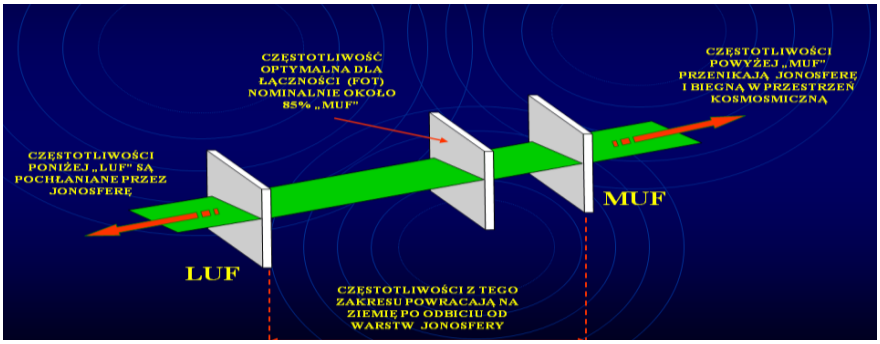
Zmienność natężenia pola w miejscu odbioru powoduje powstawanie zaników. ***Zanikiem*** nazywamy znaczne, gwałtowne obniżenie poziomu sygnału w stosunku do poziomu średniego. Na potrzeby tego opracowania, zaniki możemy podzielić na ***selektywne*** (występuje dla jednej konkretnej częstotliwości) i ***pasmowe*** (występuje dla całego pasma częstotliwości). Problem zaników w łączności radiowej jest bardzo

istotny. Rysunek 4.11 pokazuje jak rozchodzi się fala przestrzenna na duże odległości np. jonosferyczna.



Rys.4.11. *Rozchodzenie się fal przestrzennych na duże odległości.*

Z rysunku 4.11 widać, że sygnał wypromieniowany przez antenę nadawczą – lewa strona rysunku, może powrócić na Ziemię w postaci jednego „skoku jonosferycznego" ale mogą to być dwa lub więcej „skoków". Droga sygnału, w przypadku dwu skoków, jest około dwukrotnie dłuższa niż w przypadku skoku pojedyńczego. Oznacza to, że w punkcie odbioru pojawią się sygnały w fazach przeciwnych, czyli wystąpi zanik i odebranie sygnału będzie niemożliwe. Oddzielnym ważnym problemem jest dobór właściwej częstotliwości pracy. Z tego powodu w planowaniu systemów radiowych wprowadzamy dodatkowe ograniczenia na możliwe do wykorzystania częstotliwości, a mianowicie **LUF *(Low Usable Frequency)*** i **MUF *(Maximum Usable Frequency)***. Częstotliwości poniżej **LUF** zostaną pochłonięte przez jonosferę, a częstotliwości powyżej **MUF „**uciekną" w przestrzeń kosmiczną. Wynika z tego, że częstotliwość pracy powinna zawierać się pomiędzy LUF a MUF. Praktycznie częstotliwość pracy **FOT *(Frequency Optimum of Traffic)*** dobiera się jako około 85% **MUF.** Przedstawia to rysunek 4.12.



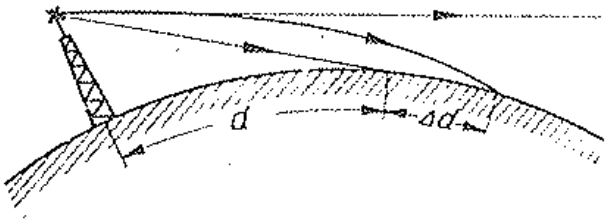
Rys.4.12. *Optymalna częstotliwość robocza.*

Ciekawym rodzajem propagacji jest przypadek odbicia od smug (śladów) meteorów, rysunek 4.9h oznaczana jako **MS *(Meteor Scatter)*.** Przenikającym do atmosfery ziemskiej meteorom towarzyszy powstawanie słupów zjonizowanego powietrza (smug, śladów) lub ***kolumn zjonizowanych***, od których następuje odbicie i rozproszenie fal radiowych zakresu metrowego. Obserwując przelot samolotu odrzutowego widzimy, że pozostawia on na niebie skondensowaną smugę pary wodnej. Podobnie przemieszczający się w atmosferze ziemskiej meteor lub rój (deszcz meteorów) pozostawia za sobą warstwę (kolumnę) zjonizowanego powietrza. Natężenie pola wytwarzanego dzięki odbiciu fali od kolumny zjonizowanej przez meteor jest znacznie większe, niż przy normalnym rozproszeniu wskutek niejednorodności.

Kolumny zjonizowane powstają zazwyczaj na wysokości około 80 d0 120 km. Ich średnia długość bywa około 25 km, zaś srednica początkowa zaledwie rzędu 1 metra; po pewnym czasie, dzięki dyfuzji średnica kolumn powiększa się. Na skutek ruchów turbulencyjnych i wichrów jonosferycznch często się zdarza, że proste początkowo kolumny przybierają o pewnym czasie kształt serpentyny. Jeśli uwzględnić wszystkie nawet najdrobniejsze cząstki, to liczba meteorów wpadających dziennie do atmosfery ziemskiej jest bardzo duża rzędu dziesiątków bilionów. Nic więc dziwnego, że meteory przyczyniają się w pewnym stopniu do jonizacji atmosfery ziemskiej w ogóle, a i większe meteory poaostawiające w jonosferze ślady w postaci wyżej opisanych zjonizowanych kolumn zdarzają się na tyle często, że zjawisko to można wykorzystać w radiokomunikacji. W odróżnieniu od łącz jonosferycznych na fali rozproszonej, łącza wykorzystujące propagację wykorzystujące propagację poprzez ślady meteorów, pracują na zasadzie kumulacji sygnału, ponieważ łączność jest zasadniczo „dorywcza". Stosunek czasu faktycznego istnienia łąvzności do czasu pracy nadajników (tzw. współczynnik wykorzystania łącza) zależy od mocy nadajnika, kierunkowości anten i czułości odbiornika. Przy niewielkich mocach nadajnika (rzędu kilkuset watów) i stosunkowo prostych antenach współczynnik ten nie bywa mniejszy od 1/20 (5% czasu – aktywna łączność, 95% czasu – oczekiwanie). W okolicznościach bardziej sprzyjających (w miesiącach pojawiania się zwiększonej ilości meteorów np. roje perseidów, 2 dekada sierpnia) oraz przy większych mocach nadajników współczynnik wykorzystania zwiększa się do 0,1 a niekiedy przybiera nawet jeszcze większe wartości. Aby zapobiec nadmiernemu gromadzeniu się informacji, przekazywanie ich powinno odbywać się z szybkością mniej więcej dwudziestokrotnie większą od normalnej.

4.5. Określanie zasięgu łączności radiowej.

Przy rozprzestrzenianiu się fal metrowych (30 ÷ 300 MHz; w tym zakresie pracują służby ratownictwa, policja, administracja rządowa i samorządowa) na odległości większe od kilkunastu kilometrów zaczyna odgrywać rolę zjawisko krzywizny powierzchni kuli ziemskiej, rysunek 4.14.



Rys.4.14. *Zwiększenie zasięgu fali przestrzennej wskutek refrakcji.*

W tym przypadku zasięg **horyzontalny geometryczny d_g** jest uzależniony od wysokości umieszczenia anten i może być wyrażony wzorem:

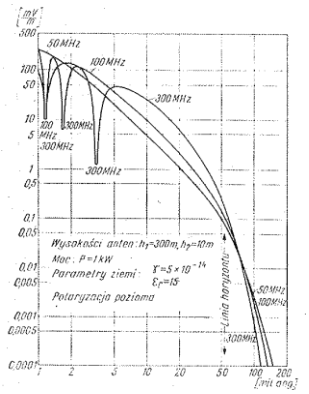
$$d_g = 3{,}57\left(\sqrt{h_n} + \sqrt{h_o}\right)[km]$$

gdzie: h_n – wysokość umieszczenia anteny nadawczej w metrach,

h_o – wysokość umieszczenia anteny odbiorczej metrach.

Współczynnik 3,57 wynika z przeliczenia stałych parametrów Ziemi - stałej dielektrycznej i konduktywności. Na rysunku 4.15 przedstawione są krzywe natężenia fali przestrzennej rozchodzącej się nad gładką powierzchnią dla częstotliwości 50, 100 oraz

300 MHz. Liczba i rozmieszczenie zaników zależy od częstotliwości – im większa częstotliwość, tym więcej punktów zaniku. Wielkość zaników uzależniona jest od parametrówziemi i wysokości umieszczeni anten. Zjawisko zaników występuje tym silniej, im wyżej umieszczone są anteny.



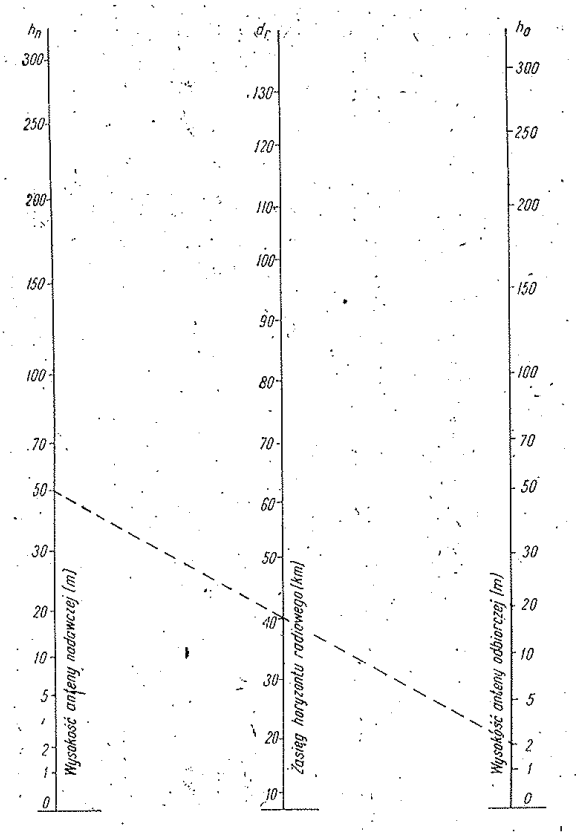
Rys.4.15. *Teoretyczne krzywe natężenia pola w funkcji odległości dla częstotliwości 50, 100 i 300 MHz.*

Ponieważ fala przyziemna rozchodzi się na granicy dwóch ośrodków: ziemi i troposfery, oba te środowiska wywierają wpływna propagację fali. Oddziaływanie to przejawia się w zakrzywieniu drogi fali wskutek refrakcji w taki sposób, że zwiększa siejej zasięg bezpośredni poza horyzont geometryczny (rys. 4.14). Miejsce styczności toru z kulą ziemską tworzą tzw. **horyzont radiowy.** Liczbowo horyzont radiowy $\mathbf{d_r}$ dla atmosfery normalnej w pobliżu powierzchni ziemi wynosi 4/3 horyzontu geometrycznego.

$$d_r = \frac{4}{3} d_g = 4{,}76\left(\sqrt{h_n} + \sqrt{h_o}\right)[km]$$

Wartość współczynnika 4/3 stosuje się do zakresów częstotliwości powyżej 30 MHz.

W celu ułatwienia praktycznego określania zasięgu horyzontu radiowego opracowane zostały nomogramy, rysunek 4.16. W sieciach radiotelefonicznych, składających się z stacji stałych oraz ruchomych, zainstalowanych w pojazdach, możliwości wysokiego umieszczenia anten stacji ruchomych są bardzo ograniczone (a to głównie decyduje o zasięgu): w praktyce wysokość ta wynosi 1 ÷ 3 m.



Rys.4.16. *Nomogram do obliczania zasięgu horyzontu radiowego*

(np. h_n = 50 m i h_o = 2m; $d_r \approx$ 40 km)

W takim przypadku o zasięgu będzie decydowała przede wszystkim wysokość umieszczenia anteny stacji stałej. W praktyce wysokości te wynoszą 10 ÷ 100 m. Przy takich wysokościach anten wartość horyzontu radiowego zawierają się w granicach 20 ÷ 60 km. Takie określenie zasięgu (wzór lub nomogram) oznacza, że łączność może być ale nie ma pewności, że na pewno będzie. Aby mieć pewność co do rzeczywistego zasięgu, należy dokonać praktycznych pomiarów natężenie pola w punkcie odbioru.

5. Urządzenia radiokomunikacyjne i systemy radiokomunikacji ruchomej.

5.1. Przepisy regulacyjne w radiokomunikacji.

Systemy radiokomunikacyjne są szczególnymi rodzajami systemów telekomunikacyjnych, w których transmisja odbywa się za pośrednictwem fal elektromagnetycznych (fal radiowych). Z jednej strony zapewnia to możliwość komunikowania się z obiektami ruchomymi, co jest wyłączną właściwością systemów radiokomunikacyjnych, ale z drugiej strony powoduje istotne ograniczenia wynikające z korzystania przez wszystkie – w skali światowej – systemy radiokomunikacyjne z tego samego widma elektromagnetycznego, które należy traktować jako dobro naturalne całej ludzkości.

W początkowym okresie rozwoju radiokomunikacji nieliczne, działające wówczas urządzenia były znacznie od siebie oddalone w przestrzeni, znajdowały się w różnych zakresach częstotliwości lub pracowały w różnych przedziałach czasowych tak, że ich wzajemnie oddziaływanie na siebie było niewielkie. Jednak w miarę postępującego rozwoju techniki do ziemskiego środowiska elektromagnetycznego zaczęto wprowadzać coraz więcej urządzeń elektrycznych, elektronicznych, telekomunikacyjnych, a w tym zwłaszcza nadawczych radiowych, które zaczęły w niekorzystny sposób wpływać na stan tego środowiska, co najczęściej objawia się zakłóceniami w pracy wielu różnych urządzeń, zwłaszcza wykorzystujących energię elektryczną w różnej postaci (zasilanie, wzmacnianie, generacja). Powstała więc konieczność podjęcia takich działań koordynacyjnych w skali międzynarodowej, które pozwoliłyby na optymalne wykorzystanie widma elektromagnetycznego bez ujemnych skutków. Działania te mają nie tylko charakter techniczny i normalizacyjny, ale także związane są ze stosowaniem odpowiednich regulacji prawnych, które porządkują wspólne wykorzystywanie widma częstotliwości radiowych przez wielu użytkowników.

Podstawowym aktem prawa międzynarodowego, regulującym użytkowanie całego widma częstotliwości radiowych przez wszystkich operatorów sieci, systemów i urządzeń radiowych, a także innych użytkowników wykorzystujących częstotliwości radiowe dla bardzo różnych potrzeb i zastosowań, jest międzynarodowy Regulamin Radiokomunikacyjny *(RR – Radio Regulations)*. Jest on jednym z dokumentów uzupełniających Konstytucję i Konwencję Międzynarodowego Związku Telekomunikacyjnego *(ITU – International Telecommunication Union)* i ma charakter obowiązujący wszystkich sygnatariuszy – członków ITU, w tym także Polskę. Jego treść jest tworzona, aktualizowana, zmieniana oraz zatwierdzana wyłącznie podczas obrad Światowych Konferencji Radiokomunikacyjnych *(WRC – World Radiocommunication Conference)*, które ostatnio odbywają się na ogół co 3 – 4 lata.

Ponieważ obowiązujące obecnie Konstytucja i Konwencja ITU, sporządzone w Genewie w dniu 22 grudnia 1992 r., zostały ratyfikowane przez Prezydenta Rzeczypospolitej Polskiej w dniu 10 maja 1995 r. i są opublikowane w Dzienniku Ustaw z 1998 r. Nr 35, poz. 196, są one zatem dokumentami traktatowymi, wynikającymi z art. 4 Konstytucji ITU, a więc stanowią prawo międzynarodowe obowiązujące również w Polsce. Tak więc Regulamin Radiokomunikacyjny stanowiący ich uzupełnienie jest podstawowym aktem prawnym normującym wszelkie działania w dziedzinie radiokomunikacji w Polsce.

Wymienione wyżej dokumenty – Konstytucja i Konwencja ITU, spełniają także wymagania wynikające z art. 88 Konstytucji Rzeczypospolitej Polskiej dotyczące obowiązku promulgacji oraz z art. 2 pkt 13 ustawy Prawo telekomunikacyjne, definiującego pojęcie międzynarodowych przepisów radiokomunikacyjnych jako *„określonych w umowach międzynarodowych ratyfikowanych przez Rzeczpospolitą Polską i ogłoszonych w Dzienniku Ustaw”*.

Jak z powyższego wynika międzynarodowy Regulamin Radiokomunikacyjny jest dokumentem szczególnie wysokiej rangi, a jego nieprzestrzeganie może realnie grozić formalną bezprawnością wielu aktów prawnych i decyzji administracji łączności, podejmowanych w oparciu o tę podstawę prawną.

Tak więc, podstawowym dokumentem w procesie zarządzania zasobami częstotliwości w każdym kraju należącym do Międzynarodowego Związku Telekomunikacyjnego ITU jest Krajowa Tablica Przeznaczeń Częstotliwości. Opracowywana na podstawie ustaleń Regulaminu Radiokomunikacyjnego – aktu prawa międzynarodowego uzupełniającego Konstytucję i Konwencję ITU, określa

przeznaczenie częstotliwości lub zakresów częstotliwości dla poszczególnych służb radiokomunikacyjnych działających w Polsce. Dokument ten ma więc na celu uporządkowanie i efektywne gospodarowanie dobrem ograniczonym, jakim jest widmo częstotliwości i będzie służyć również do systematycznego opracowywania planów zagospodarowania poszczególnych pasm i zakresów częstotliwości, które będę ogłaszane w Biuletynu UKE (*Urząd Komunikacji Elektronicznej)*.

5.2. Klasyfikacja Służb radiokomunikacyjnych.

Klasyfikacja służb radiokomunikacyjnych w zależności od przeznaczenia jest przedstawiona na rysunku 5.2.

Określenia poszczególnych służb są następujące:

Służba ziemska – służba pełniona wyłącznie na ziemi lub w obrębie niższych warstw atmosfery ziemskiej.

Służba kosmiczna – pełniona między stacjami naziemnymi a stacjami kosmicznymi, lub między stacjami kosmicznymi, lub też między stacjami naziemnymi za pośrednictwem obiektów kosmicznych.

Służba stała – służba pełniona między określonymi punktami stałymi.

Służba radiodyfuzyjna – służba której nadawania są przeznaczone do bezpośredniego odbioru przez szeroki ogół społeczeństwa (radiofonia, telewizja).

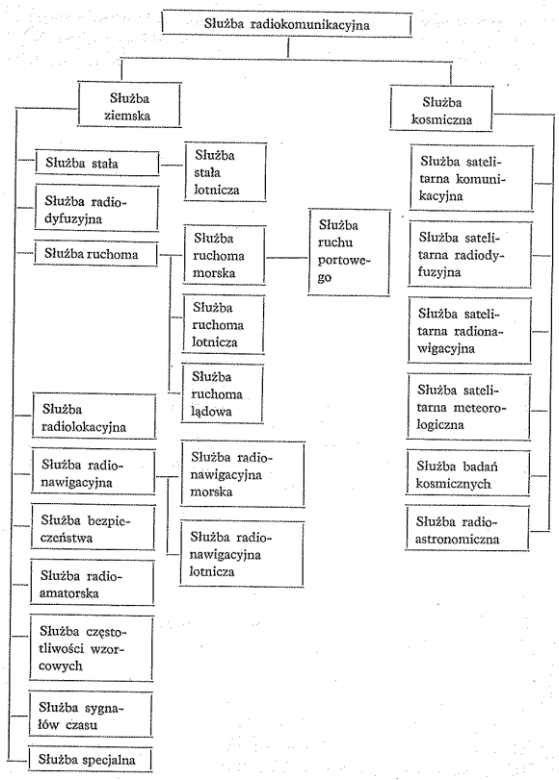
Służba ruchoma – służba pełniona między stacjami ruchomymi a stacjami lądowymi (lotniskowymi, nadbrzeżnymi, bazowymi) lub też między stacjami ruchomymi.

Służba bezpieczeństwa – służba pełniona stale lub czasowo, w celu ochrony życia i mienia ludzkiego.

Służba specjalna – służba pełniona dla zaspokojenia specjalnych potrzeb i nie przeznaczona dla ogółu.

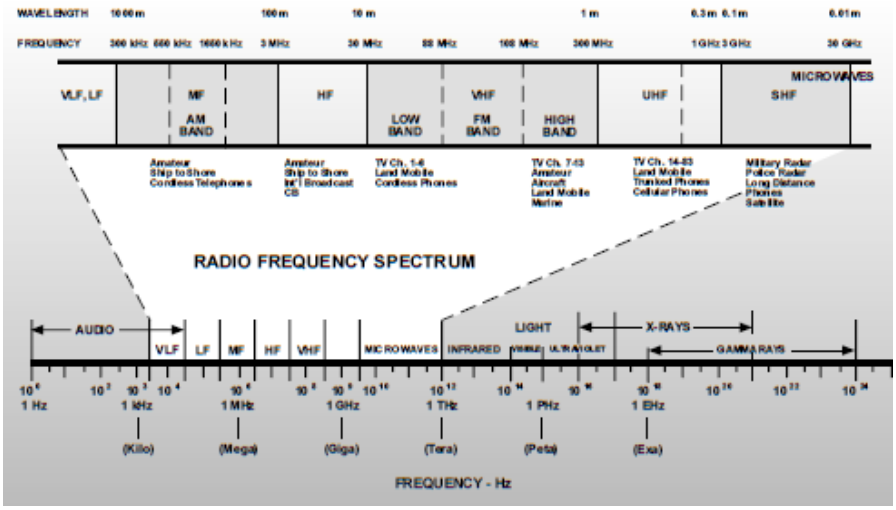
Nazwy pozostałych służb (radionawigacyjna, amatorska, sygnałów czasu czy meteorologiczna) jednoznacznie określają ich funkcje i zadania.

Poszczególne służby stałe (radiofonia, telewizja, nadawanie częstotliwości wzorcowych, radionawigacyjna), ruchome (lądowa, morska, lotnicza), radioamatorskie, meteorologiczne itp. posługują się przydzielonymi im pasmami częstotliwości. Poszczególne pasma częstotliwości są ustalane zależnie od wymagań służby, rodzaju otoczenia i zasięgu. Zależnie od wymagań dotyczących zasięgów dla poszczególnych służb są wybrane odpowiednie zakresy częstotliwości, moce nadajników oraz ewentualnie stosowane anteny o odpowiednich kierunkach promieniowania.

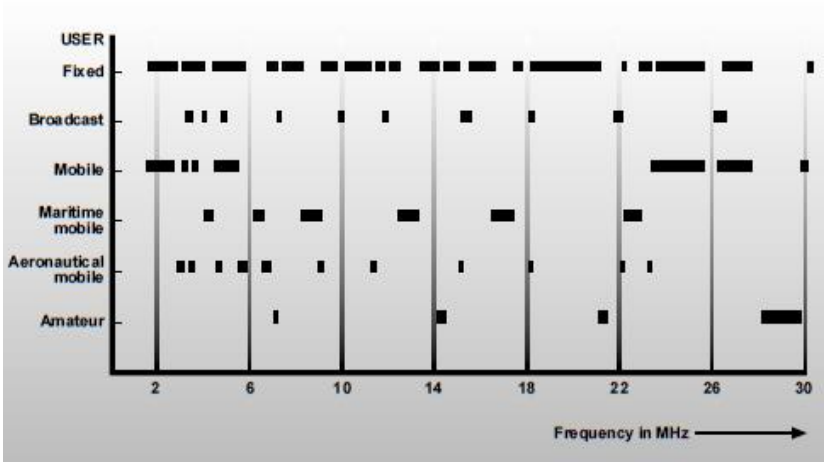


Rys.5.2. *Klasyfikacja służb radiokomunikacyjnych.*

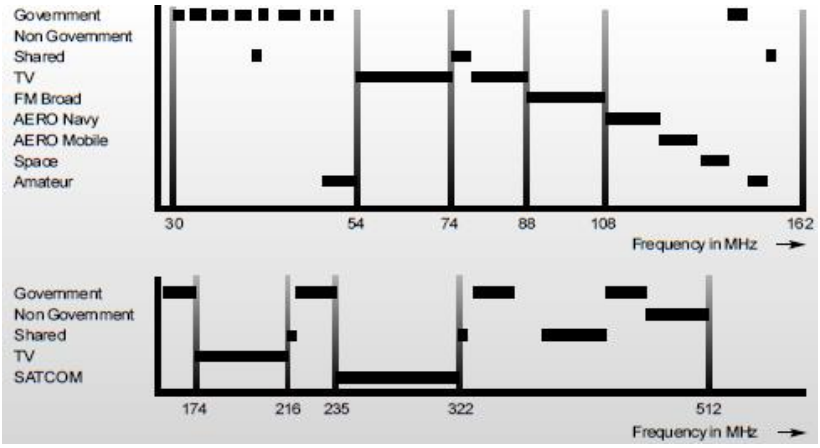
Ogólny podział widma częstotliwości radiowych przedstawia rysunek 5.3 a przykładowe alokacje poszczególnych pasm zakresów HF, VHF i UHF rysunki 5.4 i 5.5. Jak widać z przedstawionych rysunków obowiązujące przepisy regulacyjne nie zezwalają na pracę urządzeń radiowych w innych niż przewidziane dla danej służby zakresach częstotliwości. Nieprzestrzeganie tych rygorów, a ciągle notuje się takie przypadki (paralotniarze, taksówkarze z „dopalaczami" do CB radio) naraża takich użytkowników na konsekwencje karne.



Rys.5.3. *Widmo częstotliwości radiowych.*



Rys.5.4. *Przykładowa alokacja poszególnych zakresów widma zakresu HF.*



Rys.5.5. *Przykładowa alokacja zakresów widma VHF i UHF.*

5.3. Urządzenia radionadawcze

Jak wynika z rysunku 4.1 w łączu radiowym mamy po jednej stronie nadajnik wraz z anteną nadawczą - „transfomator" - dopasowujący małą impedancję układów wyjściowych nadajnika do dużej impedancji otaczającej przestrzeni, a po drugiej stronie odbiornik radiowy z anteną odbiorczą w której indukuje się sygnał przenosi informację i dopasowuje impedancję otaczającej przestrzeni w punkcie odbioru do małej impedancji obwodów wejściowych odbiornika. Oczywistym jest, że prostokąt opisany na rysunku 4.1 jako „nadajnik" (podobnie jak i ten opisany jako „odbiornik") składa się z pewnej liczby bloków funkcjonalnych.

Precyzyjniej określając powiemy, że zadaniem nadajnika jest wytworzenie nośnej o częstotliwości nośnej odpowiadającej konkretnemu kanałowi radiowemu, zmodulowanie jej sygnałem podanym z zewnątrz (zakodowanie w niej informacji użytecznej) oraz takie jego przetworzenie aby osiągnąć jak najlepsze warunki

propagacyjne (dobór typu emisji), właściwe wzmocnienie sygnału zmodulowanego do poziomu mocy, zapewniającego wymagany zasięg. Do wyjścia nadajnika podłączona jest antena nadawcza.

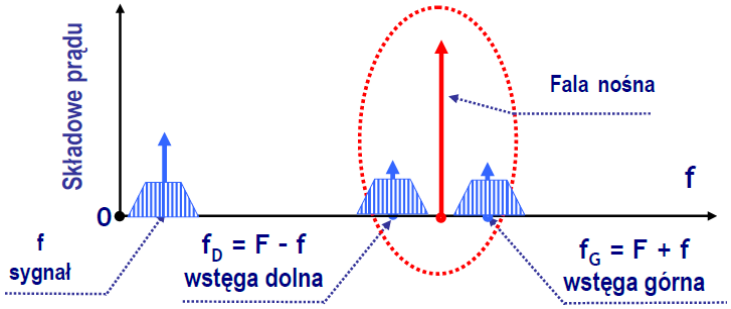
Fala nośna jest wytwarzana w generatorze wielkiej częstotliwości. Jest to częstotliwość którą emituje nadajnik, zatem jakość generatora wielkiej częstotliwości (pospolicie zwanego generatorem w.cz.) jest dość istotna dla parametrów całego łącza radiowego. Częstotliwość generatora powinna być możliwie niezmienna w czasie. Przy niewielkich wymaganiach jakościowych i częstotliwości do kilkuset kiloherców stosuje się generatory z obwodem LC - równolegle połączonymi cewką i kondensatorem. Pojemność kondensatora i indukcyjność cewki decydują o częstotliwości. Generatory LC występują także w radiolokacji, gdzie operuje się częstotliwościami rzędu gigaherców, ale przy tych wartościach i impulsowej technice pracy nadajniki radarów mają bardzo złożoną, specyficzną konstrukcję.

Generatory w.cz. o przyzwoitszych parametrach są zwykle stabilizowane rezonatorem kwarcowym. Pojedynczy rezonator może stabilizować tylko jedną częstotliwość, dla której został wykonany.

W nadajnikach przestrajanych stosuje sie dwa rozwiązania. Jedno, prostsze, polega na zastosowaniu przełączanych rezonatorów - jeden rezonator na jeden kanał łączności. Taka konstrukcja jest prosta i tania, ale opłacalna tylko dla niewielkiej liczby kanałów - z reguły do dwunastu.

Kiedy potrzeba nadajnika przestrajalnego w całym paśmie, obejmującym wiele kanałów radiowych, stosuje się syntezę częstotliwości. Polega ona na otrzymywaniu potrzebnej częstotliwości metodą mieszania („zdudniania") przebiegów wytwarzanych przez dwa (lub więcej) generatory kwarcowe. Generator w.cz. z syntezą składa się z kilkunastu „mini generatorów" kwarcowych i elektronicznego bloku sterowania (obecnie prawie zawsze cyfrowego). Kiedy przestrajamy taki nadajnik (pokrętłem lub klawiaturą numeryczną) układ sterowania włącza odpowiednie generatory i filtry, produkujące razem żądaną częstotliwość. Oczywiście synteza nie działa płynnie - stopniowanie częstotliwości dobiera się zależnie od przyjętego odstępu międzykanałowego. Na przykład dla lotniczej łączności radiowej w paśmie 118 - 136.975 MHz odstęp między sąsiednimi kanałami wynosi 25 kHz albo 8.33 kHz, w konwencjonalnej łączności radiowej w PSP 12,5 kHz, w systemach trankingowych 25 kHz, w telefonii komórkowej GSM 200 kHz, a w stałych systemach łączności radiowej 100 kHz.

Kolejny blok funkcjonalny nadajnika, modulator, służy do „nałożenia” na falę nośną sygnału użytecznego (sygnału niosącego informację). Cały proces nazywa się modulacją. Konstrukcje modulatorów zależą od typu modulacji, zastosowanego w łączności. Istnieją trzy podstawowe rodzaje modulacji: amplitudowa, kątowa (częstotliwości i fazy) oraz impulsowa. Wewnątrz każdej z nich wyróżnia się wiele rozmaitych emisji. Na rysunku blokowym wyjaśniającym prace nadajnika rys. 5.7 narysowano modulację amplitudy (amplitudową) fali nośnej, powszechnie znaną jako AM *(Amplitude Modulation).*



Rys.5.7. *Widmo sygnału z modulacją AM.*

Sygnał modulujący jest zakodowany jako obrys (fachowo: obwiednia) fali nośnej na wyjściu. Modulacja amplitudy jest podatna na zniekształcenia i nie nadaje się do przesyłania sygnałów o dużej dynamice (na przykład muzyki). Przyczyną jest niewielka różnica między najwyższą a najniższą amplitudą zmodulowanej fali (czyli głębokość modulacji), którą można utrzymać bez obcinania „czubków” fali. Za to modulacja ta jest niezrównana jeśli chodzi zasięg, prostotę i niezawodność. Największy zasięg uzyskuje się przy telegrafii, gdzie występują tylko dwa poziomy amplitudy: wysoki (element znaku, czyli kropka lub kreska) i niski, czyli przerwa.

Najbardziej znaną emisją kątową jest modulacja częstotliwości (FM - *Frequency Modulation*). Przy FM obwiednia fali nośnej jest równa, a informacja jest zakodowana w postaci zmian częstotliwości sygnału wyjściowego. Zmienia się ona o wartość częstotliwości sygnału modulującego. Zakres tych zmian nazywa się dewiacją częstotliwości. FM dobrze nadaje się do połączeń o wysokiej jakości na krótkich dystansach. Dobra jest też do łączności przewodowej (modemy i faksy). Za to odstępy między kanałami muszą być większe niż przy modulacji amplitudowej (co przedstawiono na rysunku 4.3). Modulacja częstotliwości szwankuje także przy łączności lotniczej - w wielu sytuacjach efekt Dopplera dodaje swoje trzy grosze do dewiacji, a wtedy zniekształcenia uniemożliwiają odbiór.

Dynamicznie rozwijająca się modulacja impulsowa polega na kodowaniu informacji w postaci odległości (czyli czasu) między kolejnymi impulsami. Na przykład dla radaru informacją użyteczną jest istnienie i odległość przeszkody na drodze fal radiowych, która wpływa na czas powrotu impulsu do anteny. Modulacja impulsowa wymaga skomplikowanego sprzętu, ale za to jest dobra do wszystkiego. Dźwięk i inne sygnały analogowe przesyła się w postaci próbek, pobranych dostatecznie gęsto aby odzwierciedlały przebieg pierwotny z potrzebną dokładnością. Dla muzyki wystarcza 60000 próbek (płyta kompaktowa CD 44100) na sekundę. Wartości próbek, czyli chwilowe napięcie sygnału modulującego, są wysyłane jako liczba dwójkowa (binarna), wyrażona właśnie miejscem impulsów w szeregu. Taką konkretną odmianę modulacji impulsowej nazywa się modulacją impulsowo - kodową (PCM) omówioną już w punkcie 2.4 tego opracowania. Przechodząc do praktyki. Jeżeli sygnał modulujący niesie jakąkolwiek informację, znaczy to, że jest zmienny. Jego częstotliwość zależy od natury sygnału i przyjętego rodzaju emisji. Najczęściej wysyła się „w eter" falę nośną w towarzystwie obu wstęg bocznych. Emisję dwuwstęgową stosuje radiofonia i telewizja publiczna, a także łączność lotnicza i morska rysunek 5.7. Do fali nośnej z obydwoma wstęgami łatwiej się dostroić: w miarę posuwania się po skali odbiornika poziom odbioru rośnie w miarę zbliżania się do częstotliwości nadajnika, potem odrobinkę opada, potem znów wzrasta, aby ostatecznie „odjechać w siną dal". Właśnie w tym dołku między maksymami odbiór jest najlepszy - środek pasma przenoszenia odbiornika pokrywa się dokładnie z częstotliwością fali nośnej.

Dodatkowym powodem szukania innych typów emisji jest fakt, że w sygnale zmodulowanym amplitudowo (dwie wstęgi boczne) prążek na częstotliwości nośnej to 50 % przenoszonej energii a po 25 % przypada na wstęgi boczne, więc jest to duża rozrzutność (na częstotliwości nośnej nie ma informacji). Z tego powodu szukamy takich rodzajów emisji aby móc zmniejszyć moc promieniowaną na nośnej F, a „zaoszczędzoną" moc „dołożyć" do wstęg bocznych, bo tam jest zawarta informacja.

Niektóre rodzaje emisji wykorzystują tylko jedną wstęgę boczną - drugą wycina się zaraz za modulatorem. Pozwala to zmieścić więcej kanałów radiowych w przydzielonym zakresie częstotliwości, dlatego z emisji jednowstęgowych (SSB - *Single Side Band*) korzystają rozmaite sieci łączności i radioamatorzy. Odmianą tej techniki jest emisja dwuwstęgowa z niezależnymi wstęgami bocznymi - każda niesie inną informację.

Z wyjścia modulatora sygnał wielkiej częstotliwości trafia do wzmacniacza mocy. Jego zadaniem jest wzmocnienie fali nośnej na tyle, żeby uzyskać potrzebny zasięg łączności. Większości wzmacniaczy mocy wielkiej częstotliwości modulacja i rodzaj emitowanego sygnału są całkowicie obojętne. Konstrukcja i technologia wzmacniaczy zależy od zakresu częstotliwości pracy i mocy którą mają osiągać. Moc wyjściowa nadajników z kolei zależy od ich zastosowania: od parudziesięciu miliwatów w przypadku taniego radiotelefonu, poprzez kilka kilowatów dla stacji radiofonicznej, po moce rzędu megawatów dla stacji radiolokacyjnych. Na przykład moc wyjściowa nadajników radiostacji lotniczych waha się od 5 do 250 watów. Energia wielkiej częstotliwości jest wypromieniowywana przez antenę nadawczą. Z punktu widzenia fizyki antena jest po prostu odcinkiem przewodu o wymiarach porównywalnych z długością fali nośnej. Nie wdając się w dokładniejsze rozważania, można poprzestać na stwierdzeniu że antena jest najlepiej dopasowana do częstotliwości pracy gdy jej długość równa się długości fali. Ponieważ jednak warunek ten jest trudny do spełnienia (dla fal długich - VLF, LF - długość fali mierzy się w kilometrach), w praktyce stosuje się anteny półfalowe i ćwierćfalowe. Anteny dla radiostacji przestrajalnych konstruuje się dla środkowych częstotliwości ich zakresu pracy. Częstotliwość fali nośnej miesza się (interferuje) z częstotliwością sygnału modulującego, tworząc dwie wstęgi boczne: dolna przez odejmowanie, górna przez dodawanie częstotliwości. Szerokość tych wstęg zależy od zmian częstotliwości modulującej - fala nośna jest przecież stała. Im węższe pasmo sygnału modulującego, tym węższe wstęgi boczne. Maksymalna i minimalna wartość częstotliwości wstęg bocznych wyznaczają potrzebną szerokość kanału radiowego.

Schemat blokowy rzeczywistego nadajnika radiowego np. radiotelefonicznego jest bardziej złożony niż przedstawiony na rysunku 5.6. W typowym nadajniku radiowym mamy dwa tory, tor małej częstotliwości złożony z mikrofonu (zamiana zmiennego ciśnienia akustycznego wypowiadanej frazy na sygnał elektryczny), wzmacniacza mikrofonowego (zwiększenie poziomu sygnału modulującego) i filtru (przepuszczającego tylko ten zakres widma sygnału mowy, który jest niezbędny dla zapewnienia właściwej zrozumiałości, w telefonii jest to zakres od 300 do 3400 Hz). Tor ten kończy się na jednym wejściu układu modulatora. Na drugie wejście modulatora podajemy sygnał wielkiej częstotliwości wytworzony w stabilizowanym kwarcowo generatorze (lub układzie syntezy częstotliwości). Tu pojawia się pierwsza trudność, zgodnie z rysunkiem 5.6 generator powinien „dostarczać" sygnał

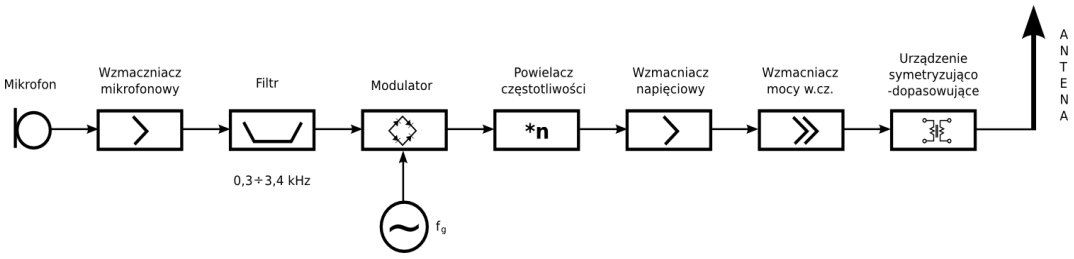
o częstotliwości nośnej. W konwencjonalnej łączności radiowej w PSP pracujemy na częstotliwości ok. 150 MHz a sygnał w torze małej częstotliwości jest rzędu 3 kHz, stąd ich stosunek jest bardzo niekorzystny. Obwody rezonansowe są budowane z elementów elektronicznych (pojemności, indukcyjności) których tolerancja wykonania jest duża i zmienna (np. kondensatory mają tolerancje rzędu ± 20%, nadruk na kondensatorze określa jego wartość na 100 pF, a to oznacza, że pojemność tego konkretnego kondensatora zawiera się w granicach 80 ÷ 120 pF) co oczywiście będzie miało wpływ na częstotliwość rezonansową obwodów w układach modulatora $f_r = \frac{1}{2\pi\sqrt{LC}}$. W tej sytuacji stosunkowo mała (w stosunku do nośnej) częstotliwość modulująca może niepoprawnie „wymodulować" nośną. Aby tego uniknąć stosujemy generatory o częstotliwościach wielokrotnie niższych (np. 30 MHz) niż częstotliwość nośna, a pobierany z wyjścia modulatora sygnał zmodulowany podajemy na powielacz częstotliwości (krotnik) aby otrzymać zmodulowany sygnał o częstotliwości konkretnego kanału radiowego - na wejście powielacza częstotliwości podajemy zmodulowany sygnał 30 MHz, a w obciążeniu krotnika mamy obwód częstotliwości rezonansowej 150 MHz – oznacza to „wyłowienie" z sygnału wejściowego piątej harmonicznej, czyli oczekiwane 150 MHz. Poziom piątej harmonicznej jest mały więc podaje się go na wzmacniacz napięciowy, aby poprawnie wysterować kolejny blok - wzmacniacza mocy w.cz. (wielkiej częstotliwości) który zapewni oczekiwany zasięg. Ostatnim blokiem, przed anteną, w nadajniku jest układ symetryzująco – dopasowujący. Zadaniem jego jest dopasowanie impedancji wyjściowej wzmacniacza mocy w.cz. do impedancji wejściowej zastosowanej anteny. Ponieważ w systemach radiokomunikacyjnych stosujemy różne typy anten, symetryczne np. antena dipolowa lub niesymetryczne np. antena prętowa to zadaniem tego bloku jest również „dopasowanie" symetrycznego wyjścia wzmacniacza mocy w.cz. do wejścia zastosowanej anteny.

Reasumując, można w trzech punktach określić funkcje nadajnika radiowego:

1. Zadaniem nadajnika jest wygenerowanie sygnału w.cz. o częstotliwości nośnej danego kanału radiowego,
2. Zmodulowanie tej częstotliwości (w.cz.) sygnałem (niosącym informację) podanym z zewnątrz,

3. Uformowanie sygnału zmodulowanego tak aby uzyskać możliwie optymalne dopasowanie do warunków propagacyjnych – dobór typu emisji i mocy wyjściowej wielkiej częstotliwości RF *(Radio Frequency).*

Schemat blokowo – funkcjonalny nadajnika radiowego przedstawiono na rysunku 5.8.



Rys.5.8. *Schemat blokowy nadajnika radiowego.*

5.3.1. Parametry nadajników

Każde urządzenie techniczne, w zależności od stopnia jego skomplikowania, można opisać pewną liczbą właściwych temu urządzeniu (lub grupie urządzeń) parametrów. Z drugiej strony ich ilość będzie zależna od potrzeb użytkownika. Innych, bardziej szczegółowych, potrzebował będzie konstruktor urządzeń a innych bardziej ogólnych eksploatator urządzenia. Dla potrzeb użytkowników urządzeń radionadawczych wystarczy określić tylko cztery podstawowe parametry charakteryzujące każdy nadajnik radiowy (niezależnie czy jest radiotelefon strażaka, telefon komórkowy czy wreszcie nadajnik radiofoniczny lub telewizyjny). Te cztery parametry to:

- stałość częstotliwości,
- moc wyjściowa wielkiej częstotliwości,
- rodzaj modulacji,
- rodzaj emisji.

Stałość częstotliwości **–** jest to parametr określający stosunek bezwzględnej maksymalnej zaobserwowanej odchyłki częstotliwości, pod wpływem czynników destabilizujących np. temperatury, do częstotliwości nominalnej kanału radiowego $k = \frac{|\Delta f|}{f_n}$. Decyduje to o stabilnym położeniu konkretnej stacji na osi częstotliwości, czyli niezakłócaniu innych leżących w pobliżu stacji. W praktyce parametr ten nie może

być gorszy niż 10^{-7}. Jeśli ten warunek nie będzie spełniony to takiego nadajnika nie można oddać do eksploatacji.

Moc wyjściowa wielkiej częstotliwości – oznacza ile energii elektromagnetycznej może wypromieniować system antenowy radiostacji. Od tego parametru zależy zasięg radiostacji. Maksymalna dozwolona moc promieniowana określona jest w zezwoleniu na eksploatację np. CB radio może pracować z mocą 4 W, stacja bazowa w JRG moc do 30 W (zalecana 16 W).

Rodzaj modulacji – ten parametr określa jakim rodzajem modulacji ma pracować nadajnik np. Program 1 i 2 polskiego radia z modulacją amplitudy AM a program 3 PR z modulacją częstotliwości.

Rodzaj emisji – najtrudniejszy do zdefiniowania parametr nadajnika. Emisją radiową będziemy nazywać promieniowanie elektromagnetyczne wysyłane przez antenę nadajnika zawierające nałożona informację. Generalnie więc, chodzi o to aby tak ukształtować sygnał promieniowany przez antenę, aby był on suboptymalny dla aktualnych warunków propagacyjnych. Na przykład rozważmy emisję A3 (telefonia z dwuwstęgową modulacją amplitudy, rys. 5.7). W tym przypadku w widmie sygnału zmodulowanego mamy prążek na częstotliwości nośnej i dwie wstęgi boczne. Prążek nośnej to 50% wypromieniowanej energii i wstęgi boczne po 25%. Informacja zawarta jest we wstęgach bocznych, więc szkoda „tracić" 50% mocy na prążek nośnej. Gdyby ograniczyć moc emitowaną na nośnej F a „zaoszczędzoną" moc dołożyć do wstęg bocznych (emisja A3A) to uzyskamy korzystniejsze warunki propagacyjne (większy zasięg). Idąc dalej ta sama informacja jest w każdej ze wstęg bocznych, więc może wystarczy przesłać tylko jedną z nich i jeszcze mocniej ograniczyć prążek nośnej, to warunki propagacyjne będą jeszcze korzystniejsze (emisja A3J).

Oznaczenia emisji radiowych według ITU.

Od 1 stycznia 1982 r. obowiązują nowe symbole dla oznaczenia emisji radiowych. Zostały one przyjęte przez Światową Administracyjną Konferencję Radiową (WARC) w Genewie w roku 1979. Trzy pierwsze symbole oznaczające rodzaj emisji są obowiązkowe; mogą one być uzupełnione w razie potrzeby dwoma dalszymi symbolami. Pierwszy symbol określa rodzaj modulacji podstawowej fali nośnej, drugi

symbol określa naturę sygnału modulującego podstawową falę nośną, zaś trzeci symbol określa typ przekazywanej informacji.

Pierwszy symbol - rodzaj modulacji głównej fali nośnej.

Amplitudowe:

A - Dwie wstęgi boczne

H - Jedna wstęga boczna, pełna fala nośna

R - Jedna wstęga boczna, zredukowana lub regulowana fala nośna

J - Jedna wstęga boczna, wytłumiona fala nośna

B - Niezależne wstęgi boczne

C - Szczątkowa wstęga boczna

Kątowe:

F - Modulacja częstotliwości

G - Modulacja fazy

D - Modulacja w amplitudzie i fazie (jednocześnie lub sekwencyjnie)

Impulsowe:

P - Niemodulowana sekwencja impulsów

K - Sekwencja impulsów modulowanych w amplitudzie

L - Sekwencja impulsów z modulacją szerokości (czasu)

M - Sekwencja impulsów z modulacją położenia (fazy)

Q - Sekwencja impulsów, w których fala nośna jest modulowana kątowo w czasie trwania impulsu

V - Sekwencja impulsów będących kombinacją powyższych lub innych

W - Przypadki nie ujęte powyżej

X - Inne przypadki nie ujęte powyżej

Drugi symbol - natura sygnału

0 - Brak sygnału modulującego

1 - Pojedyńczy kanał modulujący, zawierający informację skwantowaną lub cyfrową, bez użycia podnośnej (bez TDM - multipleksowania z podziałem czasu)

2 - Pojedyńczy kanał modulujący, zawierający skwantowaną lub cyfrową informacją z użyciem podnośnej (bez TDM – multipleksowania z podziałem czasu)

3 - Pojedyńczy kanał modulujący, zawierający informację analogową

7 - Dwa lub więcej kanałów modulujących, zawierających informację skwantowaną lub cyfrową

8 - Dwa lub więcej kanałów modulujących, zawierających informację analogową

9 - Sygnał złożony z jednego lub więcej kanałów zawierających informację skwantowaną lub cyfrową oraz jednego lub więcej kanałów zawierających informację analogową

X - Przypadki nie ujęte powyżej

Trzeci symbol - typ nadawanej informacji

N - Brak nadawanej informacji

A - Telegrafia dla odbioru słuchowego

B - Telegrafia dla odbioru automatycznego

C - Faksymile

D - Transmisja danych, telemetria, zdalne sterowania

E - Telefonia (i radiofonia)

F - Telewizja (sygnał wizji)

W - Kombinacja powyższych

X - Przypadki nie ujęte powyżej

Regulamin Radiokomunikacyjny wymaga również, aby oznaczenie emisji zawierało informację o zajmowanej szerokości pasma. Dlatego też wprowadzono nową metodę określania szerokości pasma za pomocą czteroznakowego kodu. Trzy cyfry określają szerokość pasma, zaś litera umieszczona w miejsce znaku dziesiętnego określa użytą jednostkę częstotliwości. Powyższy kod umieszcza się przed oznaczeniem rodzaju emisji.

Szerokości pasma pomiędzy 0,001 i 999 Hz są wyrażane w hecrcach (Hz) - litera H

Szerokości pasma pomiędzy 1,00 i 999 kHz są wyrażane w kilohercach (kHz) - litera K

Szerokości pasma pomiędzy 1,0 i 999 MHz są wyrażane w megahercach (MHz) - litera M

Szerokości pasma pomiędzy 1,0 i 999 GHz są wyrażane w gigahercach (GHz) - litera G

Na przykład szerokość pasma 23,4 Hz oznacza się 23H4, a szerokość pasma 0,5 Hz - H500.

Tabela 5.1. *Stare i nowe oznaczenia częściej stosowanych emisji*

Stare	**Rodzaj emisji**	**Nowe**
A0	Fala ciągła bez modulacji	N0N
A1	Fala ciągła z kluczowaną nośną (CW)	A1A
A2	Fala ciągła modulowana dwuwstęgowo kluczowanym tonem	A2A
A2A	Fala ciągła jednowstęgowo ze zredukowaną nośną	R2A
A2H	Fala ciągła modulowana jednowstęgowo kluczowanym tonem z pełną nośną	H2A
A2J	Fala ciągła modulowana jednowstęgowo kluczowanym tonem z wytłumioną nośną	J2A
A3	Telefonia dwuwstęgowa z modulacją amplitudy (AM)	A3E
A3A	Telefonia jednowstęgowa ze zredukowaną nośną	R3E
A3B	Telefonia jednowstęgowa z dwoma niezależnymi wstęgami bocznymi	B8E
A3H	Telefonia jednowstęgowa z pełną falą nośną	H3E
A3J	Telefonia jednowstęgowa z wytłumioną nośną	J3E
F1	Kluczowanie częstotliwości bez użycia tonu modulującego	F1B
F2	Kluczowanie częstotliwości z użyciem tonu modulującego	F2B
F3	Telefonia z modulacją częstotliwości (FM)	F3E
A7A	Telegrafia jednowstęgowa z kluczowaniem tonem modulującym ze zredukowaną falą nośną	R7A
A9B	Dwie niezależne wstęgi boczne dla kombinacji telefonii i telegrafii	B9W

Reasumując, w podstawowym oznaczeniu rodzaju emisji:

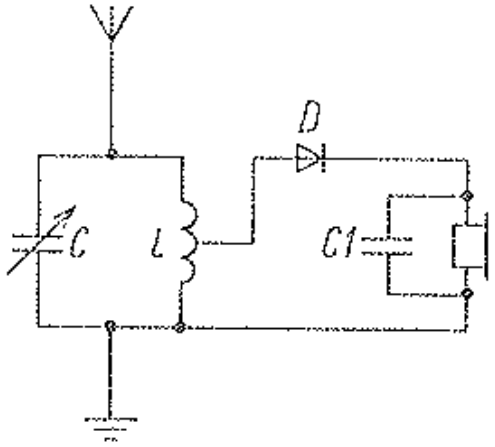
- pierwszy symbol oznacza **rodzaj modulacji,**
- drugi określa **naturę sygnału modulującego** falę nośną,
- trzeci – **typ przekazywanej informacji**.

Na przykład:

- CW – fala ciągła z kluczowaną nośną; A1A
- AM – telefonia dwuwstęgowa z modulacją amplitudy; A3E
- SSB – telefonia jednowstęgowa z wytłumioną falą nośną; J3E
- FM – telefonia z modulacją częstotliwości; F3E

5.4. Urządzenia radioodbiorcze

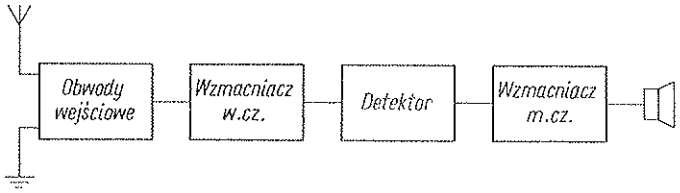
Schemat najprostszego odbiornika radiowego przedstawia rysunek 5.9. Składa się on z anteny, obwodu rezonansowego LC, detektora i słuchawki. Obwód rezonansowy LC jest dostrajany kondensatorem C (trymerem) do odbieranego sygnału w.cz. Do obwodu rezonansowego dołączona jest antena, która jest źródłem sygnału wielkiej częstotliwości, natomiast do odczepu cewki L dołączona jest dioda D. Pełni ona rolę detektora. Obciążeniem detektora jest rezystancja uzwojenia słuchawki. Kondensator C1 stanowi zwarcie dla napięć w.cz. i rozwarcie dla napięć małej częstotliwości (sygnału niosącego informację). Prąd m.cz. otrzymany w procesie demodulacji, płynie przez uzwojenie słuchawki, w której jest przetwarzany na falę akustyczną. Tego typu odbiorniki są wykorzystywane od początku XX wieku. W roku 1906 w USA Dunwood i Picard budują odbiornik kryształkowy z detektorem karborundowym (patent). W roku 1905, Karl Ferdinand Braun upowszechnia wynaleziony przez siebie detektor kryształkowy („dioda" galenowa i pirytowo miedziana). Umożliwiał on odbiór słuchowy. Detektorem mógł być, zetknięty z cienkim drutem (sprężynką) kryształ pirytu, galeny (siarczek ołowiu) lub karborundu, czyli prymitywna dioda metal – półprzewodnik powszechnie nazywana kryształkiem. Prekursorem rozwoju systemów radiowych w Polsce był profesor Stefan Manczarski, który w roku 1922 skonstruował pierwszy polski odbiornik radiowy oraz nowego typu anteny. W lutym 1925 roku uruchomiono pierwsza stację nadawczą Polskiego Towarzystwa Radiotechnicznego w Warszawie przy ulicy Narbutta 29 na Mokotowie o mocy 500 watów.



Rys.5.9. *Odbiornik detektorowy*

Odbiorniki detektorowe mają małą czułość i małą selektywność. Przeznaczone są one do odbioru stacji lokalnej. Ich zaletą było również to, że nie wymagały źródła zasilania. Do zasilania używały energii przechwyconej fali elektromagnetycznej. Trzeba było jednak używać długich anten, a natężenie dźwięku było małe (tylko odbiór słuchawkowy). Inną wada odbiorników tego typu była słaba rozdzielczość. Kondensator lub cewka w obwodzie strojonym odbiornika były regulowane tak, aby dostroić się do częstotliwości, na której nadawała dana stacja. Jednak proste obwody nie były w stanie zupełnie wyeliminować sygnałów o zbliżonych częstotliwościach. Problem ten stawał się coraz poważniejszy wraz ze wzrostem liczby nadających stacji. Zmiany konstrukcyjne polepszające rozdzielczość doprowadzały do znacznego spadku czułości, a to oznaczało cichszy odbiór audycji.

Sytuację poprawiło wprowadzenie odbiorników lampowych (lata trzydzieste ubiegłego wieku), w których do wzmacniania sygnałów zastosowano lampy elektronowe. Można było produkować odbiorniki charakteryzujące się zarówno dużą czułością jak i rozdzielczością. Pozwoliło to na zastosowanie w odbiorniku głośnika, tak, aby każda osoba przebywająca w pomieszczeniu mogła słuchać audycji. Tak narodziły się odbiorniki o wzmocnieniu bezpośrednim. Na rys. 5.10 przedstawiono schemat blokowy odbiornika o wzmocnieniu bezpośrednim.



Rys.5.10. *Schemat blokowy odbiornika o wzmocnieniu bezpośrednim*

Przy budowie takich odbiorników o wysokich parametrach technicznych, pojawiają się trudne do przezwyciężenia problemy techniczne. Można do nich zaliczyć mniejszą stabilność pracy przy dużej czułości oraz skomplikowaną konstrukcję. Wadą tego rozwiązania jest również fakt, że taki odbiornik odbierał tylko jedną stację nadająca program radiowy. Do odbioru innej potrzebny był następny odbiornik. W czasie drugiej wojny światowej, po zarekwirowaniu przez okupanta wszystkich odbiorników radiowych, wrócono do rozwiązań z lat dwudziestych ubiegłego wieku czyli stosowaniu odbiorników detektorowych. Czytając wspomnienia jeńców oflagów czy stalagów wiemy, że konstruowali Oni takie odbiorniczki (małe wymiary, brak zasilania czyli

łatwe do ukrycia) do odbioru audycji Radia Londyn, aby mieć wiadomości o postępach na frontach II wojny światowej.

Problemy z odbiornikami o wzmocnieniu bezpośrednim można rozwiązać taniej i mniejszym kosztem osiągnąć wysokie parametry stosując odbiorniki superheterodynowe, czyli odbiorniki z przemianą częstotliwości. Odbiór superheterodynowy polega na przetwarzaniu odbieranego sygnału w.cz. na sygnał w.cz. o innej częstotliwości zwanej częstotliwością pośrednią. Częstotliwość pośrednia jest równa sumie lub różnicy częstotliwości odbieranego sygnału i częstotliwości heterodyny.

$$F_p = F_s - F_h$$

$$F_p = F_h - F_s$$

przy czym: F_p – częstotliwość pośrednia, F_s – częstotliwość odbieranego sygnału,

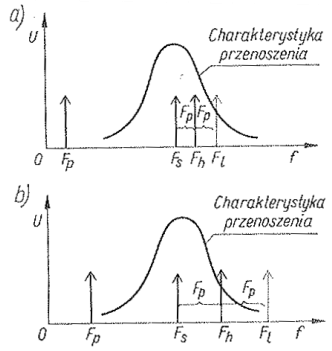
F_h – częstotliwość heterodyny

Częstotliwość pośrednia powinna być wybierana w takim zakresie, w którym nie pracuje żaden nadajnik oraz aby można było zrealizować wzmacniacz p.cz. o żądanych parametrach jak np. wzmocnienie, szerokość przenoszonego pasma. W odbiornikach AM wartość częstotliwości pośredniej wybiera się z w paśmie częstotliwości 430 do 470 kHz. Najczęściej w odbiornikach AM stosuje się częstotliwość pośrednią równą 455 kHz lub 465 kHz, natomiast dla odbiorników FM wartość częstotliwości pośredniej wynosi 10.7 MHz. Podczas przemiany częstotliwości mogą powstać zakłócenia wywołane obecnością sygnału lustrzanego. Są one specyficzne dla odbioru superheterodynowego. Możliwości ich usunięcia są ściśle związane z wyborem częstotliwości pośredniej. Jeśli odbierany jest sygnał w.cz. o częstotliwości F_s, to w celu otrzymania sygnału o częstotliwości pośredniej F_p sygnał heterodyny musi mieć częstotliwość F_h różną (np. większą) o wartość F_p od częstotliwości sygnału. Jednocześnie może się zdarzyć, że do anteny odbiornika dochodzi inny sygnał w.cz., którego częstotliwość F_l jest większa o wartość F_p od sygnału heterodyny. Jeżeli sygnał o częstotliwości F_l, zwany sygnałem lustrzanym, nie jest wytłumiony przez obwody wejściowe odbiornika lub obwody wejściowe wzmacniacza w.cz., to w wyniku w wyniku mieszania otrzymamy dwa sygnały o częstotliwości pośredniej. Jeden będzie pochodził od właściwego sygnału w.cz., a drugi od zakłócającego sygnału w.cz. (sygnał lustrzany).

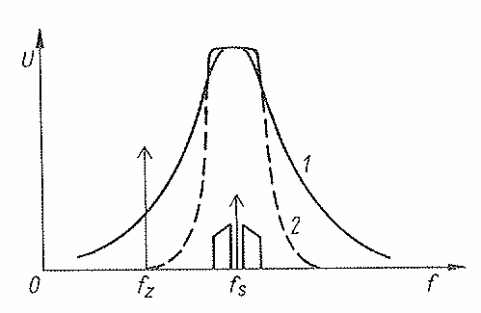
W takim przypadku mamy do czynienia z odbiorem zakłócanym przez sygnały

lustrzane. Przypadek taki przedstawia rysunek 5.11. Dla uniknięcia zakłóceń pochodzących od sygnałów lustrzanych należy wybierać częstotliwość pośrednią możliwie dużą (rys. 5.11b). Przy dużej częstotliwości pośredniej częstotliwość sygnału lustrzanego F_l znajduje się w znacznej odległości od sygnału pożądanego F_s. Częstotliwość F_l sygnału lustrzanego leży daleko poza pasmem przenoszenia obwodów wejściowych, jest więc skutecznie tłumiona przez obwody wejściowe i odbiór pożądanego sygnału jest niezakłócony (rysunek 5.12).

We wzmacniaczu p.cz. łatwiej jest osiągnąć duże wzmocnienie i dużą selektywność, gdy częstotliwość pośrednia jest mała. Aby pogodzić te sprzeczne z sobą wymagania stosuje się podwójną przemianę częstotliwości. Pierwsza częstotliwość pośrednia jest duża i zapewnia skuteczne tłumienie sygnałów lustrzanych. Druga częstotliwość pośrednia jest mała, co pozwala na uzyskanie odpowiedniej selektywności odbiornika radiowego.

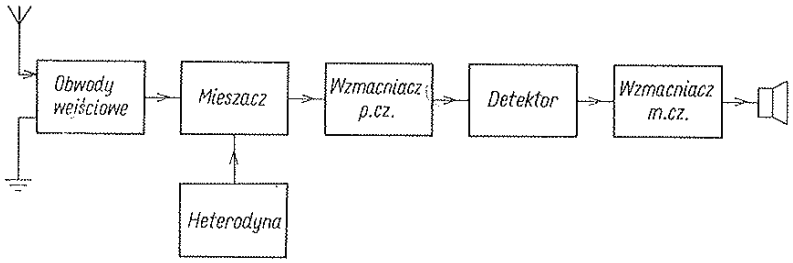


Rys.5.11. *Rozkład prążków w widmie częstotliwości przy superheterodynowym odbiorze*
a) mała częstotliwość pośrednia,
b) duża częstotliwość pośrednia.

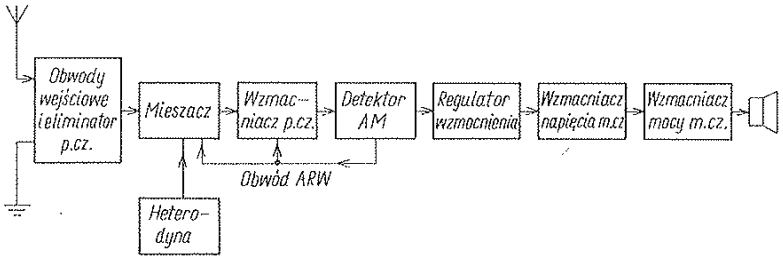


Rys.5.12. *Charakterystyka przenoszenia częstotliwości obwodu wejściowego*
1 – charakterystyka przenoszenia częstotliwości obwodu o małej selektywności,
2 – charakterystyka przenoszenia częstotliwości obwodu o dużej selektywności.

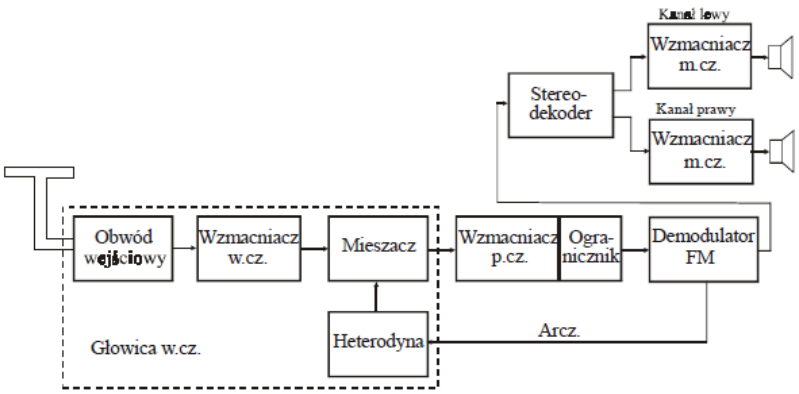
Reasumując, w celu uniknięcia zakłóceń pochodzących od sygnałów lustrzanych wybiera się częstotliwość pośrednią możliwie dużą lub stosuje się podwójną przemianę częstotliwości (dwie częstotliwości pośrednie). Pierwsza częstotliwość pośrednia jest duża, np. 2 MHz natomiast druga jest mała, np. 455 kHz. W najnowszych konstrukcjach odbiorników radiofonicznych pierwsza częstotliwość pośrednia może mieć nawet 40 MHz. Na rys. 5.13 i 5.14 przedstawiono schemat blokowy odbiornika superheterodynowego przeznaczonego do odbioru sygnałów z modulacją AM, natomiast na rys. 5.15 przedstawiono schemat blokowy odbiornika przeznaczonego do odbioru sygnałów stereofonicznych z modulacją FM.



Rys.5.13. *Schemat blokowy odbiornika superheterodynowego.*

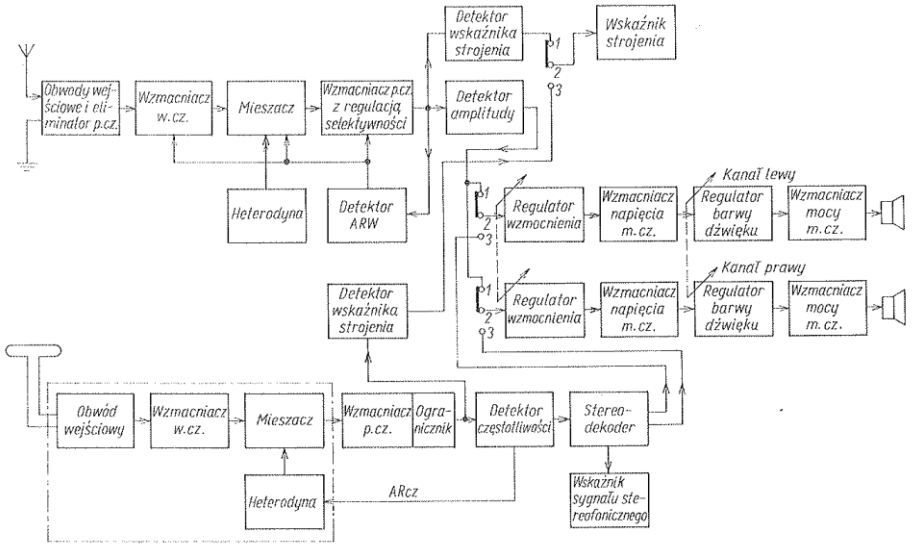


Rys.5.14. *Schemat blokowy odbiornika superheterodynowego z układem ARW (Automatyczna Regulacja Wzmocnienia)*



Rys.5.15. *Schemat blokowy odbiornika superheterodynowego FM (ARCz – Automatyczna regulacja częstotliwości)*

Oczywiście w elektronicznym sprzęcie powszechnego użytku, kłopotem by było aby mieć oddzielny odbiornik do odbioru audycji z modulacją AM (fale długie, średnie i krótkie) oraz oddzielny do odbioru audycji z modulacją FM (fale ultrakrótkie). W tej sytuacji budujemy odbiorniki o dwu torach w.cz. a po detekcji tor małej częstotliwości jest już wspólny dla obu rodzajów modulacji. Schemat blokowy takiego rozwiązania przedstawia rysunek 5.16.



Rys.5.16. *Schemat odbiornika stereofonicznego AM/FM*
Zwarte styki przełącznika: 1 – 2 → odbiór AM, 2 – 3 → odbiór FM

W torze AM przed mieszaczem stosuje się wzmacniacz wielkiej częstotliwości. Jego zastosowanie poprawia stosunek sygnału do szumu dla odbieranych sygnałów w.cz. i jednocześnie zwiększa to czułość odbiornika radiowego. We wzmacniaczu p.cz. umieszczono regulator selektywności, w którym reguluje się szerokość pasma przenoszenia odbiornika radiowego. Przy odbiorze bardzo słabych sygnałów zwężenie pasma przenoszenia odbiornika radiowego zmniejsza zakłócający wpływ silnych sygnałów o częstotliwościach bliskich częstotliwości sygnału odbieranego. Przy odbiorze stacji lokalnej odbierany sygnał jest tak duży, ze sygnały pochodzące od innych stacji praktycznie nie zakłócają odbioru. W tym przypadku pasmo przenoszenia odbiornika może być znacznie szersze, co znacznie poprawia jakość odbieranych sygnałów. W celu zapewnienia mniejszych zniekształceń demodulowanego sygnału napięcie do układu ARW, do wysterowania wskaźnika strojenia i do sterowania wzmacniaczy m.cz., jest pobierana z oddzielnych układów detektorów.

Tor FM odbiornika radiowego składa się z układów: obwodu wejściowego, wzmacniacza w.cz., wzmacniacza p.cz., detektora częstotliwości i detektora sygnału

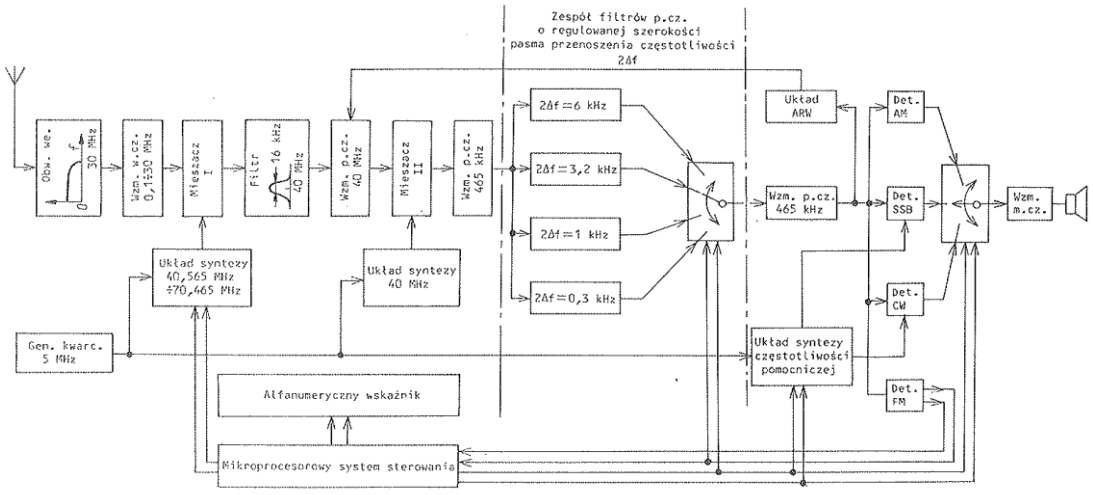
stereofonicznego (jeśli odbiornik jest przystosowany do odbioru takich sygnałów). Początkowe układy toru FM, takie jak wzmacniacz w.cz., mieszacz oraz heterodyna, spełniają podobną rolę jak w torze AM. We wzmacniaczu p.cz. jednocześnie z wzmocnieniem odbieranego sygnału jest ograniczona jego amplituda (modulacja FM). Do detektora częstotliwości doprowadzony jest sygnał o stałej amplitudzie, co zapewnia wyższą jakość sygnału zdemodulowanego. Jeśli odbierany jest sygnał stereofoniczny, to napięcie zdemodulowane jest doprowadzone z detektora częstotliwości do dekodera stereofonicznego. Na wyjściu dekodera otrzymuje się rozdzielony sygnał lewego i prawego kanału. Praca dekodera jest sygnalizowana świeceniem żarówki kontrolnej (diody LED). W przypadku odbioru sygnału monofonicznego dekoder nie działa co sygnalizuje wyłączona żaróweczka kontrolna.

W torze FM stosuje się układ ARCz, który zapewnia automatyczne dostrojanie się heterodyny do częstotliwości odbieranego sygnału. Niekiedy może być również stosowana automatyczna regulacja wzmocnienia ARW. Sygnał stereofoniczny po zdekodowaniu, jest wzmacniany przez dwa niezależne wzmacniacze m.cz. (kanału: lewego i prawego). W każdym wzmacniaczu m.cz. wyróżnia się następujące układy funkcjonalne: regulator wzmocnienia, wzmacniacz napięciowy m.cz., regulator barwy dźwięku i wzmacniacz mocy. Regulator barwy dźwięku (w sprzęcie klasy wyższej korektor graficzny – equalizer) umieszcza się zazwyczaj za wzmacniaczem napięciowym m.cz. Umożliwia on niezależną regulację niskich i wysokich tonów.

Przy odbiorze sygnałów AM lub FM monofonicznych oba wzmacniacze m.cz. są sterowane tym samym sygnałem. Znamionowa moc wyjściowa odbiornika radiowego jest rzędu kilkudziesięciu watów. Do jej przetwarzania na moc akustyczną są stosowane zespoły głośnikowe (popularnie nazywane kolumnami) o wysokiej jakości przetwarzania (o paśmie przenoszenia co najmniej 50 do 12500 Hz; norma DIN 45500 na sprzęt Hi – Fi). Należy pamiętać, że aby uniknąć zniekształceń chrypieniowych (nielinearenych) moc dostarczona do przetwornika elektroakustycznego nie powinna przekraczać 20% mocy znamionowej tego przetwornika.

Na rysunku 5.17 przedstawiono schemat profesjonalnego odbiornika radiowego o nowoczesnej konstrukcji sterowanego mikroprocesorem (rozwiązanie stosowane w większości nowego sprzętu radiowego stosowanego w służbach porządku publicznego: Policja, PSP, pogotowie Ratunkowe czy Systemy Zarządzania Kryzysowego). Obwód wejściowy takiego odbiornika wykonany jest w postaci filtru dolnoprzepustowego. Filtr ten przenosi całe pasmo odbieranych sygnałów. Sygnał

z obwodu wejściowego jest doprowadzany do wzmacniacza szerokopasmowego i następnie do pierwszego mieszacza. Pierwsza częstotliwość pośrednia wynosi 40,465 MHz. Jako pierwszą heterodynę zastosowano układ syntezy częstotliwości wytwarzający sygnał o częstotliwości w zakresie 40,565 – 70,465 MHz. Umożliwia to realizację ciągłego przestrajania heterodyny dla całego pasma odbieranych częstotliwości. Częstotliwość sygnału przestrajana jest ze skokiem 10 Hz.



Rys.5.17. *Schemat odbiornika sterowanego mikroprocesorem*

We wzmacniaczu p.cz. *I* (wzmacniacz pierwszej częstotliwości pośredniej) stosuje się zwykle filtry ceramiczne o paśmie przenoszenia kilkunastu kiloherców (około 16 kHz). Sygnał po wzmocnieniu przez wzmacniacz p.cz. *I* jest doprowadzony do mieszacza *II*. Druga częstotliwość pośrednia wynosi 465 kHz, natomiast częstotliwość *II* heterodyny – 40 MHz. Sygnał drugiej heterodyny jest wytwarzany w układzie syntezera. Szerokość pasma przenoszenia częstotliwości wzmacniacza p.cz. *II* jest regulowana skokowo od 0,3 do 6 kHz. Sygnał ze wzmacniacza p.cz. *II* jest doprowadzony do zespołu detektorów umożliwiających odbiór sygnałów z różną modulacją. Omawiany odbiornik jest przystosowany do odbioru sygnałów z modulacją AM (dwie wstęgi boczne i fala nośna), z modulacją SSB (jednowstęgowa modulacja amplitudy), z modulacją CW (z kluczowaną amplitudą – telegrafia). Do detektorów SSB i CW jest doprowadzony sygnał z lokalnego dodatkowego generatora. Przy pracy z detektorem SSB częstotliwość sygnału generatora dodatkowego jest przestrajana w zakresie 457 ÷ 473 kHz (465 ± 8 kHz), natomiast przy pracy z detektorem CW *(Continuous Wave)* częstotliwość sygnału generatora dodatkowego jest przestrajana w zakresie 465,08 ± 466,5 kHz. Sygnał generatora dodatkowego jest wytwarzany przez układ syntezatora o skoku 10 Hz. Oczywiście, odbiornik umożliwia odbiór sygnałów

z modulacją FM. Do wszystkich układów syntezatora jest dostarczany sygnał o dużej stałości częstotliwości ze wspólnego generatora kwarcowego.

Zdemodulowany sygnał, po wzmocnieniu we wzmacniaczu m.cz., jest doprowadzany do głośnika.

Do sterowania poszczególnych podzespołów odbiornika wykorzystuje się mikroprocesor. Sygnał mikroprocesorowy steruje wyborem częstotliwości sygnału pierwszej heterodyny i generatora dodatkowego. Steruje również szerokością pasma przenoszenia częstotliwości wzmacniacza p.cz. *II* oraz steruje wyborem układu detektora. System mikroprocesorowy zwiększa funkcjonalność odbiornika radiowego, np. umożliwia zaprogramowanie kilku częstotliwości sygnału odbieranego, do których odbiornik, po naciśnięciu jednego przycisku, sam szybko dostroi się. System mikroprocesorowy umożliwia automatyczne przestrajanie odbiornika w wybranym zakresie częstotliwości (skaning).

Wartość częstotliwości sygnału odbieranego dostrojenia odbiornika radiowego, rodzaj modulacji i inne dane są wyświetlane na polu wskaźnikowym (wskaźnik alfanumeryczny).

5.4.1 Parametry odbiorników radiowych.

Podobnie jak w przypadku nadajników radiowych tak i odbiorniki radiowe opisuje się czterema parametrami. Są to:

- selektywność,
- czułość,
- moc wyjściowa małej częstotliwości,
- rodzaj modulacji.

Selektywność – jest to zdolność odbiornika radiowego do wydzielania sygnału o żądanej częstotliwości spośród innych sygnałów indukowanych w antenie. Wartość selektywności określa się na podstawie charakterystyki przenoszenia toru w.cz. odbiornika. O charakterystyce przenoszenia toru w.cz. decyduje charakterystyka wzmacniacza pośredniej częstotliwości (stopni pośredniej częstotliwości). Na rysunku 5.18a przedstawiono charakterystykę przenoszenia wzmacniacza p.cz. o częstotliwości rezonansowej F_0. Na podstawie tej charakterystyki wyznacza się tłumienie dla sygnału o częstotliwości różniącej się o ΔF_1 od częstotliwości F_0, np. dla sygnału o częstotliwości $F_0 + \Delta F_1$. Tłumienie to nosi nazwę selektancji i jest liczbową miarą selektywności.

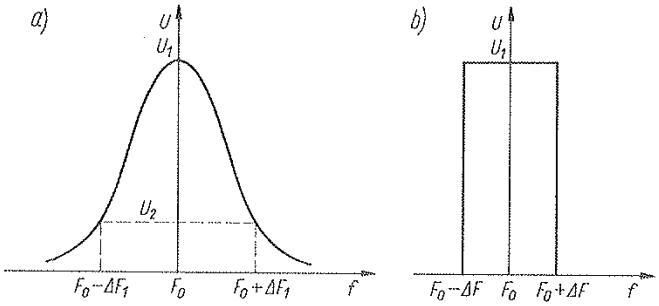
Selektancję można obliczyć ze wzoru:

$$S_{Fo} + \Delta F_1 = 20 \log \frac{U_1}{U_2}$$

Na rysunku 5.18b przedstawiono idealną krzywą przenoszenia wzmacniacza p.cz. Szerokość idealnej krzywej przenoszenia wzmacniacza p.cz. powinna być równa szerokości pasma zajmowanego przez odbierany sygnał w.cz. Dla częstotliwości leżących poza pasmem przenoszenia tłumienie jest nieskończenie duże. Do jakościowego określenia krzywej przenoszenia w funkcji częstotliwości służy współczynnik prostokątności. Współczynnikiem prostokątności nazywa się stosunek szerokości pasma przenoszenia dla spadku wzmocnienia o 3 – decybelach do szerokości pasma przenoszenia dla spadku wzmocnienia o 20 – decybelach. Współczynnik prostokątności oblicza się ze wzoru $p = \frac{2\Delta f_1}{2\Delta f_2}$ w którym:

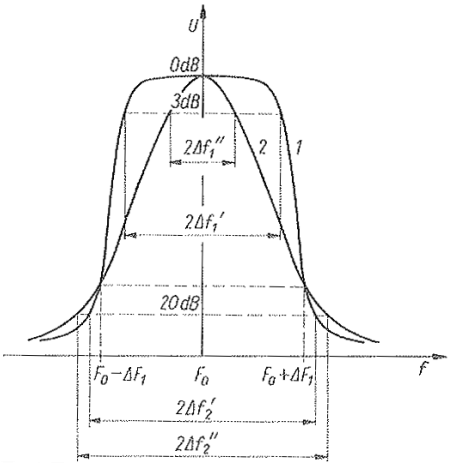
$2\Delta f_1$ – szerokość pasma przenoszenia dla spadku wzmocnienia o 3 – decybelach;

$2\Delta f_2$ – szerokość pasma przenoszenia dla spadku wzmocnienia o 20 – decybelach.



Rys.5.18. *Charakterystyka przenoszenia wzmacniacza p.cz.:*
a) rzeczywista krzywa przenoszenia wzmacniacza p.cz.,
b) idealna krzywa przenoszenia wzmacniacza p.cz.

Na rysunku 5.19 przedstawiono dwie krzywe przenoszenia o tej samej wartości selektancji (dla ΔF_1), ale o różnym współczynniku prostokątności. Krzywa *1* ma większy współczynnik prostokątności niż krzywa przenoszenia *2*. Szerokość pasma przenoszenia przy 3 – decybelowym spadku wzmocnienia jest też różna. Odbiornik radiowy o charakterystyce przenoszenia określoną krzywą *2* ma dużo większe pasmo przenoszenia częstotliwości niż odbiornik o charakterystyce przenoszenia określonej krzywą *1*. Sygnał na wyjściu tego odbiornika (o charakterystyce oznaczonej *2*) może być zniekształcony.



Rys.5.19. *Charakterystyka przenoszenia wzmacniaczy p.cz. o tej samej selektancji*
1 – charakterystyka przenoszenia o większym współczynniku prostokątności,
2 – charakterystyka przenoszenia o mniejszym współczynniku prostokątności.

Czułość odbiornika radiowego – określa najniższy poziom sygnału, jaki może odebrać odbiornik dostrojony do częstotliwości tego sygnału. Czułość może być ograniczona wzmocnieniem odbiornika lub jego szumami własnymi. Z tego powodu występuje wiele definicji czułości. Najczęściej posługujemy się pojęciami czułości maksymalnej i użytkowej.

Czułość maksymalna, określa najniższy poziom sygnału wejściowego, o parametrach podanych poniżej, przy którym otrzymuje się znormalizowaną wartość mocy na wyjściu przy maksymalnym wzmocnieniu odbiornika radiowego. Przy określaniu czułości maksymalnej szumy własne odbiornika radiowego nie są brane pod uwagę. Czułość odbiorników AM przeznaczonych do odbioru sygnałów z modulacją amplitudy określa się dla sygnału w.cz. przy głębokości modulacji równej 30%. Częstotliwość modulująca wynosi 1000 lub 400 Hz. Dla odbiorników FM z modulacją częstotliwości, przeznaczonych do odbioru sygnałów w.cz. o dewiacji maksymalnej F_{max} = 50 kHz, czułość określa się przy dewiacji ΔF = 15 kHz i częstotliwości sygnału modulującego 1000 Hz lub 400 Hz.

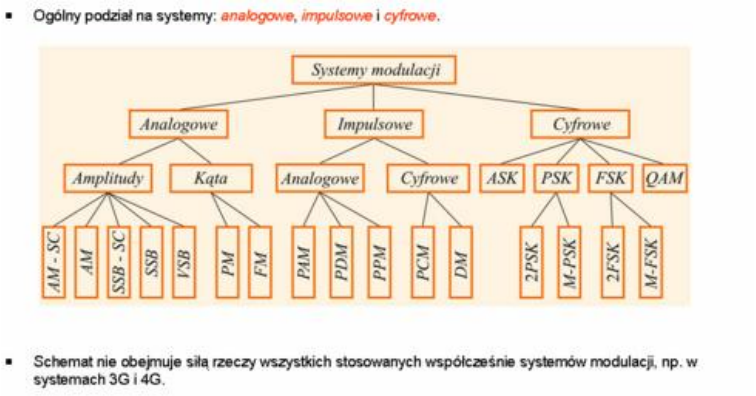
Jako znormalizowaną wartość mocy wyjściowej przyjmuje się jedną z następujących wartości: 1, 5, 50 lub 50 mW. Czułość określana jest przy największej znormalizowanej wartości mocy, ale nie większej niż 0,1 wartości największej mocy wyjściowej.

Czułość użytkowa odbiornika, określa najniższy poziom sygnału w.cz. (o parametrach podanych wcześniej) na wejściu odbiornika, przy którym uzyskuje się

znormalizowaną wartość mocy na wyjściu przy określonym stosunku mocy sygnału użytecznego P_s do mocy szumów własnych odbiornika P_{sz}. Moc sygnału użytecznego oraz moc szumów własnych jest mierzona na wyjściu odbiornika. Przy wyznaczaniu czułości użytkowej wartość wzmocnienia badanego odbiornika radiowego powinna być dobrana tak, aby stosunek mocy sygnału P_s użytecznego do mocy szumów P_{sz} był nie mniejszy niż dopuszczalna wartość. Zazwyczaj stosunek ten podaje się w decybelach (dB) $n = 10 \log \frac{P_s}{P_{sz}}$. Dla odbiorników AM czułość użytkowa jest określana jest przy stosunku mocy sygnału do mocy szumów równym 10 dB lub 20 dB. W przypadku odbiorników FM czułość użytkowa jest określana przy stosunku mocy sygnału do mocy szumów równym 26 dB. Czułość odbiornika jest podawana dla każdego zakresu fal, należy jednak pamiętać, że w przedziale jednego zakresu fal zależy ona również od częstotliwości odbieranej.

Moc wyjściowa małej częstotliwości – jest to wartość wyjściowa mocy elektrycznej dostarczonej do obciążenia (głośnika). Maksymalna wartość mocy wyjściowej, przy której zniekształcenia sygnału na wyjściu odbiornika radiowego są mniejsze niż 10% ($h \leq 10\%$) nosi nazwę maksymalnej mocy wyjściowej odbiornika. Wartość maksymalnej mocy wyjściowej jest zależna od przeznaczenia odbiorników radiowych. Najmniejsze odbiorniki słuchawkowe mają maksymalną moc wyjściową rzędu $1 \div 10$ mW, natomiast odbiorniki klasy Hi – Fi mają maksymalną moc wyjściową rzędu kilkudziesięciu watów.

Rodzaj modulacji – określa do odbioru jakich sygnałów w.cz. (jak zmodulowanych) jest przystosowany konkretny odbiornik radiowy. Obecnie stosuje się wiele różnych typów modulacji zarówno analogowych jak impulsowych. Najczęściej stosowane systemy modulacji i ich klasyfikację przedstawia rysunek 5.20.



Rys.5.20. *Klasyfikacja systemów modulacji*

Na uwagę zasługuje fakt stosowania czterech różnych modulacji amplitudy:

- **AM** *(Amplitude Modulation)* – „klasyczna" modulacja amplitudy,
- **AM – SC** *(Amplitude Modulation Suppressed Carrier)* – modulacja amplitudy z wytłumioną falą nośną,
- **SSB** *(Single Side Band)* – jednowstęgowa modulacja amplitudy z falą nośną,
- **SSB – SC** *(Single Side Band Suppressed Carrier)* – jednowstęgowa modulacja amplitudy z wytłumioną falą nośną,
- **VSB** *(Vestigal Side Band)* – rodzaj modulacji amplitudy zawierającej pozostałości dolnej wstęgi bocznej (zredukowana dolna wstęga boczna), stosowana między innymi w transmisji sygnału telewizyjnego (analogowa naziemna).

Istotnym jest również fakt, że dla potrzeb radiokomunikacji Ziemia została podzielona na 3 regiony radiokomunikacyjne:

Rejon 1 - Europa wraz z Islandią, Rosja, Syberia, Mongolia, Mongolia, Turcja, Syria, Liban, Afryka Północna i część Iranu.

Rejon 2 - Ameryka Południowa i Północna, region Morza Karaibskiego, Grenlandia
i Hawaje.

Rejon 3 - Australia, Nowa Zelandia, Azja bez Syberii i Mongolii oraz pozostała część Afryki.

W regionie radiokomunikacyjnym 1 dla potrzeb emisji radiofonicznych (radiodyfuzji), zgodnie z Krajową Tablicą Przeznaczeń Częstotliwości (punkt 5.1) przydzielono następujące zakresy częstotliwości:

- fale długie 148,5 ÷ 283,5 kHz,
- fale średnie 526,5 ÷ 1606,5 kHz.
- fale pośrednie 2300 ÷ 2498 kHz (dla radiofonii tropikalnej),
  3200 ÷ 3400 kHz (dla radiofonii tropikalnej).
- fale krótkie: pasmo 75 m 3950 ÷ 4000 kHz,
  pasmo 60 m 4750 ÷ 4996 kHz (dla radiofonii tropikalnej),
  5005 ÷ 5060 kHz (dla radiofonii tropikalnej),
  pasmo 49 m 5950 ÷ 6200 kHz,
  pasmo 41 m 7100 ÷ 7300 kHz,
  pasmo 31 m 9500 ÷ 9900 kHz,
  pasmo 25 m 11650 ÷ 12050 kHz,

pasmo 21 m 13600 ÷ 13800 kHz,
pasmo 19 m 15100 ÷ 15600 kHz,
pasmo 16 m 17550 ÷ 17900 kHz,
pasmo 13 m 21450 ÷ 21850 kHz,
pasmo 11 m 25670 ÷ 26100 kHz.

- fale ultrakrótkie (UKF):

wg normy OIRT *(Organization International de Radiodiffusion et de Television)* 66,78 ÷ 74,8 MHz,
wg normy CCIR *(Comite Consultatif International des Radiocommunication)* 87,5 ÷ 108 MHz.

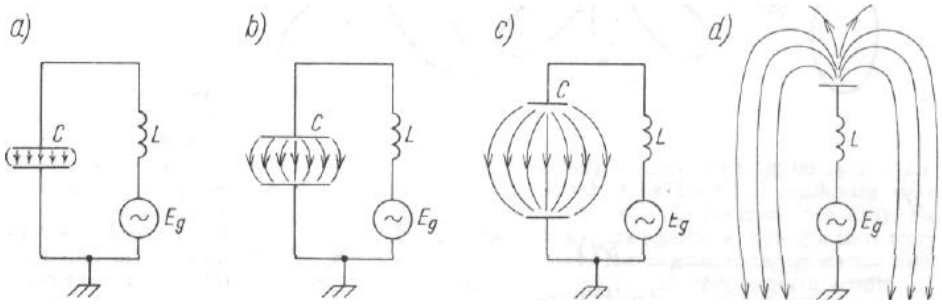
Odbiorniki radiowe w zależności od przeznaczenia i klasy są przystosowane do odbioru różnej liczby zakresów fal. Popularne, małe, przenośne odbiorniki radiowe zazwyczaj są przystosowane do odbioru fal średnich i ultrakrótkich. Odbiorniki radiowe wysokiej klasy są przystosowane do odbioru wszystkich zakresów fal.

Ponadto do potrzeb radiodyfuzji w zakresie fal metrowych przewidziano zakres 174 ÷ 230 MHz a w zakresie fal decymetrowych zakresy 470 ÷ 862 MHz i 1452 ÷ 1467 MHz. Dla radiodyfuzji satelitarnej przewidziano zakresy: 11,7 ÷ 12,5 GHz, 21,1 ÷ 22,0 GHz, 40,5 ÷ 42,5 GHz i 84,0 ÷ 86,0 GHz.

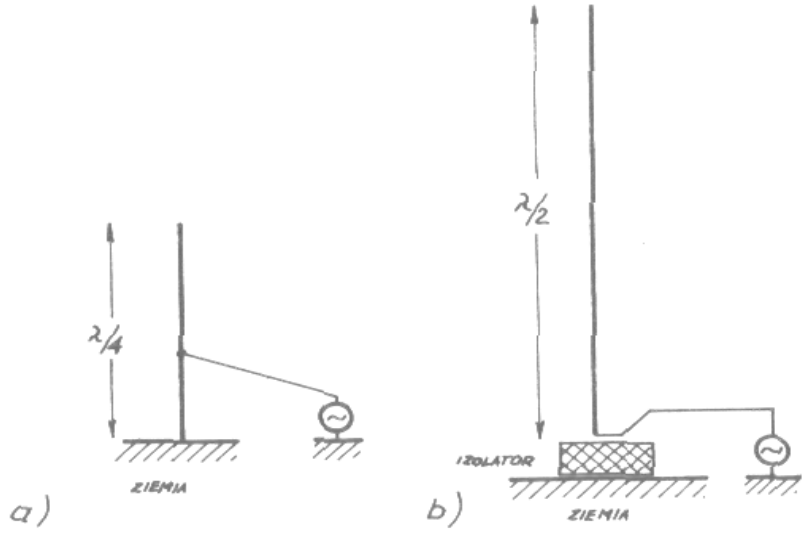
5.5. Urządzenia antenowe

Antena – jest to urządzenie służące do zamiany fal elektromagnetycznych na sygnał elektryczny i odwrotnie. Jest elementem składowym każdego systemu radiowego. W XX wieku najbardziej znanym typem anteny była antena odbiornika radiowego i telewizyjnego. W wieku XXI częściej kojarzona z elementem bezprzewodowych sieci komputerowych lub z odbiorem sygnałów z satelitów. Bardzo popularne są anteny systemów telefonii komórkowej, systemów trankingowch i radarowych. Antena jest elementem odwracalnym. Oznacza to, że antena może dokonywać przemiany energii w obu kierunkach - prądu w.cz. na falę elektromagnetyczną i fali elektromagnetycznej na prąd (siłę elektromotoryczną). Antena nadawcza może być odbiorczą i na odwrót. Ewentualne różnice dotyczą konstrukcji i wymiarów obu typów anten. W przypadku idealnym pożądane byłoby, aby cała moc prądu zmiennego dostarczanego do anteny była wypromieniowana. Zbliżenie się do tego ideału wymaga tzw. **dostrojenia** anteny. (Antenę możemy rozpatrywać jako

szczególny przypadek obwodu rezonansowego, złożonego z cewki, kondensatora i źródła energii. Obwód taki cechuje się **częstotliwością rezonansową,** dla której amplituda prądu zmiennego płynącego w obwodzie osiąga maksimum. Jeśli w obwodzie takim, uziemionym w odpowiednim punkcie (rysunek 5.21) zaczniemy rozsuwać okładziny kondensatora, to linie sił pola elektrycznego będą obejmowały coraz większą przestrzeń. W ostatniej fazie otrzymamy **tzw. obwód otwarty.** Charakteryzować się on będzie w dalszym ciągu częstotliwością rezonansową, większą niż na początku (ze względu na zmniejszenie pojemności kondensatora). Przy tej częstotliwości rezonansowej wypromieniowana ilość energii, doprowadzonej ze źródła, będzie największa. Częstotliwość ta jest funkcją wymiarów fizycznych anteny oraz sposobu jej zasilania (rysunek 5.22).



Rys.5.21. *Przekształcenie zamkniętego obwodu rezonansowego w antenę nadawczą*



Rys.5.22. *Porównanie anten Radiostacji Centralnej PR:*
a) antena ćwierćfalowa (Raszyn);
b) półfalowa (Konstantynów k/Gąbina). Przy różnych wymiarach promieniują falę o tej samej długości - różnica wysokości jest związana ze sposobem zasilania.

Istnieje wiele typów anten. Najważniejszy podział obejmuje **anteny linearne i aperturowe.** Anteny linearne mają postać przewodu (bądź układu przewodów) o długości znacznie większej od wymiarów poprzecznych. Przykładem takiej anteny jest zarówno maszt Radiostacji Centralnej, jak i antena teleskopowa radiotelefonu. Do tej grupy zaliczamy także np. anteny **dipolowe** czy **prętowe.** W przypadku anten aperturowych wypromieniowanie fali następuje z powierzchni, która może mieć rozmaity kształt, np. paraboliczny w antenach parabolicznych. Istotnym parametrem określającym antenę jest charakterystyka promieniowania. W zależności od potrzeb antena może być przystosowana do emitowania fali elektromagnetycznej z jednakową mocą we wszystkich kierunkach (w określonej płaszczyźnie). W tym przypadku mówimy o charakterystyce dookólnej anteny. Charakterystykę taką mają niemal wszystkie anteny nadawcze radiofoniczne.

Niekiedy istnieje potrzeba wyemitowania energii w ściśle określonym kierunku. Służą do tego anteny kierunkowe. W przypadku anten linearnych uzyskanie dużej kierunkowości wymaga znacznej rozbudowy anteny. Mówimy wtedy raczej o zespole anten. Na charakterystykę kierunkową anteny ma ponadto wpływ jej usytuowanie względem powierzchni Ziemi.

Parametry anten:

1. Charakterystyka promieniowania i płaszczyzny charakterystyki,
2. Zysk energetyczny,
3. Kierunkowość,
4. Impedancja wejściowa,
5. Szerokość pasma pracy,
6. Polaryzacja anteny,
7. Długość skuteczna,
8. Apertura maksymalna i powierzchnia skuteczna,
9. Zastępcza temperatura szumowa.

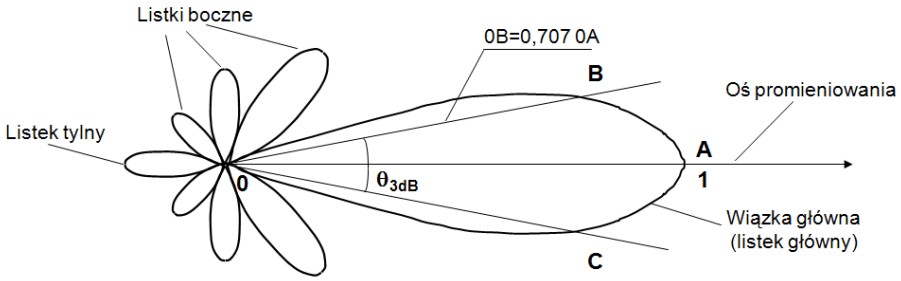
Szczegółowe omówienie parametrów anten wykracza poza niniejsze opracowanie. Najważniejszym parametrem jest charakterystyka promieniowania. Jest to parametr trójwymiarowy. Zwykle przedstawia się ją w dwóch płaszczyznach, najczęściej w układzie współrzędnych biegunowych. Aby była możliwość porównywania różnych anten, stosuje się unormowaną charakterystykę promieniowania, którą uzyskuje się po podzieleniu wyniku pomiaru przez maksymalną wartość natężenia pola elektrycznego bądź maksymalną wartość gęstości mocy.

Prezentowanie pełnej, przestrzennej charakterystyki jest dosyć kłopotliwe, dlatego najczęściej podaje się ją w dwóch charakterystycznych płaszczyznach przekroju. W praktyce stosuje się dwa typy tych płaszczyzn przekrojów, a mianowicie:

- płaszczyzny odniesione do układu współrzędnych kartezjańskich, czyli pośrednio do powierzchni ziemi. W tym przypadku rozróżnia się pionową i poziomą charakterystykę promieniowania. Niekiedy ch-ki te nazywane są: elewacyjna i azymutalna (horyzontalna)
- płaszczyzny odniesione do wektorów pola elektrycznego i magnetycznego. Płaszczyzny te nazywane są: płaszczyzna E i płaszczyzna H. Płaszczyzna E jest przekrojem, w którym jest zawarty wektor natężenia pola elektrycznego oraz wektor kierunku rozchodzenia się fali. Z kolei płaszczyzna H zawiera w sobie wektor natężenia pola magnetycznego i kierunek propagacji fali.

Odniesienie do x, y, z; czyli do powierzchni ziemi → zmiana położenia anteny.
Odniesienie do płaszczyzn E i H → bardziej uniwersalne, ale traci sens, gdy mamy do czynienia z polaryzacją kołową lub eliptyczną.

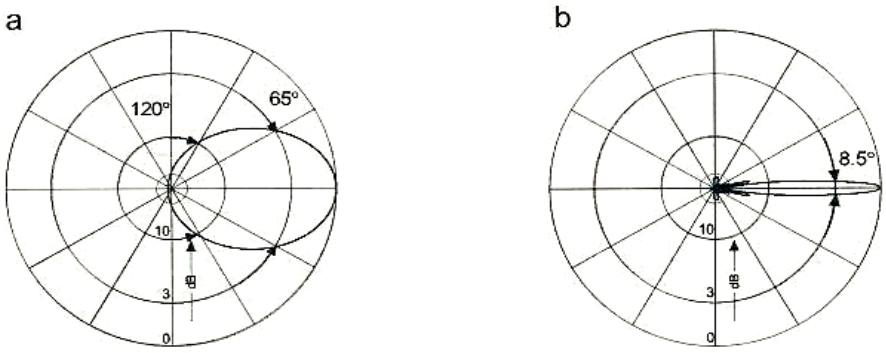
W charakterystyce promieniowania można wyróżnić: wiązkę główną, listki boczne, listek tylny (rysunki 5.23 ÷ 5.26)



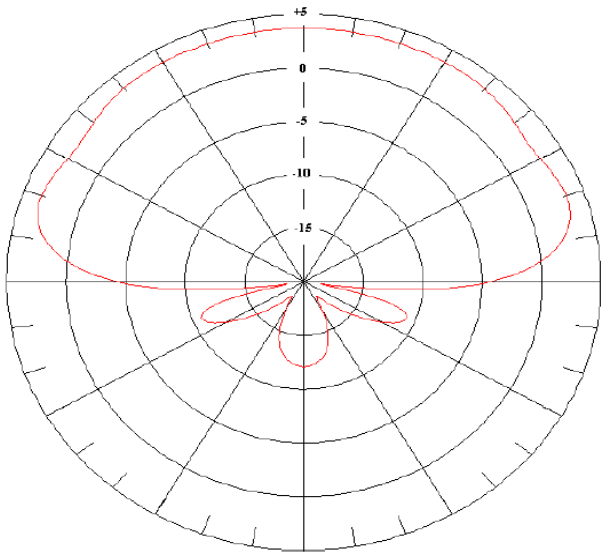
Rys.5.23. *Przykładowy wykres charakterystyki promieniowania w biegunowym układzie współrzędnych*

- wiązka główna, nazywana również listkiem głównym,
- oś promieniowania,
- szerokość wiązki głównej - mocowa spadek 3 dB, amplitudowa spadek 0,707,
- listki boczne określają wartości energii elektromagnetycznej propagującej w kierunkach innych niż zamierzone. Anteny są tak projektowane, aby poziom listków bocznych był niski,

- kierunki zerowe to takie, w których poziom promieniowania jest do zaniedbania,
- listek tylny to taki, którego kierunek jest przeciwny do kierunku wiązki głównej.

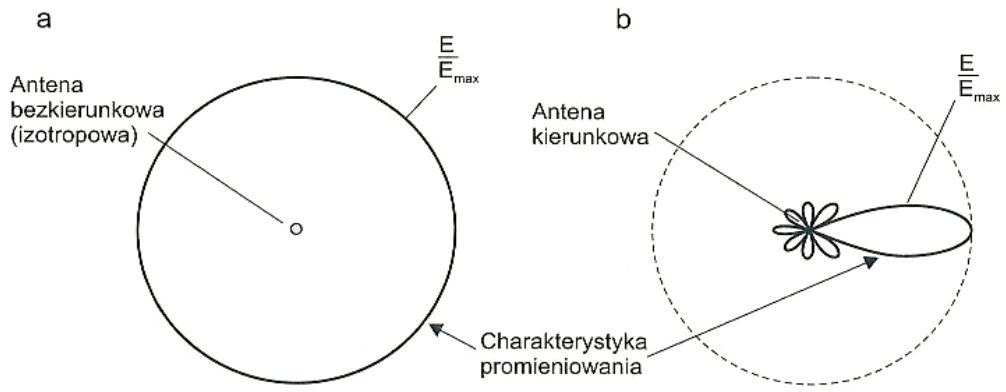


Rys.5.24. *Przykładowe charakterystyki promieniowania: a) pozioma b) pionowa*



Rys.5.25. *Typowa charakterystyka promieniowania we współrzędnych biegunowych*

W rzeczywistych antenach mamy do czynienia ze źródłami, które wysyłają więcej energii EM na określonych kierunkach kosztem pozostałych kierunków. Własność ta nazywana jest kierunkowością i określa możliwości anteny koncentrowania energii EM na wyróżnionym kierunku (rysunek 5.26).



Rys.5.26. *Charakterystyka promieniowania anteny: a) izotropowej b) kierunkowej*

Kierunkowość anteny oznacza się literą D i definiuje się następująco:

$$D = 4\pi \frac{\text{max. moc promieniowana w jedn. kat bryłowy}}{P_{pr}}$$

gdzie: P_{pr} – moc promieniowania z anteny

W technice antenowej jest również stosowany parametr nazywany zyskiem energetycznym, oznaczany literą G, który jest stosunkiem maksymalnej wartości gęstości mocy (na kierunku maksymalnego promieniowania do mocy doprowadzonej do wejścia anteny P_{we}.

$$G = 4\pi \frac{\text{max. moc promieniowana w jedn. kat bryłowy}}{P_{we}}$$

Gdzie P_{we} – moc doprowadzona do anteny

Zysk energetyczny jest również nazywany zyskiem anteny. Zysk ten określony powyższą zależnością obejmuje straty mocy w antenie i jej niedopasowanie impedancyjne do impedancji wolnej przestrzeni: zwykle wyrażany jest dB. Antena kierunkowa $G_{dB} = 10\log G$ wytwarza w miejscu odbioru, na kierunku maksymalnego promieniowania, takie samo pole jak antena izotropowa promieniująca moc G razy większą. A więc użycie anteny kierunkowej na kierunku maksymalnego promieniowania, jest równoznaczne z zastosowaniem anteny izotropowej zasilanej mocą G razy większą. Dla podkreślenia, że wartość zysku energetycznego w dB jest odnoszona do anteny izotropowej często zysk ten oznacza się jako dBi. W praktyce zysk energetyczny odnoszony jest do natężenia pola E lub gęstości mocy można wyrazić następująco:

$$G = 4\pi \frac{\text{max. moc promieniowana w jedn. kat bryłowy}}{P_{we}}$$

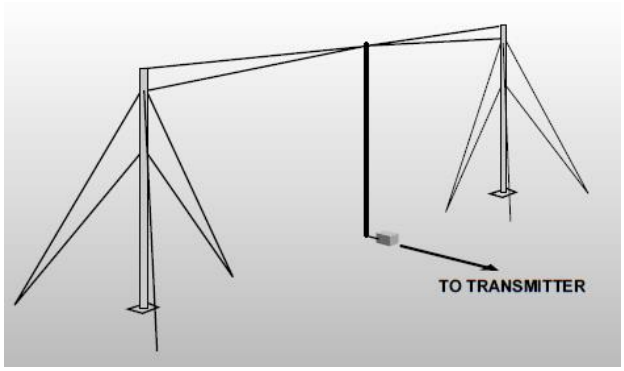
$$G_{dBi} = 20\log \frac{\text{max. gęstość mocy pochodzącej od badanej anteny}}{\text{gęstość mocy od izotropowej anteny zasilanej tą samą mocą}}$$

W zależności górnej zysk energetyczny odniesiony jest do natężenia pola elektrycznego, zaś w dolnej do gęstości mocy. Zysk energetyczny jest parametrem podobnym do kierunkowości anteny, a wielkością która różnicuje te parametry jest odniesienie do mocy przedstawionej w mianownikach powyższych wyrażeń. W kierunkowości przyjmowana jest moc promieniowana P_{pr}, a w zysku energetycznym występuje moc doprowadzona do anteny P_{we}. Zyski energetyczne przykładowych anten w zakresie mikrofalowym przedstawia tabela 5.1

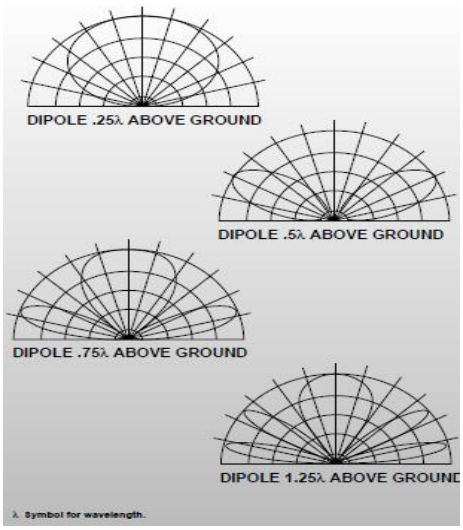
Tabela 5.1. *Zyski antenowe przykładowych anten*

Typ anteny	Długość/średnica anteny	Pasmo (zakres częstotliwości)	G_{dBi}	G [razy]
Antena sektorowa stacji bazowej K-730370	1,3 m	GSM (870 – 960 MHz)	14 dB	25
Antena sektorowa stacji bazowej K-730691	1,9 m	GSM (870 – 960 MHz)	17 dB	50
Antena sektorowa stacji bazowej K-742213	1,9 m	DCS (1710 – 1880 MHz)	19 dB	79
Antena sektorowa stacji bazowej K-742213	1,9 m	UMTS (1920 – 2170 MHz)	19,5 dB	89
Antena linii radiowej VHP2-220	0,6 m	23 GHz	41	12589
Antena linii radiowej VHP4-220	1,2 m	23 GHz	46,8	47853
Antena linii radiowej łączności satelitarnej	6 m	23 GHz	57	501187
Radar AVIA	12 m	Pasmo L (1300 – 1400 MHz)	32,9	1950
Radar wysokościomierz	10 m	Pasmo E (2600 – 3200 MHz)	40	10000

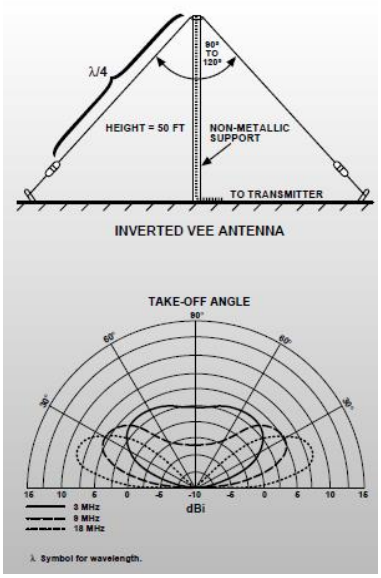
Przykłady częściej stosowanych anten i ich charakterystyki promieniowania przedstawiają rysunki 5.27 do 5.31.



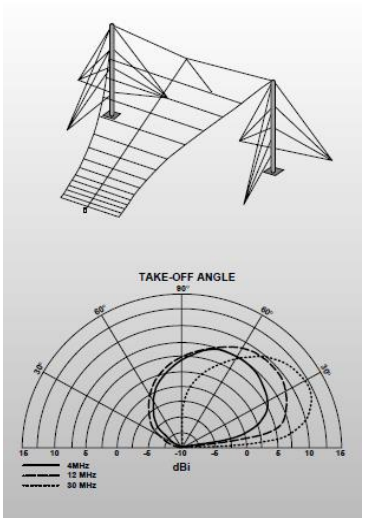
Rys.5.27. *Horyzontowa antena dipolowa*



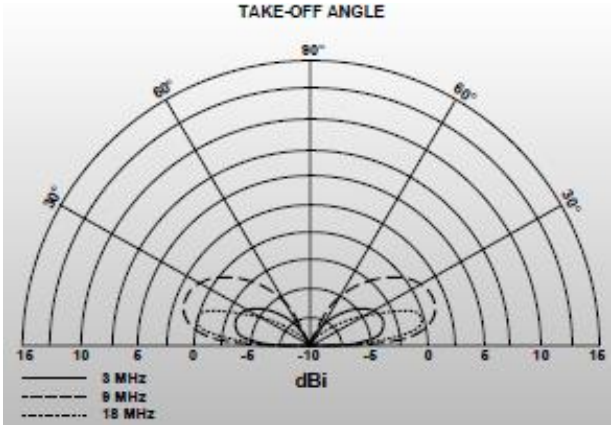
Rys.5.28. *Horyzontowa antena dipolowa. Charakterystyki promieniowania w funkcji długości fali*



Rys.5.29. *Antena odwrócone V*

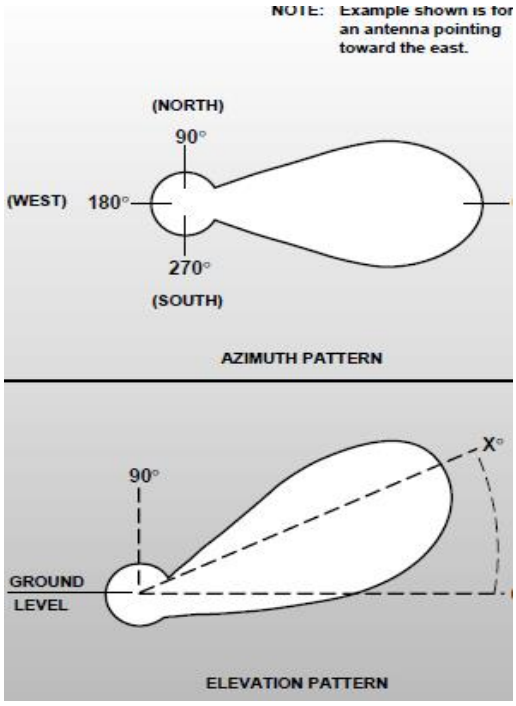


Rys.5.30. *Horyzontowa antena logarytmiczno – periodyczna*



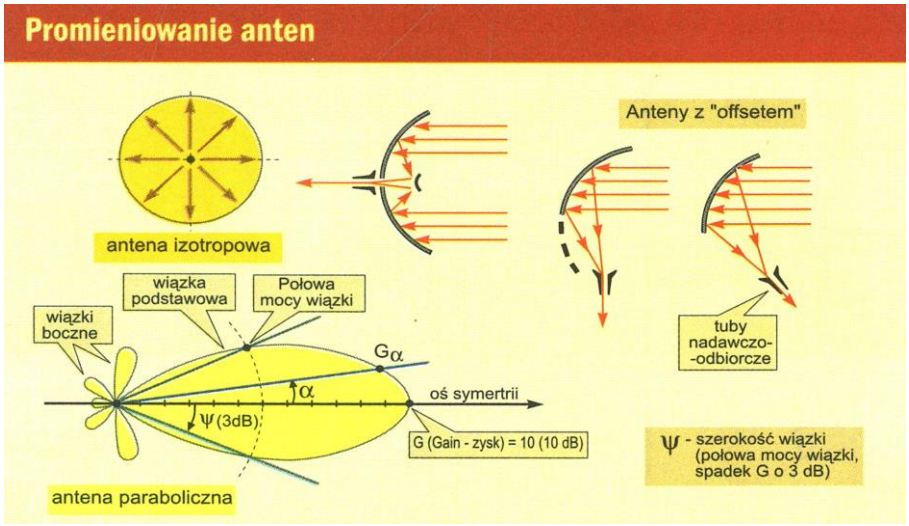
Rys.5.31. *Charakterystyka promieniowania pionowej anteny prętowej*

Aby wykorzystać właściwości kierunkowe anten należy określić dwie wielkości; azymut kierunku maksymalnego promieniowania, oraz kąt elewacji (kąt pomiędzy powierzchnią Ziemi, w miejscu instalowania anteny, a osią wiązki maksymalnego promieniowania).



Rys.5.32. *Pionowa i pozioma charakterystyka promieniowania anten kierunkowych*

Dobrym przykładem powszechnie stosowanych anten kierunkowych są anteny do odbioru telewizji satelitarnej (DVD–S). W tym przypadku tradycyjne anteny paraboliczne, dla naszej szerokości geograficznej nie są optymalnym rozwiązaniem. Czasza takiej anteny jest praktycznie równoległa do powierzchni Ziemi, więc w okresie zimowym gromadzić się w niej będzie śnieg i lód, co zaowocuje dużą liczbą „dropów" na ekranie telewizora. Aby tego uniknąć skonstruowano anteny „podświetlane" inaczej offsetowe. Czasza takiej anteny stanowi wycinek paraboloidy, tak dobrany, że promiennik (tuba) nadawczo – odbiorczy znajduje się poza środkiem geometrycznym anteny. Powoduje to, że dla naszej szerokości geograficznej (Polska), taka antena jest niemal prostopadła do powierzchni Ziemi co eliminuje niebezpieczeństwo zbierania się śniegu i zapewnia poprawny odbiór programów telewizyjnych w ciągu całego roku. Porównanie poziomej charakterystyki promieniowania anteny izotropowej i kierunkowej oraz zasadę pracy anten podświetlanych przedstawia rysunek 5.33.



Rys.5.33. *Charakterystyki promieniowania anten*

Ważnym problemem, niestety bardzo często niedocenianym, jest zabezpieczenie instalacji antenowych, właściwą ochroną odgromową i przeciwprzepięciową wywołaną wyładowaniami atmosferycznymi. Najczęstszym punktem trafień podczas wyładowań atmosferycznych doziemnych jest wierzchołek konstrukcji antenowej. Dotyczy to zarówno masztu, jak i samej anteny. Stalowe maszty kratownicowe są dobrze chronione z powodu swojej konstrukcji, ponieważ są dobrym elementem do odprowadzania prądu piorunowego. Uszkodzeniu ulegają zwykle anteny jeśli przepływający prąd będzie

wystarczająco duży. Dlatego należy antenę umieszczać w strefie osłonowej, która utworzona jest przez samą konstrukcję wsporczą. Konstrukcję osłonową mogą stanowić również odpowiednio rozmieszczone zwody umieszczone na konstrukcjach wsporczych ponad anteną.

Jeżeli maszty wykonane są z materiałów izolacyjnych, to kable koncentryczne mają cienkie powłoki i nie mogą służyć jako przewody odprowadzające udar piorunowy.

Uziom jest podstawową drogą rozładowania prądu piorunowego do ziemi. W celu ograniczenia do minimum wzrostu potencjału w całej instalacji jego impedancja powinna być wystarczająco mała. O wartości impedancji instalacji odgromowej decyduje przede wszystkim jej indukcyjność. Ważnym elementem przy projektowaniu uziomu jest dokładna znajomość rezystywności gruntu, ponieważ wchodzi ona do wszystkich zależności dotyczących wyznaczania rezystancji uziemienia.

Mimo nawet z pozoru doskonałej konstrukcji część energii i tak przedostanie się kablem koncentrycznym do urządzenia radiokomunikacyjnego. Jaka wartość tej energii przeniknie zależeć będzie od wartości prądu wyładowania i stopnia sprzężenia obwodu rozładowania prądu piorunowego z kablem koncentrycznym.

5.6. Systemy radiokomunikacji ruchomej

Systemy radiokomunikacji z obiektami ruchomymi (co najmniej jeden użytkownik - abonent połączenia porusza się, pozostaje w ruchu). Jednym ze sposobów podziału radiokomunikacji ruchomej (ruchowej) jest stopień ich komplikacji i możliwości realizacyjne usług. Wg. tej klasyfikacji możemy je podzielić na:

- Systemy przywoławcze (*paging*),
- Systemy telefonii bezprzewodowej (telefonia bezsznurowa),
- Systemy trankingowe,
- Systemy telefonii komórkowej,
- Systemy telefonii satelitarnej.

W ostatnim czasie jako kolejny rodzaj radiokomunikacji ruchomej zaliczamy systemy dostępu bezprzewodowego oraz bezprzewodowe sieci komputerowe. Pokrótce omówimy każdy z nich.

5.6.1. Systemy przywoławcze

Systemy przywoławcze (*paging*) - jednokierunkowy rozsiewczy system radiokomunikacyjny do przesyłania alarmu, krótkich wiadomości numerycznych lub alfanumerycznych.

Cechy:

- korzystanie z pasma UKF lub wąskiego pasma w zakresie kilkuset MHz,
- małe rozmiary stacji ruchomych (odbiorników),
- brak potwierdzenia dotarcia informacji do odbiorcy (w nowych rozwiązaniach jest).

Przesłanie wiadomości przez słowny kontakt z operatorem w centralnym biurze zleceń, który następnie nadaje wiadomość cyfrową do stacji ruchomej. Możliwe jest również przekazywanie automatyczne za pomocą transmisji pod określony numer informacji cyfrowej wygenerowanej za pomocą PC - ta wyposażonego w modem lub teleksem.

Klasyfikacja sieci przywoławczych

- ***Sieci zakładowe (prywatne) (ETSI 300 224)*** - zainstalowane na terenie określonej instytucji lub ściśle wyznaczonego obszaru (duży budynek, obiekt terenowy, magazyny) i mają charakter prywatny.
- ***Sieci publiczne*** – w odróżnieniu od sieci zakładowych są wykorzystywane przez abonentów publicznych i dalej dzielą się na następujące kategorie:
    - sieci miejskie (pojedynczy kanał radiowy w paśmie 160 MHz – sygnał cyfrowy o przepływności 512 bit/s),
    - sieci ogólnokrajowe – o zasięgu obejmującym kraj (taką siecią była sieć POLPAGER).

Aby zapewnić efektywne wykorzystanie pasma niezakłócania odbioru innym użytkownikom zdefiniowano **Wymagania Techniczno – Eksploatacyjne (WTE)** zawierający zbiór parametrów, które muszą spełniać systemy przywoławcze, aby mogły być dopuszczone do eksploatacji.

WTE sieci zakładowych:

- ✓ Zakres częstotliwości,
- ✓ Moce nadajników przywoławczych,
- ✓ Wybrane parametry emisji (np. dopuszczalne zakłócenia w sąsiednim kanale),

- ✓ Odstęp międzykanałowy,
- ✓ Niestabilność częstotliwości nadajnika,
- ✓ Poziom promieniowania na zaciskach antenowych,
- ✓ Parametry eksploatacyjne w warunkach skrajnej temperatury i skrajnych wartości napięć zasilających.

Metody transmisji i zabezpieczenia informacji (formatowanie danych w bloki, detekcja i korekcja błędów oraz rodzaj stosowanych modulacji) pozostają nieznormalizowane i zależą od producenta sprzętu. Najczęściej (sieci zakładowe) wykorzystują sprzęt jednego producenta. W komplecie pagery, stacja bazowa i centrala przywoławcza. Konieczna jednak ich homologacja.

Sieci miejskie

Sieć działa na pojedynczej częstotliwości nośnej, tej samej na całym pokrywanym terytorium. Stacje bazowe pracują synchronicznie z dużą dokładnością, gdyż pager może odbierać sygnał z kilku stacji bazowych równocześnie. Brak synchronizacji spowodowałby kłopoty z detekcją sygnału. Aby utrzymać synchronizację konieczne jest kontrolowanie i utrzymanie w pewnych granicach tolerancji wartości opóźnienia przesyłania liniami transmisyjnymi sygnałów do poszczególnych stacji bazowych. Uważa się, że sygnały docierające do pagera z dwóch stacji bazowych mogą się różnic w czasie o odstęp nie większy niż ¼ czasu trwania jednego bitu. Z przyjętej szybkości transmisji oraz czasu propagacji wynika, że stacje bazowe trzeba rozmieszczać w odległości około 8 km, a ich anteny w celu uniknięcia zbyt dużego wzajemnego pokrycia obszarów zasięgu, powinny być zawieszone na wysokości do 100 metrów.

W Polsce sieci miejskie stosują pojedynczą w paśmie 160 MHz, która służy do przekazywania sygnału cyfrowego z szybkością 512 bitów/sek.

Wszystkie stacje stosują protokół POCSAG *(Post Office Code Standards Advisory Group*) opisany zaleceniu CCIR (ITU –R) nr 584 znanego pod nazwą kodu przywoławczego CCIR Nr.1.

Opracowano również WTE na sieć ogólnokrajową POLPAGER stosującą inny protokół formatowania danych oznaczony MBS *(Mobile Search)*. Wykorzystuje (a właściwie wykorzystywał) istniejące nadajniki radiowe UKF pracujące w paśmie 66 ÷ 74 MHz. Wykorzystano 31 nadajników TP S.A., oraz 45 nadajników prywatnych uzupełniających pokrycia nadajników TP S.A. W sieci Polpeger wykorzystywano (po zaprzestaniu nadawania na „dolnym UKF – fie" sieć nie działa).

Elementy sieci POLPAGER

- ✓ Radiowa centrala przywoławcza (RCP),
- ✓ koncentratory terenowe,
- ✓ centralne i terenowe biura zleceń służby przywoławczej,
- ✓ sieć dystrybucji sygnałów przywoławczych z centrali przywoławczej do stacji bazowych,
- ✓ sieć nadajników z urządzeniami zwielokrotnienia,
- ✓ system monitorowania nadajników,
- ✓ analizator ruchu centrali przywoławczej,
- ✓ zbiór pagerów.

Przy zasięgu krajowym stosuje się jeszcze inne protokoły:

- ▪ APOC (*Advanced Paging Operators Code*) - opracowany przez Philips i popierany przez Ericssona.
- ▪ FLEX – opracowany przez Motorolę i wdrażany w USA, w wersji ReFLEX pozwala na dwustronną transmisję (pager odpowiada na przesłane komunikaty sygnałem potwierdzenia).

Protokół POCSAG stosują działające w kraju Firmy: Metro Bip, Telepage, Easy Call i Elite. Stosowane zabezpieczenia kodowe przed błędami to kod BCH nazwany tak od nazwisk jego wynalazców Bose-Chauhuri-Hocqunenghen (31,21) o wielomianie generującym; $g(x) = x^{10} \oplus x^9 \oplus x^8 \oplus x^6 \oplus x^5 \oplus x^3 \oplus 1$

W sieci POLAGER – stosowano cykliczny kod blokowy Kasamiego (26,16) o wielomianie generującym; $g(x) = x^{10} \oplus x^8 \oplus x^7 \oplus x^5 \oplus x^4 \oplus x^3 \oplus 1$

który zapewnia zdolność korekcji paczek błędów o długości równej 5. Oznaczenie (n,k) określa jaka jest długość ciągu kodowego - n, oraz ilość pozycji informacyjnych - k.

Europejski System Przywoławczy ERMES (*European Radio Messaging System*); Unia Europejska i ETSI a roku 1994 ITU – rekomendowała jako pierwszy światowy standard systemu przywoławczego o możliwości międzynarodowego działania.

Cechy systemu:

- ✓ możliwość korzystania z systemu poza własnym krajem,
- ✓ duża pojemność informacyjna i powiększenie liczby użytkowników w porównaniu z dotychczasowymi systemami,

- ✓ zwiększenie szybkości transmisji w porównaniu z protokołem POCSAG,
- ✓ standaryzacja odbiorników przejawiająca się możliwością korzystania z nich w sieciach różnych operatorów.

ERMES realizuje:

- przesyłanie wywołania akustycznego — możliwych jest 8 różnych tonów powiadamiania,
- przesyłanie komunikatów numerycznych — o maksymalnej długości 16 000 znaków,
- przesyłanie komunikatów alfanumerycznych — o maksymalnej długości 9 000 znaków.

Dodatkowo:

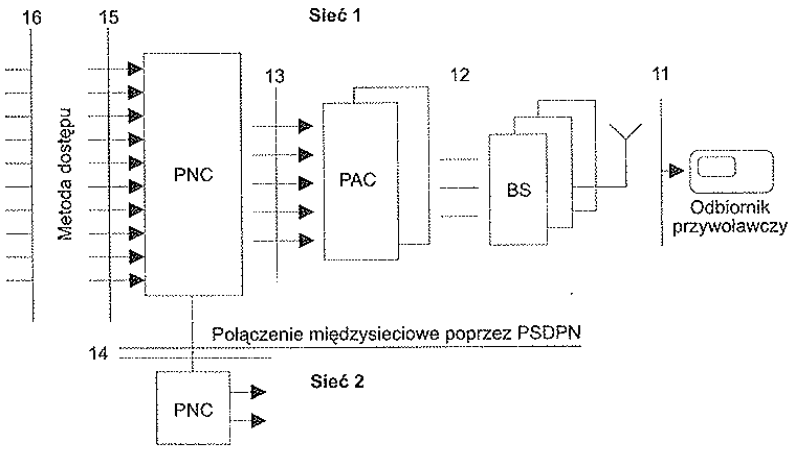
▪ Przesyłanie danych w kanale przezroczystym, blok nie może przekraczać 64 kbit. ***Przezroczystość*** kanału oznacza, że dane transmitowane są w postaci takiej, jak podane są na wejściu nadajnika. Z taką samą szybkością wysyłane są z wyjścia odbiornika a ich jakość zależy natomiast od aktualnych własności transmisyjnych kanału.

▪ Transmisja w kanale nieprzezroczystym polega na zastosowaniu procedur zabezpieczenia informacji np. metoda ARQ *(Automatic Request to Repeat)* czyli zastosowanie kodów blokowych z detekcją błędów, dzięki którym dane odebrane charakteryzują się stałą jakością, lecz nierównomiernym strumieniem w wyniku zdarzających się powtórzeń bloków danych, na które jest podzielony strumień danych.

System stosuje 4 typy odbiorników: tonowe, alfanumeryczne, z przezroczystym kanałem danych.

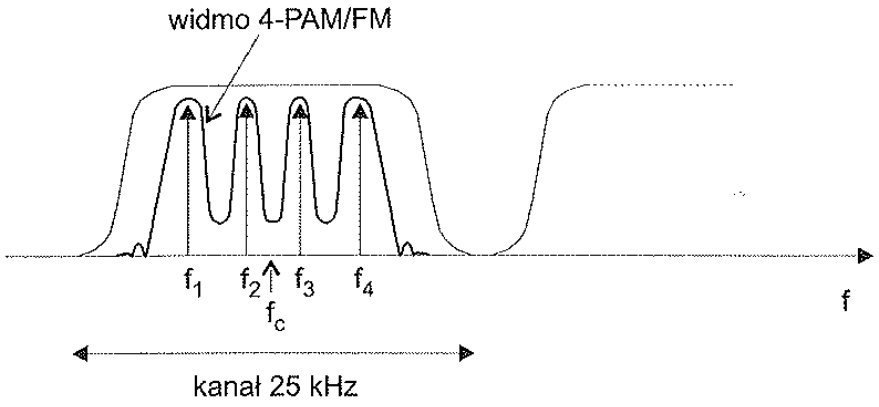
Oferowane usługi dodatkowe:

- ✓ Potwierdzenie odbioru komunikatu,
- ✓ Wywołanie grup abonentów,
- ✓ Usługi ograniczania zakresu wywołań,
- ✓ Usługi dotyczące ochrony komunikatu i skierowania go w odpowiedni obszar przeznaczenia,
- ✓ Wywołanie z trójpoziomowym priorytetem,
- ✓ Inne.



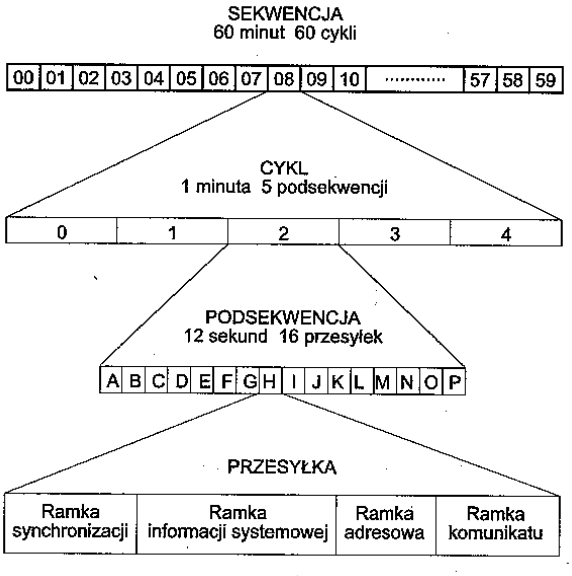
Rys.5.34. *Architektura sieci przywoławczej ERMES*

W systemie ERMES zastosowano modulację 4-PAN/FM (4-FSK), oznacza to, że dane binarne łączone są w bloki dwubitowe, które wyznaczają jeden z czterech możliwych impulsów PAM stanowiących równocześnie sygnał modulujący dla modulatora FM(lub też jedną z czterech częstotliwości znamiennych modulatora 4-FSK). System działa przy co najwyżej 16 kanałach częstotliwościowych rozmieszczonych z odstępem 25 kHz w paśmie od 169,4125 do 169,8125 MHz. Tak więc możliwe jest zwielokrotnienie częstotliwościowe, a na pojedyńczej nośnej - zwielokrotnienie czasowe. Na rysunku 5.35 przedstawiono przykładowe rozmieszczenie widma sygnału z modulacją 4-PAM/FM na osi częstotliwości w ramach kanału częstotliwościowego. Częstotliwość nośna znajduje się w środku 25-kilohercowego kanału. Symbolami $f_1,...,f_4$ zaznaczono częstotliwości znamienne odpowiadające poszczególnym kombinacjom binarnych dwubitowych bloków.



Rys.5.35. *Rozmieszczenie widma sygnału 4-PAM/FM na osi częstotliwości*

Na rysunku 5.36 przedstawiono schemat organizacji protokołu radiowego. Strumień danych organizowany jest w postaci jednogodzinnych sekwencji. Nadawanie ich odbywa się w synchronizmie z czasem uniwersalnym UTC *(Uniwersal Time Coordinated.)* Sekwencja składa się z kolei z 60 jednominutowych cykli, a każdy cykl dzieli się na pięć podsekwencji. Z podziału czasowego wynika, że podsekwencja trwa 12 sekund. Podsekwencje z kolei składają się z przesyłek *(batches)* skierowanych do konkretnych odbiorników lub ich grup. W każdej podsekwencji jest 16 przesyłek oznaczonych literami od A do P. Przesyłka stanowi całość niezbędną do prawidłowego odbioru komunikatu przeznaczonego dla abonenta . W jej skład wchodzą: ramka synchronizacji, ramka informacji systemowej, ramka adresowa i właściwy komunikat. Przepływność binarna w kanale wynosi 6,25 kbit/s.

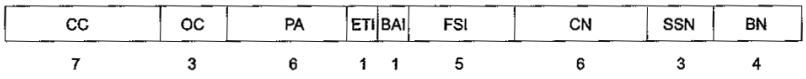


Rys.5.36. *Hierarchia czasowa systemu ERMES*

Ramkę informacji systemowej przedstawia rysunek 5.37. Poszczególne jego pola oznaczone skrótami mają następujące znaczenie:

- CC – *Country Code* – kod kraju sieci nadawczej,
- OC – *Operator's Code* – kod operatora sieci,
- PA – *Paging Area* – kod pola wywoławczego,
- CN – *Cycle Number* – numer cyklu,
- SSN – *Subsequence Number* – numer podsekwencji,
- BN – *Batch Number* – numer przesyłki,
- ETI – *External Traffic Indicator* – wskaźnik ruchu zewnętrznego,
- BAI – *Border Area Indicator* – wskaźnik pola granicznego,

• FSI – *Frequnezy Subset Indicator* – wskaźnik pola granicznego.



Rys.5.37. *Struktura ramki informacji systemowej w systemie ERMES*

Każdy kanał systemu ERMES oferuje pojemność około pięciokrotnie większą niż kanał tradycyjnego systemu przywoławczego. Przy transmisji 6,25 kb/s każdy kanał może obsłużyć do 500 000 abonentów w przypadku wiadomości numerycznych dziesięciocyfrowych oraz 160 000 abonentów w przypadku transmisji alfanumerycznej o długości 40 znaków. Dane te są wyznaczone przy założeniu średnio 0,2 wywołań na godzinę. Olbrzymie możliwości adresowania w systemie ERMES powodują, że pojedynczy abonent może uzyskiwać wiadomości od różnych sieci informacyjnych, dotyczące np. wiadomości specjalnych, informacji o ruchu ulicznym, prognoz pogody, kursów akcji, notowań kursów walut czy wyników zawodów sportowych.

5.6.2. Systemy telefonii bezprzewodowej

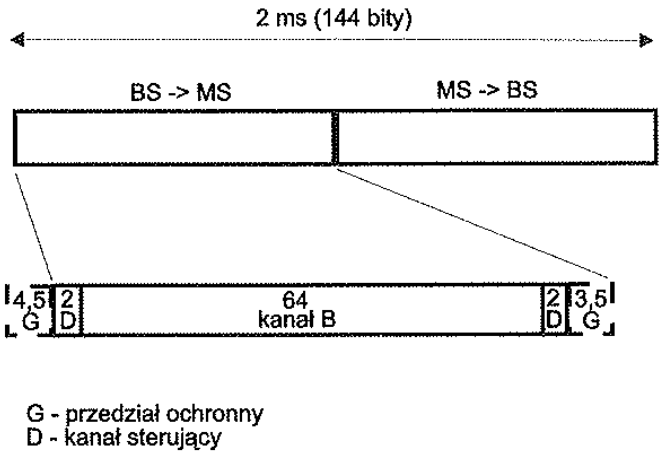
Systemy telefonii bezprzewodowej pojawiły się w końcu lat siedemdziesiątych. Mogą być one scharakteryzowane jako środek łączności bezprzewodowej o niewielkiej mocy dla użytkownika poruszającego się powoli w bardzo ograniczonym zakresie wokół stacji bazowej. Celem telefonu bezprzewodowego miało być w większości zastąpienie przewodowego, zatem jakość połączenia oraz cena aparatu z założenia znacznie nie powinna odbiegać od tradycyjnego telefonu. Stacja bazowa to część systemu telefonii bezprzewodowej dołączona do publicznej sieci telefonicznej i widziana prze nią jako| zwykły telefon. W olbrzymiej większości przypadków stacja bazowa współpracuje jedynie z jedną stacją ruchomą, której czas pomiędzy kolejnymi ładowaniami baterii powinien być maksymalny. W rezultacie tak przyjętych warunków, systemy telefonii bezprzewodowej cechują się małą liczbą użytkowników przypadającą na jednostkę przydzielonego dla tego typu systemów pasma, niewielką liczbą użytkowników ruchomych na każdą stację bazową (najczęściej jednym), możliwą dużą liczbą stacji bazowych na jednostkę powierzchni oraz krótkim zasięgiem stacji bazowej. Niniejsze cechy dotyczą tradycyjnej telefonii bezprzewodowej zrealizowanej w technice analogowej. Chcąc uniknąć kolizji polegających na połączeniu się stacji ruchomej z obcą stacją bazową i realizacji połączenia na nie swój rachunek, stosuje się różnorakie zabezpieczenia techniczne polegające na wymianie „hasła” - kodu cyfrowego pomiędzy

stacją ruchomą i bazową, czy też poszukiwaniu wolnego kanału spośród tych, które są dostępne dla pary stacja bazowa – stacja ruchoma. Wprowadzenie techniki cyfrowej w dziedzinie telefonii bezprzewodowej spowodowało poważne wzbogacenie możliwości takich systemów. Przede wszystkim doszło do rozszerzenia ich działania poza lokalny zasięg bezpośrednio w miejscu pracy użytkownika lub w miejscu jego zamieszkania. Wprowadzony przede wszystkim w Wielkiej Brytanii system drugiej generacji, znany pod nazwą CT-2 *(Cordless Telephony-2*), oferuje dodatkową usługę zwaną *telepoint.* Stacje bazowe systemu CT-2 rozmieszczone są w centrach dużych skupisk ludzkich. Użytkownik z zarejestrowaną usługą „telepoint" jest w stanie inicjować połączenie z telefonu bezprzewodowego systemu CT-2. Nie może być jednak przez stację bazową znaleziony. Dzwonić do niego może jedynie jego własna stacja bazowa, jeśli w jej zasięgu się znajduje. Nie jest również możliwe przejmowanie rozmowy zainicjowanej połączeniem się z określoną stacją bazową przez inną stację bazową. System CT-2 oferowany początkowo w Wielkiej Brytanii nie przyjął się tam. Odniósł jednak sukces w dwóch centrach azjatyckich: Hongkongu i Singapurze. Był również stosowany w Paryżu. Niektóre z aparatów CT-2 wyposażono dodatkowo w standardowe pagery, dając tym samym możliwość przekazania informacji od użytkownika zewnętrznego o pożądanym kontakcie z użytkownikiem sytemu CT-2.

Prace unifikacyjne prowadzone w ramach Unii Europejskiej doprowadziły do ustanowienia europejskiego standardu cyfrowej telefonii bezprzewodowej *(Digital European Cordless Telephony).* System ten został zoptymalizowany na zastosowanie wewnątrz budynków. Stacje bazowe systemu DECT poprzez kontroler do wewnętrznych (zakładowych) central telefonicznych. Kontrolery - układy sterowania są w stanie sterować przejmowaniem połączeń przez kolejne stacje bazowe wraz ze zmianą miejsca położenia użytkownika ruchomego. Możliwe jest również wywoływanie pożądanego użytkownika znajdującego się w zasięgu stacji bazowej. Cyfrowa telefonia bezprzewodowa znajduje zastosowanie nie tylko wewnątrz obiektów. Systemy takie instaluje się również w miejscach dużej potencjalnej koncentracji ruchu telekomunikacyjnego, takich jak porty lotnicze, centra miast, dworce itp. Technologia cyfrowej telefonii bezprzewodowej jest po pewnych modyfikacjach wykorzystywana w realizacji bezprzewodowych pętli abonenckich. Oprócz standardu CT-2 istnieje również kolejny standard cyfrowej telefonii bezprzewodowej znany pod skrótem CT-3. Został on wprowadzony w Szwecji przez firmą Ericsson i nie ma wielu wad

systemu CT-2. Nie ma on jednak zbyt wielkiego znaczenia praktycznego z powodu wprowadzenia standardu europejskiego DECT. W tabeli 5.2 przedstawiono niektóre parametry techniczne analogowych oraz cyfrowych systemów telefonii bezprzewodowej kolejnych generacji.

W standardzie CT-2 stosuje się pasmo 4 MHz w przedziale 864 ÷ 868 do realizacji 40 kanałów z częstotliwościami nośnymi rozmieszczonymi co 100 kHz. Każda nośna jest przypisana na czas połączenia pojedynczej parze abonentów. Ich strumienie binarne transmituje się w systemie dupleksowym z podziałem czasu (patrz punkt 2.4). Szybkość strumienia binarnego wynosi 72 kb/s. Struktura ramkowa standardu CT-2 jest pokazana na rysunku 5.38.



Rys.5.38. *Struktura ramki i szczeliny systemu CT-2*

Tabela 5.2. Podstawowe parametry techniczne analogowych i cyfrowych systemów telefonii bezprzewodowej

System	CT1 plus	CT2/CAI	CT2 plus	CT3	DECT
Szerokość pasma [MHz]	2	4	4/8	4/8	20
Pasmo [MHz]	885 ÷ 887 (1) 930 ÷ 932 (2)	864 ÷ 868	800 ÷ 1000	800 ÷ 1000	1880 ÷ 1900
Szerokość kanału [kHz]	25	100	100	1000	1728
Metoda wielodostępu	FDMA	FDMA	FDMA	FDMA/ /TDMA	FDMA/ /TDMA
Metoda dupleksu	FDD (45 MHz)	TDD	TDD	TDD	TDD
Liczba nośnych	80	40	40/80	4/8	10
Ilość kanałów/nośną	1	1	1	8	12
Liczba kanałów	80	40	38/76 (3)	32/64	132
Rodzaj modulacji	analog. FM	BFSK + filtr gauss. 72 kbit/s	BFSK + filtr gauss. 72 kbit/s	BFSK + filtr gauss. 640 kbit/s	GMSK 1152 kbit/s
Przenoszenie rozmów	nie	nie	tak	tak	tak
Wywoływanie dwustronne	nie	nie	tak	tak	tak
Szybkość cyfrowego strumienia mowy [kbit/s]	mod. FM analogowa	32	32	32	32
Promień komórki [m]	50 ÷ 300	30 ÷ 100	30 ÷ 200	30 ÷ 100	30 ÷ 200
Moc nadawana (śr./maks.)	10 m W/ 10 m W	5 m W/ 10 m W	5 m W/ 10 m W	5 m W/ 80 m W	10 m W/ 250 m W

(1) kierunek transmisji „w górę"
(2) kierunek transmisji „w dół"
(3) 2 lub 4 nośne zarezerwowane dla kanałów sygnalizacyjnych

Ramka składająca się z bloku transmitującego strumień binarny w kierunku od stacji bazowej do ruchomej oraz z bloku transmitującego w kierunku przeciwnym, trwa 2 ms. Każdy blok (szczelina) przekazuje 64 bity informacji abonenta oraz 4 bity informacji sterujących (w dwóch porcjach po 2 bity). Poszczególne bloki rozdzielone są przedziałami ochronnymi trwającymi odpowiednio 3,5 i 4,5 bita. Sumując 136 bitów bloków transmitowanych oraz łącznie czas trwania 8 bitów jako czasy ochronne otrzymujemy podział 2 – milisekundowej ramki na 144 bity, co odpowiada szybkości nadawania 72 kb/s. Strumień danych moduluje sygnał nośny zgodnie z modulacją BFSK *(Binary Frequency Shift Keying)*, co przy odstępie kolejnych nośnych 100 kHz daje efektywność wykorzystania pasma równą 0,72 bit/s/Hz. Binarny sygnał mowy jest uzyskany za pomocą kodera ADPCM zgodnego z zaleceniem ITU-T G.721 (patrz punkt 2.4). Jakość sygnału mowy jest porównywalna z jakością doświadczalną w przewodowej transmisji telefonicznej, gdzie stosuje się kodowanie (modulację) PCM. Obecnie, praktycznie stosowane są systemy CT-2 oraz DECT. W kraju jest dużo telefonów bezprzewodowych telefonów z tzw. „importu prywatnego" pracujących w paśmie 52 ÷76 MHz, mających tylko jeden kanał radiowy (taki sam dla wszystkich

użytkowników). Używanie takich telefonów prowadzi do konfliktów z prawem, stosowanie niezgodnego z Krajową Tablicą Przeznaczeń Częstotliwości, zakresu częstotliwości i może prowadzić do nadużyć (płacenie za rozmowy „sąsiada").

System DECT, podobnie jak GSM jest rezultatem wspólnego działania standaryzacyjnego w Unii Europejskiej w ramach ETSI. Opisany jest w zbiorze standardów składają z dziesięciu następujących części, zwanych *Common Interface* (wspólnym interfejsem - stykiem) zawierających:

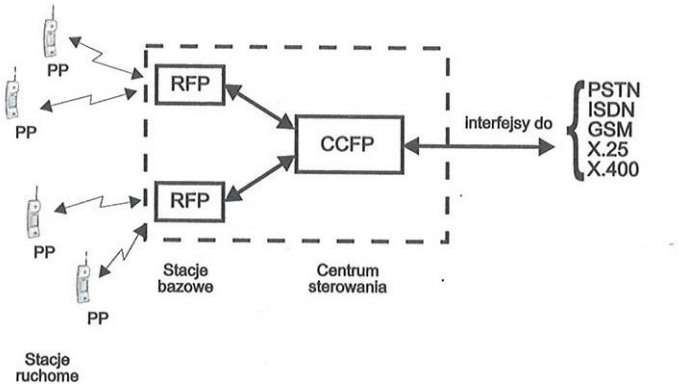
1. Przegląd systemu,
2. Warstwę fizyczną (PHL — *Physical Layer*),
3. Warstwę sterowania dostępem do medium transmisyjnego (MAC, *Medium ss Control Layer),*
4. Warstwę sterowania łączem danych (DLC — *Data Link Control*),
5. Warstwę sieciową (NWK — *Net Work Layer),*
6. Opis identyfikacji i adresowania,
7. Cechy związane z bezpieczeństwem,
8. Kodowanie mowy i transmisję,
9. Profil dostępu publicznego,
10. Algorytm kryptograficzny.

System DECT jest rozumiany jako system realizujący metodą radiową dostęp do sieci stałych na obszarach o dużym natężeniu ruchu telekomunikacyjnego. Składa się zbioru małych i niedrogich radiowych terminali ręcznych nawiązujących łączność ze stacjami bazowymi na bliskie odległości (jak widać z tablicy 5.2 na odległość do 200 m).

Standard DECT przewidziano do działania w następujących zastosowaniach

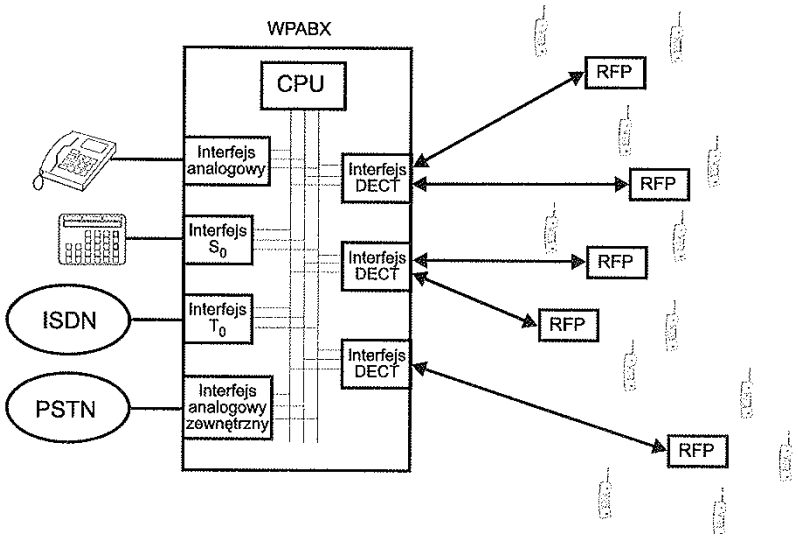
- jako domowy telefon bezprzewodowy,
- w niewielkich sieciach telefonicznych w firmach,
- w pełnych bezprzewodowych sieciach firmowych z centralą abonencką,
- w usługach typu Telepoint,
- w realizacji pełnego bezprzewodowego dostępu do sieci lokalnych (LAN),
- uzupełnianiu dostępu do systemów komórkowych,
- realizacji bezprzewodowej pętli abonenckiej.

Struktura systemu DECT opiera się na konstrukcji mikrokomórek o promieniu kilkuset metrów, w której komunikują się części ruchome (PP – *Portable Parts)* z częściami stałymi (FP — *Fixed Parts)* systemu. System toleruje szybkość poruszania się stacji ruchomej PP do wartości 20 km/h. Na rysunku 5.39 przedstawiono podstawową architekturę systemu DECT wraz z jej elementami.



Rys.5.39. *Podstawowa architektura systemu DECT*

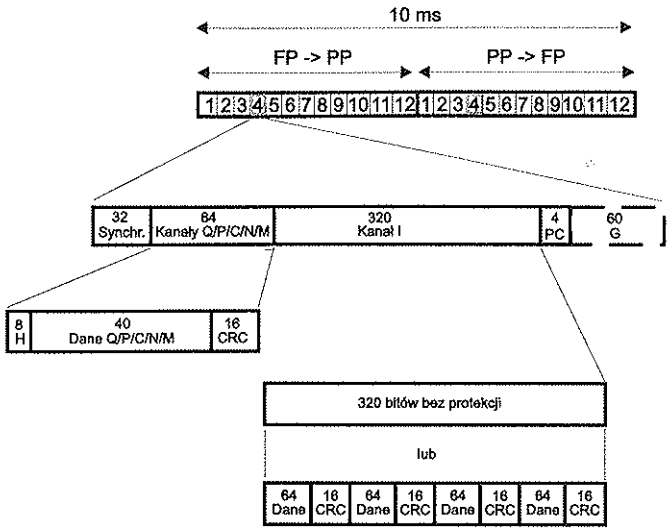
Wspomniane już stacje ruchome, oznaczane w systemie DECT skrótem PP łączą się drogą radiową ze stacją bazową nazywaną w opisie systemu DECT radiową częścią stałą systemu (RFP — *Radio Fixed Part).* Jedna lub więcej części RFP połączone są z centrum sterowania (CCFP — *Central Control Fixed Part),* które z kolei jest dołączone do stałej publicznej sieci telefonicznej, sieci ISDN lub GSM. Zespół stacji RFP oraz CCFP tworzy razem część stałą systemu FP. W mniejszych zastosowaniach centrum sterowania może nie występować a sieć DECT nie musi być dołączona do sieci zewnętrznej.



Rys.5.40. *Typowa konfiguracja systemu z bezprzewodową centralą abonencką*

Na rysunku 5.40 przedstawiono jedno z możliwych rozwiązań zakładowego systemu telekomunikacyjnego składającego się z radiokomunikacyjnej centrali abonenckiej (WABX — *Wireless Private Branch Exchange),* w której skład wchodzi oprócz jednostki centralnej szereg interfejsów z innymi sieciami lub urządzeniami, wśród których występują interfejsy systemu DECT. Każdy z nich steruje zespołem stacji bazowych, z którymi łączą się stacje ruchome.

Podstawowe dane techniczne systemu DECT zawarte są w tablicy 5.2 nie będą tutaj powtarzane. Zwróćmy jedynie uwagę na tryb TDMA wraz z pracą dupleksową z podziałem czasu. W ciągu 10-milisekundowej ramki zawartych jest 12 kanałów dupleksowych (w 24 szczelinach czasowych), co wobec przyjętej struktury czasowej pakietu w pojedynczym kanale daje dużą szybkość transmisji wynoszącą 1152 kb/s. Strumień danych dla pojedynczego kanału transmisyjnego realizowanego w konkretnej szczelinie czasowej na odpowiedniej częstotliwości nośnej jest oczywiście dużo wolniejszy i wynosi 32 kbit/s w kanale rozmównym (w tzw. polu B) oraz 6,4 kbit/s w D (sterowanie i sygnalizacja - tzw. pole A). Na rysunku 5.41 przedstawiono strukturę pojedynczego pakietu systemu DECT.



Rys.5.41. *Struktura pakietu w systemie DECT: (H – (Header) – nagłówek, PC – (Parity Check) – bity parzystości, CRC – (Cyclic Redundancy Check) – bity nadmiarowe kodowego zabezpieczenia przed błędami, G – (Guard Time) – czas ochronny*

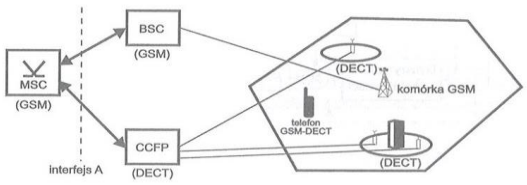
Pakiet mieści się w szczelinie o czasie trwania 0,417 ms co odpowiada czasowi trwania 480 bitów. Fizyczny pakiet trwa 420 bitów, natomiast resztę czasu trwania

szczeliny zajmuje przedział ochronny (60 bitów) służący do wyrównywania niedokładności fazowania pakietów w ramach szczeliny czasowej oraz realizacji procesów włączania i wyłączania stopnia mocy stacji ruchomej na początku i końcu pakietu. 420-bitowy pakiet rozpoczyna 16-bitowa preambuła (bity początkowe) a następnie nadawany jest 16-bitowy ciąg synchronizacyjny. Kolejne 388 bitów jest podzielonych na 64-bitowe pole sterujące i sygnalizacyjne (pole A) oraz na 320 bitów informacyjnych niosących strumień danych użytkownika (pole B). Pakiet kończą 4 bity kontroli parzystości całego pakietu. 64-bitowe pole sterujące, ze względu na ważność niesionej informacji systemowej ma strukturę składającą się z 8-bitowego nagłówka 40-bitowego bloku danych sterujących oraz 16-bitowego bloku kontroli parzystości (CRC). Blok ten wynika z zastosowania kodu korekcyjnego BCH (63,48), co oznacza, że długość ciągu kodowego n wynosi 63 bity a ilość pozycji informacyjnych wynosi 48 bitów, poprawiającego 2 błędy uzupełnionego o bit kontroli parzystości całego słowa kodowego. Blok danych sterujących, w zależności od aktualnie realizowanego połączenia tworzy sterujący kanał wywoławczy (*Paging Channel*) - kanał P, kanał sterujący (*Control Channel)* - kanał C - przesyłający sygnały sygnalizacyjne wyższych warstw systemu, kanał identyfikacji abonenta *(hand shake)* - kanał sterujący warstwy MAC - kanał M oraz kanał rozsiewczy (*Broadcasting Channel)* - kanał Q działający jedynie w kierunku od stacji bazowych do ruchomych. Szczelina czasowa może mieć format z protekcją przed błędami lub bez niej. W ostatnim przypadku 320 bitów informacyjnych przesyłanych jest bez zabezpieczenia kodowego. Przy zastosowaniu protekcji dane abonenta podzielone są na cztery bloki 64-bitowe przedzielone 16-bitowymi blokami kontroli parzystości CRC.

Ciągi binarne są transmitowane za pomocą modulacji GMSK o parametrach BT = 0,5 (B jest 3 - decybelową szerokością pasma filtru o charakterystyce gaussowskiej, T – jest to czas trwania pojedynczego bitu). Sygnał taki jest demodulowany w odbiorniku metodą niekoherentną i bez zastosowania korektora adaptacyjnego usuwającego wpływ wielodrogowości. Ponieważ czas trwania pojedynczego bitu przy szybkości transmisji 1152 kbit/s wynosi 0,868 μs, a bez korektora możliwe jest tolerowanie różnicy opóźnień sygnału około 10% czasu trwania pojedynczego bitu, zatem rozproszenie opóźnień nie może być większe niż 200 - 300 ns, co odpowiada różnicy długości dróg poszczególnych promieni (składowych) około 100 m. W przypadku wielu środowisk i wielkości komórki

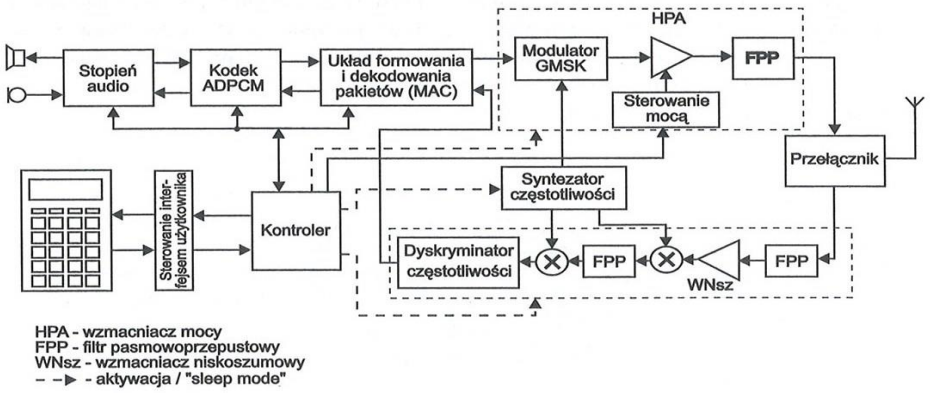
o średniej 200 m warunki te są spełnione. Gdyby zaś tak nie było (np. w dużej hali dworca z doskonale odbijającymi fale elektromagnetyczne ścianami), konieczne jest pieczołowite planowanie rozkładu komórek i wprowadzenie anten sektorowych, Anteny stacji bazowych powinny mieć zysk antenowy około 22 dBi. Stosunek poziomu nośnej do interferencji (C/I) powinien być w systemie DECT co najmniej równy 10 dB. W systemie DECT przewidziano możliwość przenoszenia połączenia pomiędzy komórkami. Założono, że pomiędzy dwoma kolejnymi przeniesieniami połączenia muszą upłynąć co najmniej 3 sekundy. Zapobiega to zbędnym przełączeniom kanałów komórek, co mogłoby mieć miejsce przy równoczesnym stosowaniu w systemie DECT dynamicznego przydziału kanału. Operacja przenoszenia połączenia jest wykonywana przy podanych ograniczeniach wtedy, gdy inna niż aktualna stacja bazowa tego samego zespołu komórek jest odbierana jako silniejsza lub też wtedy, gdy w tej samej komórce inny kanał niż aktualny zapewnia wyższą jakość połączenia w trakcie jego trwania.

System DECT jest instalowany nie tylko w firmach „prywatnych" ale również w miejscach publicznych o dużym natężeniu ruchu telekomunikacyjnego: porty lotnicze, stacje kolejowe czy centra dużych miast. Dodatkową możliwością zastosowania systemu DECT jest współdziałanie z systemem telefonii komórkowej systemu GSM *(Global System for Mobile Communication).* Stosuje się wtedy stacje ruchome o dwóch trybach pracy – trybie GSM i DECT. Taki telefon działa jako telefon komórkowy (stacja mobilna) w miejscach, w których system GSM jest dostępny, lub gdy abonent porusza się z dużą szybkością. W miejscach o szczególnie dużym natężeniu ruchu, w których system GSM nie jest w stanie obsłużyć wszystkich abonentów, ale równocześnie obszar taki objęty jest działaniem systemu DECT, możliwe jest przejście telefonu w tryb DECT. Tak więc na obszarach komórki GSM umieszcza się „wyspy" pokrycia systemem DECT. Na rysunku 5.42 przedstawiono współdziałanie obu systemów.



Rys.5.42. *Współdziałanie systemów GSM i DECT*

Centralny układ sterowania DECT (CCFP) jest dołączony do centrali systemu GSM poprzez znormalizowany interfejs A standardu GSM, i jest przez centralę MSC *(Mobile Switching Center)* widziany jako kontroler stacji bazowych BSC *(Base Station Controller)*. Takie połączenie obu sieci radiokomunikacyjnych zostało zestandaryzowane przez ETSI *(European Telecommunications Standards Institute)* jako profil międzysieciowy systemu GSM *(GSM Interworking Profile)*. W takim połączonym systemie możliwa jest również transmisja danych oraz krótkich wiadomości SMS *(Short Message Services)*.



Rys.5.43. *Schemat blokowy typowej stacji ruchomej systemu DECT*

Rysunek 5.43 przedstawia schemat blokowy typowej stacji mobilnej systemu DECT. Należy zwrócić uwagę, że w stacji ruchomej zarówno część nadawcza jak i odbiorcza są nadzorowane przez układ sterujący, który zajmuje się protokołami transmisyjnymi, sygnalizacją, sterowaniem częścią radiową i sterowaniem styku z użytkownikiem – klawiaturą, wyświetlaczem, i buczkiem. Istotne są również sygnały sterujące włączaniem nadajnika, sterowania poziomem mocy nadawanej, sterowanie wyborem częstotliwości syntezatora oraz wprowadzaniem i wyprowadzaniem poszczególnych części układu nadawczego w stan „uśpienia". Ta funkcja jest bardzo ważna ze względu na konieczność maksymalnego wydłużenia czasu pomiędzy ładowaniem baterii. Podstawową zasadą projektowania stacji ruchomej jest minimalizacja zużycia energii poprzez optymalny podział układu nadawczo – odbiorczego na takie fragmenty, aby możliwie duża część układu była przez większość czasu wyłączona lub znajdowała się w stanie minimalnego poboru prądu.

5.6.3. Systemy trankingowe

Systemy trankingowe są to systemy radiokomunikacyjne z obiektami ruchomymi wyspecjalizowane w łączności niezbędnej w dużych przedsiębiorstwach typu transportowego i służbach specjalnych, np. pogotowiu gazowym, energetycznym, ratunkowym, policji, straży pożarnej itp. Cechą charakterystyczną łączności w tych zastosowaniach jest istnienie centrum dyspozytorskiego, zarządzającego zasobami i ruchem pojazdów z zainstalowanymi stacjami ruchomymi. Pożądane są więc pewne rodzaje specyficznych połączeń, które w zwykłej sieci telefonicznej są możliwe jedynie jako specjalne usługi. Są to rozmowa centrum z wszystkimi stacjami ruchomymi lub z ich wybraną grupą, jak również wspólne połączenie całej grupy.

Systemy trankingowe ewoluowały od systemów z jedną stacją bazową i przydzielonym wspólnym kanałem, w którym poszczególne stacje ruchome mogły się nawzajem słyszeć, przez złożone systemy analogowe, zgodne z normą angielską MPT 1327, poprzez systemy zamknięte (firmowe) np. EDACS Firmy Ericsson, aż do w pełni cyfrowego systemu o standardzie europejskim TETRA mogącym transmitować zarówno głos jak i dane.

Zasadniczą ideą będącą podstawą działania takich systemów jest przydział jednego ze skończonej liczby działających w systemie kanałów jedynie na czas realizacji połączenia i jego zwrot do wspólnej puli kanałów po zakończeniu połączenia. Tym właśnie różni się system trankingowy od klasycznych systemów dyspozytorskich, w których kanały były na stałe przydzielone określonym grupom użytkowników.

Systemy trankingowe zyskują coraz większe znaczenie praktyczne. Wypełniają one potrzebę łączności z poruszającymi się pojazdami wyspecjalizowanych firm np. transportowych, gospodarki komunalnej czy służb takich jak policja, służby energetyczne, pogotowie, straż pożarna i inne. Wiele z tych firm musi liczyć się codziennie z możliwością wystąpienia sytuacji awaryjnych, wymagających szybkiej reakcji i często współdziałania zespołów osób. Inną grupą użytkowników systemów tego typu są firmy, których teren działania jest wprawdzie bardziej zwarty, ale niedogodny dla łączności przewodowej, np. służby obsługi portów, stacji kolejowych i lotnisk, pracownicy firm budowlanych, dużych zakładów pracy, służby ochrony itp.

Opisane powyżej sytuacje mają kilka cech wspólnych. Poszczególni abonenci systemu są pracownikami tej samej firmy, która zgadza się być operatorem systemu

i pokrywać koszty jego działania. Obok pewnej liczby stacji ruchomych, w systemie pracuje jeden, a czasem kilka terminali stałych, obsługiwanych przez dyspozytorów mających uprawnienia do wydawania poleceń pozostałym pracownikom. Większość rozmów odbywa się pomiędzy dyspozytorem a abonentami obsługującymi stacje ruchome. Do wyjątków należą sytuacje, kiedy występuje potrzeba realizacji połączenia z abonentem publicznej stałej sieci telefonicznej. Większość połączeń trwa krótko, a jakość przesyłanego sygnału mowy nie jest sprawą pierwszorzędną gdyż połączenia nie są taryfikowane.

Już od lat 60-tych istniała techniczna możliwość zapewnienia łączności radiowej w opisanych wyżej sytuacjach, poprzez wprowadzanie tzw. systemów dyspozytorskich. Oparte są one na wykupieniu od krajowego urzędu administracji radiowej prawa do wykorzystywania jednego lub kilku kanałów częstotliwościowych na określonym obszarze. Typowa szerokość pasma takiego kanału wynosi 25 kHz, a częstotliwości nośne położone są zwykle w paśmie od 30 do 300 MHz. Typowy system dyspozytorski składa się najczęściej z jednej, rzadziej z kilku stacji bazowych oraz pewnej liczby terminali ruchomych. Łączność prowadzona jest w tzw. kanale otwartym, tzn. każdy użytkownik na bieżąco słucha prowadzonych w kanale rozmów i na tej podstawie decyduje o dostępności lub zajętości kanału. W razie występowania konfliktów, o uprawnieniu do prowadzenia rozmowy, słyszalnej przez pozostałych abonentów, decyduje dyspozytor.

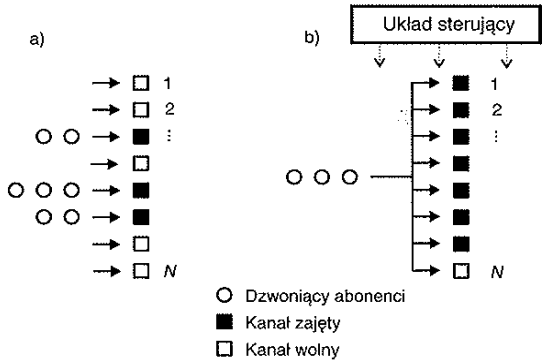
Zazwyczaj takie przedsiębiorstwa i służby mają prywatne systemy łączności ruchomej (PMR – *Private Mobile Radio*). W tradycyjnym rozwiązaniu prywatne systemy łączności ruchomej posiadają kanały radiowe na stałe przyporządkowane określonym zadaniom. Brak odpowiedniego zarządzania kanałami częstotliwościowymi prowadzi do sytuacji, gdy pewne kanały są zajęte dla usiłujących z nich korzystać użytkowników mimo, że inne przydzielone na stałe innym użytkownikom nie są aktualnie wykorzystywane. Takie systemy nazywa się tradycyjnymi systemami dyspozytorskimi.

5.6.3.1. Idea systemów trankingowych

Jednym ze sposobów zwiększających efektywność wykorzystania ograniczonej liczby kanałów radiowych jest technika trankingu *(ang. trunking)*. Polega ona na automatycznym

i dynamicznym przydziale wspólnego zbioru kanałów radiowych znacznie większej liczbie użytkowników, często należących do różnych przedsiębiorstw.

Zasadę realizacji łączności trankingowej pokazano na rys. 5.44. Rysunek 5.44a pokazuje sytuację jaka ma miejsce w klasycznych systemach dyspozytorskich. Na danym terenie istnieje *N* grup użytkowników (np. *N* przedsiębiorstw), z których każda dysponuje jednym kanałem częstotliwościowym. Jeśli w pewnym momencie w niektórych grupach użytkowników jest więcej niż jeden chętny do uzyskania dostępu do kanału, a w innych grupach kanały są niewykorzystane, to i tak niektóre żądania dostępu nie zostaną obsłużone. W systemie trankingowym istnieje wspólna kolejka do wszystkich *N* kanałów (rys. 5.44b). Jeśli tylko łączna liczba żądań obsługi w danej chwili nie przekroczy N, wówczas wszystkie żądania zostaną obsłużone.



Rys.5.44. *Zasada przydziału kanałów radiowych w systemach: a) dyspozytorskim, b) trankingowym*

W praktyce, zasada systemu trankingowego nadaje się do zastosowania zarówno w pokazanej na rys. 5.44 sytuacji, w której system trankingowy zastępuje kilka jednokanałowych systemów dyspozytorskich, jak i w wielkich firmach, które wykorzystują klasyczne systemy dyspozytorskie oparte na wielu kanałach częstotliwościowych. W przypadku systemów trankingowych właścicielem i operatorem systemu może być sam użytkownik, ale także wyspecjalizowana firma operatorska świadcząca usługi na rynku publicznym. W tym pierwszym przypadku mówimy o prywatnym systemie trankingowym (ang. *Private Mobile Radio PMR),* a w tym drugim przypadku o publicznym systemie trankingowym (ang. *Public Access Mobile Radio PAMR).*

Koncepcja trankingu opiera się na teorii prawdopodobieństwa. W szczególności, prawdopodobieństwo tego, że wszyscy użytkownicy chcieliby jednocześnie korzystać

z systemu jest znikome. W konsekwencji, efektywność wykorzystania dynamicznie przydzielanych kanałów jest znacznie wyższa niż w sytuacji gdyby każdy z użytkowników miał swój własny, na stałe przydzielony kanał.

W każdym systemie trankingowym istnieje specjalna procedura (oraz odpowiadające jej urządzenie) sterująca procesem kolejkowania abonentów żądających obsługi oraz przydziałem kanałów. Przypomnijmy, że w systemie dyspozytorskim funkcję tę spełniali poszczególni abonenci, wykonujący bezustanny nasłuch w kanale radiowym. Tak więc, w systemie trankingowym nie zachodzi potrzeba sprawdzania przez indywidualnych użytkowników zajętości kanałów, co umożliwia zachowanie prywatności prowadzonych rozmów. Jest to tym ważniejsze, że systemy trankingowe mogą być użytkowane przez kilka grup użytkowników zatrudnionych w różnych przedsiębiorstwach, dla których wykluczona byłaby łączność w kanale otwartym. Pamiętać jednak trzeba, że w systemach trankingowych nie ma połączeń anonimowych. Każde żądanie zestawienia połączenia jest odnotowane przez „System" – układ sterujący i w przypadku jego niezrealizowania powiadamiany jest Administrator systemu.

Podsumowując, w porównaniu z klasycznymi systemami dyspozytorskimi systemy trankingowe charakteryzują się następującymi zaletami:

- dużą pojemnością, przy ustalonej liczbie kanałów; w rezultacie w systemach trankingowych uzyskuje się wysoką efektywność wykorzystania widma, co pozwala zredukować liczbę kanałów wymaganych do obsługi grupy użytkowników i obniżyć koszty połączeń;
- wysoką niezawodnością działania; w systemie trankingowym awaria pojedyńczego kanału powoduje jedynie spadek jakości oferowanych usług (wydłużenie czasu oczekiwania na przydział kanału) i nie blokuje połączeń w żadnej grupie użytkowników;
- 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 już kanał i zakłócać lub podsłuchiwać zestawionego wcześniej połączenia;

- dostępnością usług trankingowych także dla niewielkich grup użytkowników, generujących mały ruch; użytkownik taki może korzystać z publicznych systemów trankingowych;
- elastycznością systemu; w razie powiększenia się grupy użytkowników łatwo jest zaspokoić zmieniające się potrzeby;
- prostotą obsługi związaną z brakiem konieczności ręcznego przeszukiwania kanałów częstotliwościowych (jak to ma miejsce w systemach dyspozytorskich dysponujących kilkoma kanałami częstotliwościowymi).

5.6.3.2. Klasyfikacja systemów trankingowych

Z jednej strony, jak już wspomniano wcześniej, sieci trankingowe mogą być publiczne oraz prywatne. Sieci publiczne przeznaczone są dla nie powiązanych ze sobą interesami grup użytkowników, którzy stają się abonentami systemu po wykupieniu abonamentu na usługę u wyspecjalizowanego operatora. Użytkownikami sieci publicznych są najczęściej odbiorcy zbiorowi działający na ograniczonym obszarze tj. firmy transportowe, usługowe, służby miejskie. Dla użytkowników takich sieci najważniejszy jest niewielki koszt, prywatność połączeń, a także możliwość dostępu w razie potrzeby do publicznej sieci telefonicznej. Sieci prywatne są przeznaczone wyłącznie dla określonego użytkownika. Służby takie jak policja czy straż pożarna są właścicielami częstotliwości oraz systemu trankingowego, który samodzielnie eksploatują. Najważniejsze wymagania co do funkcjonowania systemu trankingowego dla tego typu użytkowników stanowią: szybki dostęp do kanału radiowego oraz niezawodność pracy systemu, nawet w bardzo trudnych warunkach.

Systemy trankingowe działają na świecie od początku lat 80-tych. Według stanu istniejącego w połowie lat 90 - tych, większość systemów trankingowych działających w Europie, a także w wielu krajach Azji, działa wykorzystując standard MPT zaproponowany pod koniec lat 80-tych przez Brytyjskie Ministerstwo Przemysłu i Handlu *(Ministry of Post and Telecommunication)*. W ramach tego standardu powstało kilka związanych ze sobą norm.

Są to:

- MPT 1327 - standard sygnalizacyjny określający sposób komunikowania się przenośnych terminali ze stacjami bazowymi;
- MPT 1343 - opis styku radiowego dla publicznych sieci trankingowych;

- MPT 1352 - propozycja procedury testów przeznaczonych do homologacji przenośnych terminali używanych w sieciach trankingowych.

Oprócz systemów trankingowych opartych na standardach z rodziny MPT, na świecie działają również systemy opracowane bezpośrednio przez producentów sieci trankingowych. Do bardziej znanych rozwiązań tego typu należą: systemy trankingowe StarSite, SmartNet II oraz SmartZone firmy Motorola oraz system EDACS opracowany przez firmę Ericsson. Rosnące zapotrzebowanie na nowe usługi w systemach trankingowych, potrzeba efektywnego wykorzystania dostępnego pasma, jak również postępująca integracja europejska i związany z tym wymóg współdziałania narodowych służb publicznych doprowadziły w 1990 roku do rozpoczęcia prac w ramach ETSI zmierzających do opracowania standardu nowoczesnego europejskiego cyfrowego systemu trankingowego pod nazwą TETRA *(Trans-European Trunked Radio* lub *Terrestial Trunked Radio).*

5.6.3.3. Systemy trankingowe wykorzystujące standardy MPT

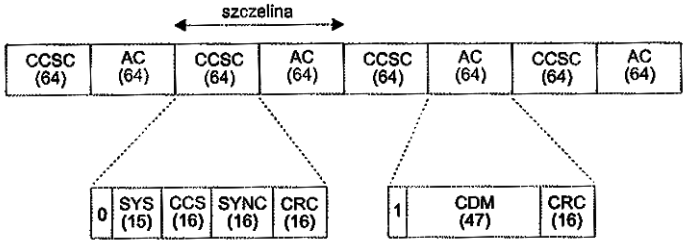
Spośród wymienionych wcześniej standardów z rodziny MPT, najciekawszym wydaje się być standard MPT 1327. Definiuje on protokół komunikacyjny pomiędzy sterownikiem systemu trankingowego a stacjami ruchomymi. Standard ten umożliwia transmisję mowy oraz danych o przepływności 1200 bit/s z normalnym oraz podwyższonym priorytetem. Odbiorcą wiadomości nadawanej przez abonenta sieci trankingowej może być inny indywidualny użytkownik, grupa użytkowników, a także abonent publicznej sieci telefonicznej.

Szerokość kanałów radiowych wykorzystywanych w standardzie MPT 1327 wynosi 12,5 kHz. Jeśli system umożliwia pracę dupleksową, wówczas odstęp pomiędzy kanałami wynosi 8 MHz. Terminale odbierają wiadomości na częstotliwościach z zakresu 193,5 ÷ 199,4875 MHz, nadają je natomiast na częstotliwościach z zakresu 201,5 ÷ 207,4875 MHz. Do transmisji sygnału mowy wykorzystuje się analogową modulację fazy. Dane oraz informacje w kanale sygnalizacyjnym przesyłane są z wykorzystaniem modulacji FFSK *(Fast Frequncy Shift Keying)* o przepływności 1200 bit/s.

W standardzie MPT 1327 zdefiniowano dwa typy kanałów logicznych: kanały rozmówne oraz sygnalizacyjne. Kanał rozmówny używany jest do przesyłania sygnału

mowy. Kanał sygnalizacyjny wykorzystywany jest natomiast do transmisji informacji systemowych tj. do przesyłania sygnałów służących do zestawiania, nadzorowania i rozłączania połączeń oraz do transmisji danych. Kanał sygnalizacyjny może być zrealizowany z wykorzystaniem kanału fizycznego wydzielonego lub współdzielonego. System rankingowy z wydzielonym kanałem sygnalizacyjnym posiada jeden kanał stale dostępny wyłącznie dla sygnalizacji. W przypadku współdzielonego kanału sygnalizacyjnego, układ sterowania sieci umożliwia użycie tego samego kanału również jako kanału rozmównego, jeśli wszystkie pozostałe kanały rozmówne są już zajęte.

Kanały sygnalizacyjne są podzielone na szczeliny o długości 106.7 ms. Każdej szczelinie odpowiada jeden 128-bitowy komunikat (rys.5.45), podzielony na dwa 64-bitowe pola. Pierwsze pole zawiera tzw. słowo systemowe kanału sygnalizacyjnego CCSC *(Control Channel System Codeword)* które umożliwia zarówno identyfikację systemu jaki synchronizację terminali. W drugim polu umieszczone jest tzw. słowo adresowe AC, które zawiera treść komunikatu.



Rys.5.45. *Struktura komunikatu sygnalizacyjnego przesyłanego w kanale sygnalizacyjnym*

W standardzie MPT 1327 dostęp do kanału transmisyjnego oparty jest na algorytmie dostępu ALOHA.

Działanie algorytmu wielodostępu w systemie trankingowym opartym na standardach MPT nie odbiega od klasycznej procedury ALOHA. Na polecenie odpowiednich modułów sterujących pracą systemu trankingowego, poszczególne stacje bazowe wysyłają w kanale sygnalizacyjnym cyklicznie ponawiany komunikat ALOHA. Sygnał ten stanowi zachętę dla terminali do wysyłania zgłoszeń. Z sygnałem ALOHA skojarzony jest parametr *n,* który określa liczbę następujących po nim wolnych szczelin. Po odbiorze sygnału ALOHA, terminal żądający dostępu do kanału rozmownego wybiera w sposób losowy jedną ze szczelin i wysyła w niej swoje

zgłoszenie. W przypadku braku potwierdzenia otrzymania wiadomości przez sterownik systemu, np. na skutek kolizji, terminal po pewnym czasie (długość tego okresu ustalana jest w sposób losowy) ponawia próbę.

Moduł sterujący systemu na bieżąco optymalizuje działanie systemu poprzez zmianę liczby wysyłanych szczelin (parametr n) w zależności od panujących warunków ruchowych. Im ruch w systemie jest większy, tym wartość *n* jest także większa. W celu minimalizacji prawdopodobieństwa kolizji, system może w sygnale ALOHA zezwolić na transmisję zgłoszeń tylko o określonym priorytecie lub pochodzących od terminala o podanym numerze identyfikacyjnym.

W sieciach trankingowych opartych na protokole MPT 1327 można zrealizować m.in. następujące usługi:

- transmisję sygnału mowy w trybie półdupleksowym lub dupleksowym,
- transmisję danych z przepływnością 1200 bit/s,
- transmisję sygnałów alarmowych,
- nadawanie połączeniom różnych priorytetów (normalny lub podwyższony),
- zestawianie połączeń indywidualnych i grupowych,
- połączenia z publiczną siecią telefoniczną,
- przekazywanie rozmów na inny numer.

Każdy z terminali posiada 20-bitowy numer składający się z 7 - bitowego prefiksu oraz 13-bitowego numeru lokalnego. Terminale używane przez jedną grupę użytkowników posiadają ten sam prefiks. Rozwiązanie takie umożliwia realizację wywołań w ramach tej samej grupy użytkowników przy użyciu jedynie numerów skróconych.

W systemie MPT 1327 istnieje możliwość zestawienia połączenia indywidualnego z użytkownikiem należącym do tej samej grupy (tj. posiadającym ten sam prefiks), indywidualnego z użytkownikiem należącym do innej grupy (o innym prefiksie), połączenia grupowego oraz połączenia służącego transmisji danych. Poniżej pokazano przykład procedury sygnalizacyjnej służącej do zestawienia połączenia indywidualnego z abonentem należącym do tej samej grupy.

Podczas zestawiania połączenia, abonent wywołujący musi podać swój numer identyfikacyjny oraz numer abonenta wywoływanego. W przypadku połączenia z użytkownikiem należącym do tej samej grupy, nadawca wysyła najpierw wspólny numer prefiksu, a następnie oba numery lokalne: swój oraz abonenta wywoływanego, W ten sposób oba numery mieszczą się w jednym słowie adresowym.

5.6.3.3.1. Przykład systemu trankingowego opartego na standardach MPT

W tym punkcie omówiony zostanie system Digicom 7 będący przykładem systemu trankingowego opartego na standardach MPT. System Digicom 7 produkcji firmy Alcatel jest dupleksowym systemem trankingowym pracującym w paśmie 170 MHz lub w paśmie 400÷500 MHz. Digicom 7 umożliwia realizację zarówno systemów jednokomórkowych, o stosunkowo niewielkim zasięgu, jak również rozległych sieci wielokomórkowych. W obu przypadkach sieć trankingowa może być połączona z publiczną siecią telefoniczną.

Na rysunku 5.46 przedstawiono architekturę systemu Digicom 7 w realizacji wielokomórkowej.

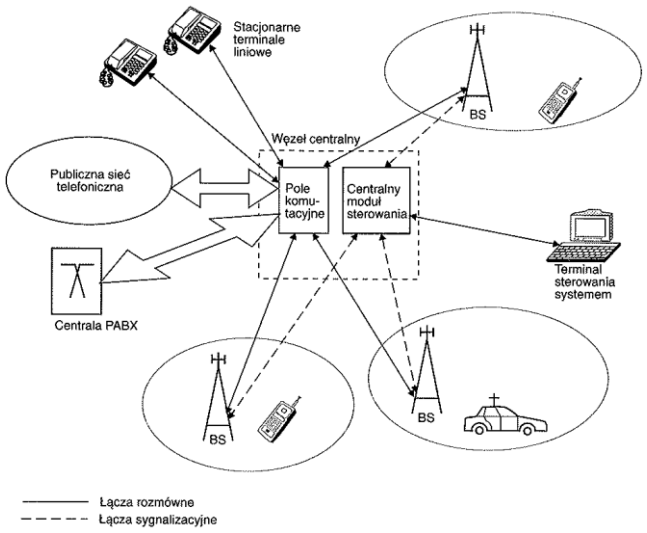
System składa się z następujących elementów:

=> węzła centralnego,

=> stacji bazowych,

=> terminali użytkowników, przenośnych lub przewoźnych

=> terminali stacjonarnych, central PBX (opcjonalnie).



Rys.5.46. *Przykładowa architektura systemu Digicom 7*

Do zadań węzła centralnego należy:

- zestawianie połączeń pomiędzy użytkownikami systemu Digicom 7 oraz pomiędzy użytkownikami systemu Digicom 7 a abonentami publicznej telefonicznej sieci stałej lub abonenckiej centrali PABX,

- zarządzanie pracą sieci, w tym m.in. nadawanie uprawnień terminalom, gromadzenie danych otrzymywanych od stacji bazowych a dotyczących obsługiwanego ruchu oraz nadzór pracy systemów peryferyjnych.

Zestawianie połączeń odbywa się w polu komutacyjnym, realizowanym przy wykorzystaniu cyfrowych central telefonicznych produkowanych przez firmę Alcatel. Funkcje zarządzające pełni centralny moduł sterowania połączony z terminalem sterowania systemem, którym jest komputer klasy PC. Do zadań realizowanych przez terminal sterowania systemem należy m.in.: definiowanie struktury sieci, ustalanie parametrów pracy stacji bazowych, a także zarządzanie bazą danych dotyczącą użytkowników. Do jednego węzła centralnego może być podłączonych do 16 stacji bazowych. Dodatkowo, węzeł centralny umożliwia tworzenie wielkoobszarowych systemów trankingowych. Łączy on wtedy szereg regionalnych systemów Digicom 7 w jedną sieć. Możliwe jest połączenie nawet 16 systemów regionalnych.

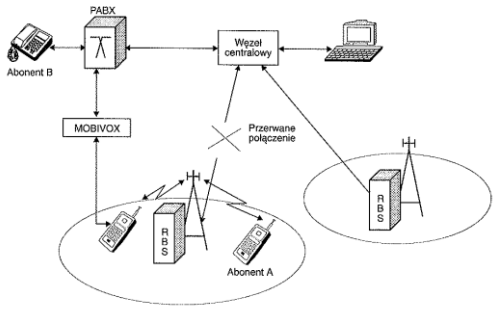
Stacje bazowe w systemie Digicom 7 mają typowo zasięg od 10-ciu do 30 km. Do podstawowych funkcji stacji bazowej należy: nadzorowanie przydziału częstotliwości i określanie funkcji kanałów (kanał: sygnalizacyjny/rozmówny), zestawianie połączeń, przyjmowanie zgłoszeń od terminali, jakie znalazły się na obszarze danej stacji bazowej, rejestrowanie informacji o przebiegu połączenia (dla celów taryfikacji oraz statystyki) itp. Liczba kanałów częstotliwościowych przyporządkowanych jednej stacji bazowej wynosi od 1 do 20. W przypadku systemów o małej pojemności, bez wymogu dostępu do publicznej sieci telefonicznej, stosuje się tzw. samodzielną stację bazową, która nie jest podłączona do węzła centralnego. Umożliwia ona łączność jedynie wewnątrz pojedynczej komórki. W przypadkach, w których wymagane jest zdalne sterowanie, może być ona podłączona do terminala sterowania systemem. W miarę rozwoju sieci, jeśli zajdzie potrzeba zwiększenia pojemności oraz uzyskania dostępu do wszystkich funkcji systemu, samodzielna stacja bazowa może zostać podłączona do węzła centralnego.

Terminale systemu Digicom 7 przystosowane są do pracy z różnymi protokołami sygnalizacyjnymi. Oprócz cyfrowej sygnalizacji zgodnej z normami MPT możliwa jest również min. sygnalizacja trankingowa zgodna z protokołami 3 RP, Chekker, Regionet 43, Speedcom lub Privatex oraz pięciotonowa sygnalizacja

analogowa. Wybór jednego z tych protokołów związany jest ze zmianą oprogramowania terminala; do tego celu terminal wyposażono w odpowiednie złącze.

Dostęp do funkcji terminala wymaga podania żądanego hasła. Terminal umożliwia: łączność głosową, transmisję wiadomości statusowych, transmisję krótkich pakietów danych, przenoszenie połączeń oraz wywołania abonentów publicznej sieci telefonicznej oraz centrali PBX. Terminal posiada alfanumeryczną pamięć wywołań przychodzących oraz pamięć numerów. Interfejs z użytkownikiem składa się z mikrofonu, głośnika, wyświetlacza oraz klawiatury. Dodatkowo istnieje możliwość podłączenia zewnętrznego mikrofonu i głośnika. Podstawowe funkcje terminala takie jak: wywołanie, odbiór wywołania, zakończenie połączenia, regulacja poziomu głośności oraz podświetlanie klawiatury i wyświetlacza dostępne są bezpośrednio z klawiatury. Funkcje specjalne, np. wybór trybu pracy, programowanie terminala oraz korzystanie z pamięci, dostępne są po wciśnięciu kombinacji klawiszy.

W przypadku przerwania łączy pomiędzy węzłem centralnym a stacją bazową istnieje możliwość samodzielnej pracy stacji bazowej, tj. realizowania połączeń w ramach jednej komórki. Jako ciekawostkę warto dodać, że projektanci systemu Digicom 7 zastosowali w systemie rozwiązanie umożliwiające w sposób pośredni uzyskanie połączenia pomiędzy terminalami znajdującymi się w komórce odizolowanej od systemu a centralą abonencką, typowo znajdującą się w głównym budynku użytkownika. Łączność taka wymaga zastosowania modułu specjalnego interfejsu (tzw. Mobivox), który podłącza się z jednej strony do centrali abonenckiej, a z drugiej do terminala przewoźnego systemu Digicom 7 (rys. 5.47).



Rys.5.47. *Zastosowanie interfejsu Mobivox do nawiązania łączności z centralą PABX w przypadku utraty łączności pomiędzy stacją bazową a węzłem centralnym.*

Usługi oferowane przez system Digicom 7 to przede wszystkim transmisja sygnałów mowy, w trybie dupleksowym, półdupleksowym lub w kanale otwartym (tzn. wszyscy abonenci znajdujący się na danym obszarze lub należący do danej grupy słyszą rozmowy prowadzone w kanale). Łączność półdupleksowa wykorzystywana jest do bezpośredniej łączności pomiędzy terminalami bez pośrednictwa stacji bazowej. Praca w kanale otwartym inicjowana jest przez dyspozytora sieci. Dyspozytor przydziela stacje bazowe oraz terminale (lub grupy terminali) do pracy w kanale otwartym. Wszyscy użytkownicy korzystający z kanału otwartego mogą porozumiewać się ze sobą w sposób ciągły w zasięgu określonych przez dyspozytora stacji bazowych.

Obok transmisji sygnałów mowy, system Digicom 7 umożliwia także transmisję danych z prędkością 1200 bit/s. W takim przypadku interfejs pomiędzy terminalem użytkownika a zewnętrznym urządzeniem transmisji danych oparty jest na protokole MAP 27. Usługi dodatkowe oferowane w systemie Digicom 7 to m.in.: łączność z priorytetami, połączenia grupowe i konferencyjne, przenoszenie połączeń, przesyłanie wiadomości statusowych (polega to na przesyłaniu krótkich standardowych wiadomości w kanale sygnalizacyjnym; możliwe jest zdefiniowanie do 32 różnych wiadomości), możliwość ograniczania czasu trwania połączenia w zależności od ruchu generowanego w danej komórce, identyfikacja terminala wywołującego itp.

5.6.3.4. System EDACS

System EDACS (ang. *Enhanced Digital Access Communication System)* oferowany przez firmę Ericsson 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 systemu podczas pracy w niesprzyjających warunkach, w tym także w czasie klęsk żywiołowych, w warunkach nie w pełni sprawnej infrastruktury itp,
- zapewnienie łączności na rozległym obszarze, np. całego kraju,

- hierarchiczna struktura łączności dająca się dopasować do struktury przedsiębiorstwa,
- poufność przekazywanych informacji.

System znalazł zastosowanie, jako prywatny system łączności radiowej *(Private Mobile Radio - PMR)*, w takich służbach jak policja, straż pożarna, energetyka, gazownictwo, ochrona portów lotniczych, może być też wykorzystywany jako publiczny system łączności radiowej *(Public Access Mobile Radio)* świadczący usługi dla mniejszych firm lub przedsiębiorstw.

5.6.3.4.1. Architektura i działanie systemu

System EDACS został zaprojektowany dla konfiguracji, w której ze wspólnej sieci łączności korzysta pewna liczba instytucji, organizacji lub firm, z których każda posiada w sieci starannie określoną autonomię, ale także wzajemne połączenia. W dalszej części opracowania, pod pojęciem „system EDACS" będziemy rozumieć taką część dużej sieci EDACS, w której wykorzystywany jest pojedynczy kanał sygnalizacyjny. Kilka lub kilkanaście systemów EDACS może być połączonych w sieć EDACS. W konfiguracji podstawowej system EDACS składa się z jednej stacji bazowej oraz przenośnych, przewoźnych lub stacjonarnych terminali użytkowników. Stacja bazowa pełni w tym przypadku zarówno funkcje związane z transmisją i odbiorem sygnałów radiowych, jak również funkcje sterujące związane np. z przydzielaniem kanałów radiowych. Stacja bazowa wyposażona jest w jeden kanał sygnalizacyjny oraz w kanały rozmówne, razem maksymalnie 20 kanałów.

W przypadku awarii kanału sygnalizacyjnego, każdy kanał rozmówny jest w stanie przejąć jego funkcję - tę wymienność funkcji realizuje się dzięki wyposażeniu każdego kanału radiowego w specjalny sterownik. Takie działanie stacji bazowej istotnie zwiększa niezawodność systemu.

Opisana powyżej podstawowa konfiguracja systemu, utworzonego wokół pojedynczej stacji bazowej, może być modyfikowana w celu zwiększenia odporności systemu na uszkodzenia oraz liczby dostępnych usług. W systemie EDACS zdefiniowano cztery możliwości stopniowego wzbogacania możliwości systemu polegające, w uproszczeniu na:

=> dołączeniu sterownika stacji bazowej i stanowiska zarządzania systemem,

=> dołączeniu konsoli dyspozytora,

=> dodaniu szyfrowania sygnałów w kanale radiowym,

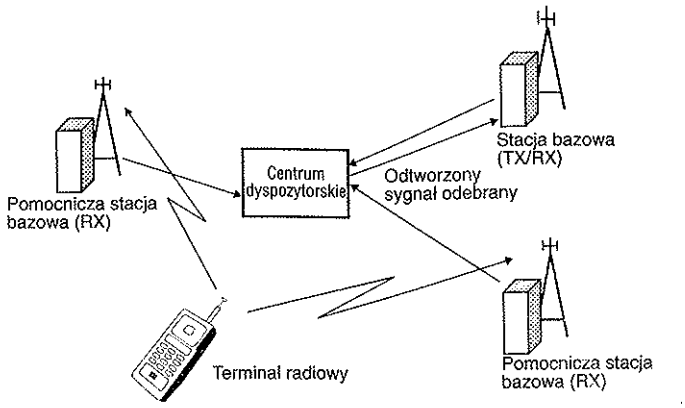
=> zwiększeniu zasięgu radiowego systemu.

Po dodaniu do podstawowej konfiguracji systemu sterownika stacji bazowej oraz stanowiska zarządzania systemem, funkcje zarządzania systemem realizowane zarówno przez sterownik stacji bazowej, jak i samą stację bazową. W przypadku awarii sterownika system przechodzi do pracy w konfiguracji podstawowej. Konsola operatora pozwala dyspozytorowi na utrzymywanie łączności z kilkoma grupami użytkowników równocześnie, a dodanie szyfrowania zwiększa bezpieczeństwo przesyłanych sygnałów. Zwiększenie zasięgu radiowego systemu może odbywać się następująco:

- przez zastosowanie techniki odbioru zbiorczego *(ang. voting system)*
- przez równoczesny odbiór i nadawanie za pomocą kilku różnych stacji bazowych *(ang. simulcast transmission)*.

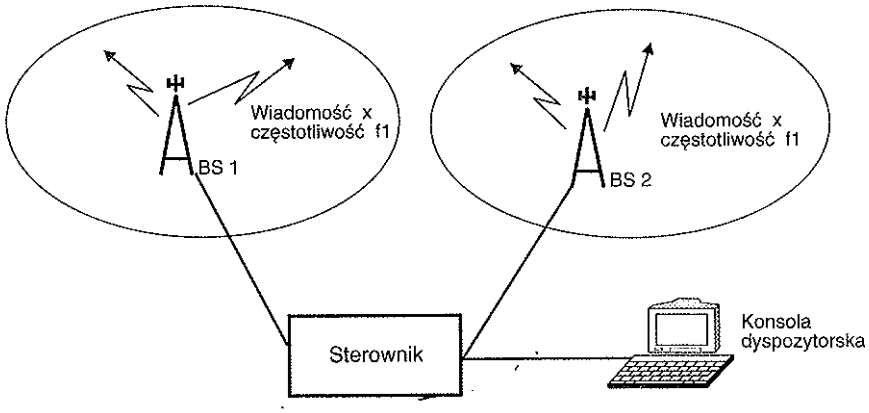
Moc sygnału nadawanego przez stacje bazowe jest większa niż moc sygnałów wysyłanych przez terminale radiowe, może więc się zdarzyć, że terminal odbiera sygnał od stacji bazowej, natomiast stacja bazowa nie jest zdolna odebrać sygnału z terminala.

W systemie EDACS, w takiej sytuacji, zasięg nadawczy terminali radiowych można zwiększyć stosując równoczesny odbiór sygnału radiowego przez kilka stacji bazowych (rys.5.48). W strefie zasięgu stacji bazowej umieszcza się wówczas pewną liczbę pomocniczych stacji bazowych pełniących tylko funkcje odbiorcze. Poszczególne stacje bazowe połączone są łączami stałymi z centrum dyspozytorskim. Pomocnicze stacje bazowe wysyłają odebrane sygnały, cyfrowe oraz analogowe, do centrum dyspozytorskiego, gdzie na ich podstawie odtwarza się sygnał nadany przez terminal, po czym sygnał ten jest przesyłany do właściwej stacji bazowej.



Rys.5.48. *Zasada pracy systemu z odbiorem zbiorczym; TX – nadajnik, RX - odbiornik*

Drugie rozwiązanie pozwala zwiększyć zasięg systemu przez zwiększenie liczby stacji bazowych (rys. 5.49). Te same analogowe lub cyfrowe informacje nadawane są z kilku stacji bazowych równocześnie i na tej samej częstotliwości radiowej, bez podziału czasowego. Każda stacja bazowa podłączona jest łączami stałymi do centralnego sterownika. Ułatwia to uzyskanie pełnego pokrycia radiowego na większych obszarach warunkach, w których stworzenie klasycznego planu częstotliwości, typowego dla systemów komórkowych, jest niemożliwe lub niecelowe. W kierunku odbiorczym system działa w ten sam sposób jak system z odbiorem zbiorczym.

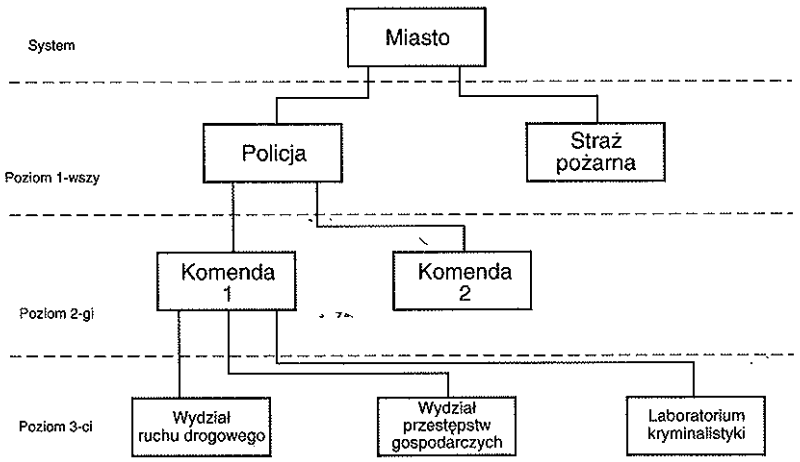


Rys.5.49. *Zwiększanie zasięgu systemu za pomocą równoczesnej pracy dwukierunkowej kilku stacji bazowych*

Przedstawione powyżej konfiguracje dotyczyły pojedynczego systemu, zbudowanego wokół jednej stacji bazowej (ewentualnie kilku stacji bazowych

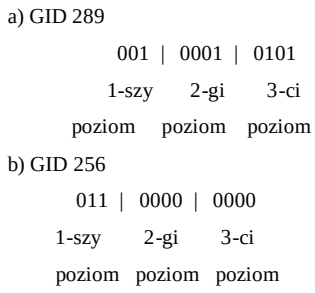
pracujących w trybie *simulcast).* Jeśli zasięg jednej stacji bazowej nie wystarcza do pokrycia obszaru, na którym mają być dostępne usługi, tworzy się sieć. Sieć łączy ze sobą systemy pracujące w tych samych lub różnych konfiguracjach za pomocą dodatkowego sterownika sieci. W ramach sieci użytkownicy mogą przemieszczać się z jednego systemu do drugiego oraz generować połączenia międzysystemowe. Sterownik sieci jest odpowiedzialny za kierowanie połączeń między systemami oraz za śledzenie ruchu abonentów.

Organizacja łączności w systemie EDACS opiera się na hierarchicznej strukturze tzw. grup użytkowników. Na rys. 5.50 przedstawiono organizację grup na przykładzie systemu łączności dla służb miejskich. Na najwyższym poziomie znajduje się system obejmujący swoim zasięgiem wszystkie służby miejskie, a dalej następuje trzypoziomowy podział hierarchiczny na kolejne, coraz mniejsze grupy użytkowników. Tak więc, system dzieli się najpierw na podzespoły zespoły 1-szego poziomu (ang.*Agency)* w rozważanym przypadku mogą to być poszczególne służby np. policja, straż pożarna itp. Dalej następuje podział podzespoły 2-go poziomu (ang.*fleet),* np. w przypadku policji mogą to być poszczególne komendy policji w mieście, oraz podzespoły 3-go poziomu *(ang. subfleet),* którym mogą odpowiadać np. wydziały w danej komendzie policji wydział drogowy, wydział przestępstw gospodarczych, laboratorium kryminalistyki itp.



Rys.5.50. *Hierarchia grup w systemie EDACS na przykładzie systemu łączności służb miejskich*

Na najniższym poziomie znajdują się terminale użytkowników. Pełen adres systemowy zawiera 14 bitów, tak więc przestrzeń adresowa zawiera ponad 16 000 kombinacji. Aby zrealizować wywołanie grupowe, należy wybrać 11 – bitowy adres grupy GID *(ang. Group ID),* który tworzą: adres podzespołu 1 – szego poziomu, adres podzespołu 2 – poziomu (min. 1 bit) oraz adres podzespołu 3 – poziomu (min. 2- bity). Na rys. 5.51a pokazano przykładowy adres grupy dla wywołania realizowanego na poziomie podzespołu 3 – poziomu. Na wywołanie odpowiedzą wszystkie terminale należne do podzespołu 3-go poziomu oznaczonego numerem 5. Na rys. 5.51b przedstawiono przykład wywołania grupowego w ramach podzespołu 1-go poziomu. W tym przypadku na wywołanie odpowiedzą terminale wszystkiej podzespołów niższych poziomów należących do podzespołu 1-szego poziomu oznaczonego numerem 3.



Rys.5.51.*Struktura adresu grupy dla wywołania grupowego:*
a) w ramach podzespołu 3-go poziomu,
b) w ramach podzespołu 1 - szego poziomu

Przedstawiony sposób adresowania połączeń oznacza, że w systemie EDACS struktura grup wpisana jest w system sygnalizacyjny. Innym rozwiązaniem mogłoby być dynamiczne łączenie odpowiednich podzespołów w przypadku wywołania grupowego. Do tego celu musiałaby jednak istnieć centralna baza danych przechowująca informacje o istniejących podzespołach. Jednakże w przypadku krytycznym zerwanie łączności pomiędzy bazą danych a systemem uniemożliwiłoby zestawianie połączeń.

5.6.3.4.2. Transmisja w kanale radiowym

System EDACS dostępny jest w wersji szerokokanałowej oraz wąskokanałowej. W wersji szerokokanałowej odstęp pomiędzy sąsiednimi kanałami częstotliwościowymi wynosi 25 kHz lub 30 kHz, a w wersji wąskokanałowej kanały mają szerokość 12.5 kHz. System EDACS może pracować w wersji szerokokanałowej

w kilku pasmach częstotliwości: 136-174 MHz,403 ÷ 515 MHz i 806 ÷ 870MHz. Wersja wąskokanałowa dostępna jest tylko w paśmie896 ÷ 941MHz.

System umożliwia trzy rodzaje transmisji:

→ transmisję analogowego sygnału mowy,

→ transmisję cyfrowego sygnału mowy,

→ cyfrową transmisję danych.

Analogowy sygnał mowy może być transmitowany zarówno wersji szeroko - jak i wąskokanałowej, sygnalizację realizuje się wówczas cyfrowo z przepływnością 9600 bit/s. Transmisja danych oraz cyfrowo zakodowanej mowy w wersji szerokokanałowej odbywa się także z prędkością 9600 bit/s. Kodowany cyfrowo sygnał mowy jest dodatkowo szyfrowany przy użyciu jednego z kilku algorytmów kryptograficznych. W wersji wąskokanałowej nie jest możliwa cyfrowa transmisja sygnału mowy, a dane przesyła się z prędkością 4800 bit/s.

5.6.3.4.3. Usługi

W zależności od konfiguracji, system umożliwia zestawianie połączeń pomiędzy terminalami oraz połączeń dyspozytorskich pomiędzy terminalem lub terminalami radiowymi i konsolą dyspozytorską. Możliwe są cztery rodzaje połączeń:

→ połączenia grupowe,

→ połączenia grupowe alarmowe,

→ połączenia indywidualne,

→ połączenia systemowe.

Połączenia grupowe w systemie EDACS są usługą typową dla systemów trankingowych. W zależności od adresu grupy mogą być one zestawiane i trzech poziomach (rys. 5.51). Połączenia grupowe są dostępne we wszystkich trzech rodzajach transmisji: przy analogowej i cyfrowej transmisji mowy oraz przy cyfrowej transmisji danych.

Połączenia alarmowe generowane są po naciśnięciu odpowiedniego przycisku w terminalu. System po rozpoznaniu zgłoszenia alarmowego przydziela połączeniu wolny kanał lub w przypadku braku wolnych zasobów wstawia zgłoszenie alarmowe na początek kolejki zgłoszeń oczekujących na wolny kanał rozmówny. W przypadku zwykłych połączeń rozmownych stosuje się przydzielanie kanału rozmównego jedynie

na czas rzeczywistej transmisji w danym kierunku *(po zwolnieniu przycisku PTT ang. Push To Talk)*. W przypadku połączeń alarmowych stosuje się przydział kanału radiowego na cały czas trwania połączenia. Połączenia alarmowe zestawiane do dyspozytora oraz do innych członków grupy *(ang. Emergency Group Notification).* Tylko dyspozytor lub terminal z odpowiednimi uprawnieniami mogą zakończyć grupowe połączenie alarmowe.

Połączenie indywidualne pozwala na prowadzenie rozmowy między dwoma terminalami, która nie jest słyszalna przez innych użytkowników systemu. Połączenie indywidualne może zostać zestawione przez dyspozytora lub przez odpowiednio wyposażony terminal. Połączenia takie dostępne są dla analogowej i cyfrowej transmisji mowy oraz dla cyfrowej transmisji danych.

Połączenia systemowe umożliwiają operatorowi systemu *(ang. Supervisor),* wyposażonemu w terminal z zaprogramowanymi odpowiednimi uprawnieniami, nawiązać natychmiastową łączność ze wszystkimi użytkownikami w systemie. Wygenerowanie połączenia systemowego powoduje przerwanie wszystkich realizowanych połączeń i zestawienie pojedynczego kanału do wszystkich użytkowników w systemie. Połączenie systemowe mogą być wykonywane tylko dla analogowej transmisji mowy.

5.6.3.5. Standard TETRA

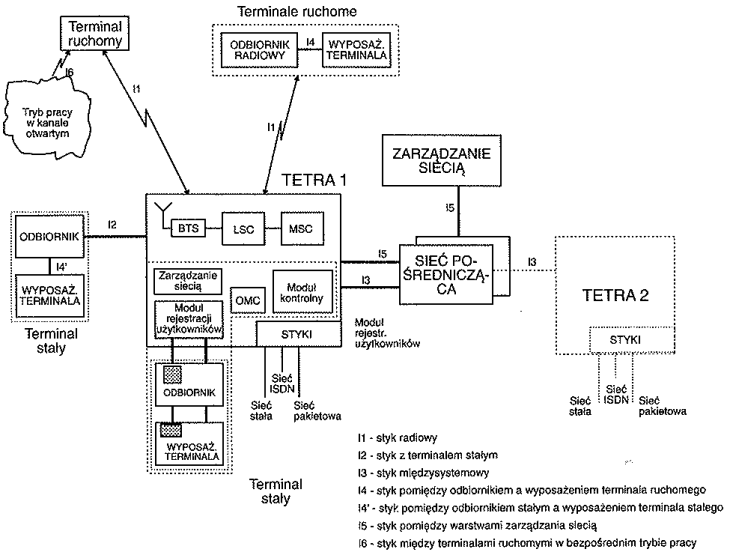
Standard TETRA (ang.: *Trans European Trunked Radio)* jest europejskim cyfrowym standardem dotyczącym łączności trankingowej, opracowywanym przez ETSI od 1992 roku. Światowy sukces standardu GSM sprawia, że wielu ekspertów przewiduje rozpowszechnienie się standardu TETRA także na innych kontynentach. Poniżej omówiono podstawowe cechy tego standardu.

5.6.3.5.1. Architektura systemu i interfejs radiowy

Standard TETRA został zaprojektowany w sposób, który umożliwia efektywne przesyłanie w kanale radiowym zarówno sygnałów mowy jaki i danych, w trybie połączeniowym, a także w trybie pakietowym (dotyczy tylko przypadku transmisji danych). Istotnym wymaganiem stawianym projektantom była także możliwość współpracy systemów eksploatowanych przez różnych operatorów.

Architekturę ogólną przykładowego systemu TETRA pokazano na rys. 5.52. Można w niej 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 sterownikami stacji bazowych w systemie GSM. W części komutacyjno-sieciowej znajduje się jeszcze 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 systemie TETRA wyróżniamy dwa typy terminali: terminale ruchome oraz terminale stałe, obsługiwane typowo przez dyspozytora systemu. Podobnie jak to ma miejsce w systemach telefonii komórkowej, terminale ruchome mogą mieć tylko najprostsze funkcje pozwalające na transmisję sygnałów mowy, ale mogą mieć także połączenie z urządzeniami pozwalającymi na transmisję danych i inne usługi. Sieć TETRA poprzez sieci tranzytowe może być połączone także z sieciami TETRA innych operatorów. W omawianym standardzie zdefiniowano liczne standardowe interfejsy (rys. 5.52) Jest wśród nich interfejs radiowy, w dwóch wersjach: do pracy w kanale prywatnym (styk I1) oraz do pracy w trybie bezpośrednim (styk I6), a także styk z terminalami stałymi (styk I2). Oprócz tego, zdefiniowano również styk terminala z jego wyposażeniem (styki I4 i I4') oraz styk pomiędzy sieciami TETRA obsługiwanymi przez różnych operatorów (styki I3 i I5).



Rys.5.52. *Architektura systemu trankingowego TETRA; BTS (Base Transceivwer Station)- stacja bazowa, LSC (Local Switching Centre) - centrala lokalna, MSC (Main Switching Centre) - centrala główna, OMC (Operations & Maintenance Centre) - centrum eksploatacji i utrzymania sieci*

.

5.6.3.5.2. Transmisja w kanale radiowym

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 ramkowa pozwalająca na utworzenie czterech kanałów rozmównych zwielokrotnionych czasowo. Tak więc, efektywna szerokość pasma zajmowanego przez pojedynczy kanał rozmówny wynosi 6,25 kHz. Transmisja w kanale radiowym odbywa się z wykorzystaniem modulacji $\pi/4$ DQPSK *(Differential Quadrature Phese Shift Keying)* tj. różnicowej kwadraturowej modulacji fazy z przesunięciem o $\pi/4$.

Sygnały mowy kodowane są z przepływnością 4.8 kbit/s, co zapewnia jakość transmisji niższą wprawdzie niż w telefonii publicznej, ale wystarczającą dla systemów prywatnych. Tak więc, sumaryczna przepływność danych w pojedynczym kanale częstotliwościowym wynosi 19.2 kbit/s a po kodowana protekcyjnym 36 kbit/s. Dostęp do kanału radiowego realizowany jest przy pomocy omawianego wcześniej algorytmu ALOHA. Zdefiniowano trzy klasy terminali ruchomych,o mocach odpowiednio:

1, 3 i 10 W. Umożliwia to realizację zasięgów nawet do 60 km od stacji bazowej. Podstawowe parametry techniczne opisujące interfejs radiowy standardu TETRA zebrano w tabeli 5.3.

Tabela 5.3. Ważniejsze parametry standardu TETRA

Parametr	Wartość
Modulacja	π/4 DQPSK
Odstęp między sąsiednimi nośnymi	25 kHz
Liczba kanałów na jednej nośnej	4
Zwielokrotnienie dostępu	FDMA/TDMA
Przepływność danych na jednej nośnej	19,2 kbit/s
Przepływność danych po kodowaniu protekcyjnym	36 kbit/s
Szybkość modulacji	18 kbodów
Algorytm dostępu do kanału transmisyjnego	ALOHA
Czas zestawiania połączenia	300 ms
Czas przejścia terminala z obszaru działania jednej stacji bazowej w zasięg drugiej	< 1 s
Klasy mocy terminali ruchomych	1, 3 oraz 10 W
Wielkość komórek	Do 60 km
Maksymalna prędkość terminala	Do 200 km/h

Intencją twórców standardu TETRA było zdefiniowanie systemu który mógłby być używany co najmniej w całej Europie. Aby to zrealizować, konieczne było znalezienie pasma częstotliwości dogodnego dla wszystkich krajów Europy (w praktyce, dostępnego choćby w większości krajów Europy). Niestety, okazało się, że w Europie w zakresie poniżej 1 GHz nie istnieje pasmo częstotliwości o szerokości 220 MHz, które byłoby powszechnie dostępne. Następną możliwością był przydział częstotliwości w kilku mniejszych, nie przylegających do siebie pasmach. Rozważano m.in. pasma: 410÷439 MHz, 450÷470 MHz, 870÷888 MHz i 915÷933 MHz. Rozwiązania tego nie uznano jednak za zadawalające i w wyniku kolejnych negocjacji uzyskano zgodę NATO na pracę przyszłościowych systemów TETRA w części pasma będącego dotąd w dyspozycji systemów łączności wojskowej: 380÷400 MHz (jest to niewielki fragment pasma 225÷400 MHz, będącego w całości w dyspozycji systemów wojskowych NATO). Podpisane porozumienie z NATO zezwala na pracę

w przydzielonym paśmie jedynie systemom trankingowym będącym w dyspozycji służb publicznych.

5.6.3.5.3. Tryby pracy systemu

Standard TETRA definiuje dwa podstawowe tryby pracy systemu:

=> *Voice plus Data* (w skrócie: TETRA VD), służący do transmisji sygnału mowy oraz danych,

=> *Packet Optimized Data* (w skrócie: TETRA POD), przeznaczony wyłącznie do transmisji danych.

W standardzie TETRA *Voice plus Data* system pracuje w trybie połączeniowym. Transmisja sygnałów mowy realizowana jest w opisanych wcześniej kanałach rozmownych zwielokrotnianych czasowo po cztery na każdej nośnej. Transmisja danych realizowana jest z przepływnością dopasowywaną do aktualnych potrzeb użytkownika. Układ sterujący umożliwia korzystanie w części lub w całości z czterech szczelin czasowych znajdujących się w obrębie każdego kanału częstotliwościowego. Oznacza to możliwość transmisji danych z szybkościami od 4.8 kbit/s do 19.2 kbit/s. W tym trybie pracy możliwa jest także łączność bezpośrednia pomiędzy terminalami, z pominięciem stacji bazowej (tryb DMO), zarówno wewnątrz jak i na zewnątrz obszaru działania sieci trankingowej. Dla celów takiej transmisji zdefiniowano specjalny styk radiowy I6 (rys. 5.52).

Standard TETRA w wariancie *Packet Optimized Data* został zoptymalizowany pod kątem transmisji danych i będzie wykorzystywany w aplikacjach, w których transmisja głosu nie jest wymagana. W tym wariancie, system ten może przesyłać dane zarówno w trybie połączeniowym jak i bezpołączeniowym. Transmisja danych może być wówczas realizowana z różnymi priorytetami, do odbiorców indywidualnych oraz grupowych, z przepływnością do 19.2 kbit/s.

5.6.3.5.4. Procedury sieciowe w systemie

Każdy system łączności do swojego poprawnego działania potrzebuje szeregu procedur sieciowych. System TETRA definiuje wiele takich procedur, 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".

Procedury te w wielu aspektach są podobne to odpowiednich procedur obowiązujących w systemie GSM. Procedury wykorzystywane w standardzie TETRA będą pokrótce, kolejno, omówione poniżej. Podobnie jak w systemie GSM, decyzja o zmianie komórki, w obrębie które działa terminal, jest podejmowana samodzielnie przez terminal przy wykorzystaniu cyklicznie wykonywanych pomiarów sygnałów pochodzących od okolicznych stacji bazowych. Ze zmianą stacji bazowej może być związana również zmian obszaru lokalizacji (obszar lokalizacji to część obszaru centralowego; system rejestruje zmiany położenia abonentów tylko jeśli zmieniają oni obszar lokalizacji), w którym zarejestrowano odbiornik w systemie. W takim przypadku terminal podaje przez kanał radiowy do rejestru systemowego dane dotyczące swojego nowego położenia. W trakcie rejestracji terminala w nowym obszarze lokalizacji system może przeprowadzić ponowną procedurę identyfikacji terminala.

Jeśli terminal znajdzie się poza obszarem działania sieci, w której jest zarejestrowany, o ile operatorzy sieci TETRA zawarli odpowiednie porozumienie abonent może korzystać z zasobów sieci TETRA eksploatowanej przez innego operatora. Migracja do innej sieci jest możliwa dzięki szczegółowemu zdefiniowaniu styku pomiędzy dwoma sieciami TETRA, w tym metod wymiany informacji o zarejestrowanych użytkownikach, oraz rozwiązaniu kwestii naliczania opłat.

Bardzo istotnym aspektem standardu TETRA, szczególnie wobec perspektywy wykorzystania go m.in. w takich służbach jak policja, wojsko itp., jest zabezpieczenie systemu przed niepowołanym dostępem do usług, do informacji, a także przed używaniem skradzionych terminali. Procedura identyfikacji przeprowadzana jest przez system w zasadzie każdorazowo podczas rejestracji terminala w nowym obszarze lokalizacji. Sposób identyfikowania abonentów w standardzie TETRA jest zbliżony do metod wykorzystywanych w standardzie GSM.

Terminale w systemie TETRA umieszczane są na dwóch listach: terminali włączonych i wyłączonych. Wiadomości przeznaczone dla terminali włączonych są im przekazywane natychmiast, a wiadomości przeznaczone dla terminali wyłączonych są przechowywane w pamięci systemu. Włączenie zasilania terminalu powoduje, że terminal próbuje odczytać informacje z kanału sygnalizacyjnego stacji bazowej, w której był zarejestrowany przed wyłączeniem. Gdy odnalezienie tego kanału jest niemożliwe, wówczas terminal przeszukuje pozostałe kanały radiowe w celu znalezienia nowego kanału sygnalizacyjnego. Jeśli kanał taki zostanie znaleziony, wtedy terminal wykonuje procedurę inicjalizacji, która polega na wysłaniu żądania uaktualnienia swojego statusu w systemie (tj. zmiany statusu na włączony oraz wpisania aktualnego położenia stacji ruchomej). W odpowiedzi, system zmienia status terminala oraz sprawdza czy w pamięci systemu nie znajdują się przesłane do niego wcześniej wiadomości, sygnalizacyjne lub wiadomości od innych użytkowników.

Wyłączenie zasilania w terminalu powoduje automatyczne wysłanie przez terminal żądania wyrejestrowania terminala z systemu, co w rejestrze systemowym powoduje zmianę statusu terminala na wyłączony. W przypadku kiedy system, po określonej liczbie prób, nie może nawiązać łączności z terminalem zakłada się, że terminal jest poza jego zasięgiem i jego status automatycznie zmieniany jest na wyłączony.

Użytkownik przed przystąpieniem do pracy w systemie na określonym terminalu, musi przekazać do systemu dane umożliwiające identyfikację pary: użytkownik - terminal. Procedurę tę realizuje się przez wprowadzenie do terminala odpowiedniej karty identyfikacyjnej lub podanie hasła. Zastosowanie takiej procedury zwiększa bezpieczeństwo pracy w systemie, a także umożliwia pracę użytkownika na różnych terminalach. Dzięki temu wiadomości przeznaczone dla danego użytkownika są kierowane do terminala, na którym użytkownik aktualnie pracuje.

Standard TETRA jest bardzo obszerny i nie sposób wyczerpująco go, w takim opracowaniu, omówić. Posiada on szereg cech ułatwiających pracę użytkowników i zwiększających jej efektywność. Na przykład, system pozwala na chwilowe zawieszenie transmisji, a następnie jej wznowienie, na zlecenie terminala. Do wysłania sygnału chwilowego zawieszenia transmisji dochodzi m.in. w sytuacji, gdy terminal jest przepełniony i nie nadąża z przetwarzaniem nadchodzących danych. Nadchodzące do terminala dane są wówczas przechowywane w pamięci systemu i przekazywane do terminala po otrzymaniu od niego zlecenia wznowienia transmisji.

5.6.3.5.5. Usługi

Standard TETRA przewiduje realizację bardzo szerokiego wachlarza usług, począwszy od transmisji sygnałów mowy w różnych wariantach, poprzez różnorodne formy transmisji danych, do klasycznych usług dodatkowych typu przekazywanie rozmów, blokowanie określonych połączeń itp. Wiele z tych usług znanych jest z nowoczesnych systemów telefonii komórkowej. Standard oferuje także cały szereg usług niespotykanych w typowych systemach komórkowych: od monitorowania rozmów przez rozbudowane możliwości nadawania priorytetów po tzw. dyskretne słuchanie.

Poniżej wymieniono ważniejsze usługi zdefiniowane w standardzie TETRA:

- transmisja sygnałów mowy, półdupleksowa lub dupleksowa, z szyfrowaniem lub bez, do abonentów indywidualnych lub grupowych,
- transmisja danych, w trybie połączeniowym, z szyfrowaniem lub bez, z różnymi poziomami zabezpieczenia przed błędami, z maksymalnymi przepływnościami od 9.6 kbit/s (wysokie zabezpieczenie przed błędami) nawet do 28.8 kbit/s (brak kodowania protekcyjnego), do abonentów indywidualnych lub grupowych,
- pakietowa transmisja danych, w tym także 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,
- autoryzację zestawianych połączeń przez centrum nadzoru, np. w sieciach używanych przez policję,
- dyskretne słuchanie - oznacza to, że użytkownik posiadający takie uprawnienia może monitorować rozmowy prowadzone przez innych użytkowników,
- możliwość warunkowego zestawiania połączeń, np. tylko wtedy abonent wywoływany znajduje się na wskazanym obszarze,

- przechowywanie przez system wiadomości użytkowników chwilowo nieobecnych w systemie (nieaktywnych) i ich przekazywanie po wznowieniu przez nich pracy.

Na zakończenie warto dodać, że 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. Na przykład przewiduje się, że wysoka przepływność danych oferowana przez system umożliwi policji, po raz pierwszy, m.in. transmisję z centrum nadzoru do radiowozu zdjęć przedstawiających poszukiwano osoby, a w przeciwną stronę przekazywanie zdjęć z miejsca wypadku.

5.6.3.5.6. Stan obecny i perspektywy rozwoju systemów trankingowych

Systemy trankingowe działają w Polsce od roku 1991, kiedy to powstała sieć Radio-Net, której operatorem jest spółka Uni-Net i Telekomunikacja Polska SA. Pracuje ona wykorzystując opisane w punkcie 5.7.3.4 standardy MPT, System ten dysponował w połowie lat 90-tych około 20 stacjami bazowymi, zlokalizowanymi w większych miastach Polski. Oprócz sieci Radio-Net, powstały także dwie sieci o mniejszych zasięgach: sieć Metrobip działająca w kilku miastach Polski, w której wykorzystywany jest system firmowy Motoroli StartSite, oraz sieć Akselnet działająca na Śląsku, wykorzystująca standardy MPT. Wszystkie wymienione powyżej sieci mają nieciągłe pokrycie radiowe i oferują łączność w większych aglomeracjach miejskich i ich bezpośredniej okolicy. Poza wymienionymi powyżej sieciami publicznymi, w Polsce działają także sieci prywatne. Należą do nich m.in: oparty na standardach MPT system AktionNet firmy Nokia używany przez płocką Petrochemię, oparty na standardach MPT system Digicom firmy Alcatel wykorzystywany przez energetykę, system Key firmy Key Radiosystems będący w użyciu przez PLL LOT, a także system trankingowy EDACS firmy Ericsson wykorzystywany przez policję (w aglomeracji warszawskiej również PSP).

Publiczne systemy trankingowe w Polsce wdrożone w połowie lat 90-tych ubiegłego wieku, cierpiały przede wszystkim na niedostateczną liczbę abonentów. Optymistyczne prognozy dotyczące szybkiego wzrostu liczby abonentów w tych systemach nie zostały spełnione. Na taki stan rzeczy wpłynęło wiele czynników, w tym przede wszystkim brak dłuższej tradycji stosowania łączności przez średnie i małe

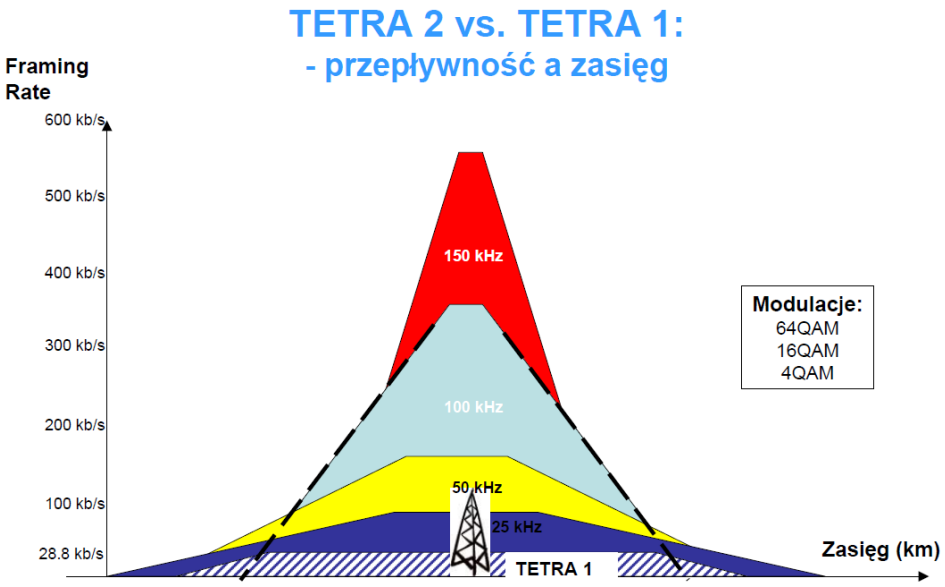
firmy, a dla nich przede wszystkim przeznaczone są publiczne sieci trankingowe. Problemy operatorów sieci prywatnych są innego typu. Operatorzy finansowani z budżetu państwa, tacy jak policja, służby celne czy straż pożarna, nie dysponują dostatecznymi środkami co opóźnia wprowadzanie nowych generacji systemów łączności. Operatorzy prywatni, tacy jak energetyka czy gazownictwo mają niekiedy wrażenie, że brak jest systemu w pełni odpowiadającego wymaganiom przełomu wieków: analogowe systemy pierwszej generacji stają się powoli przestarzałe, rozwiązania firmowe poszczególnych producentów nie wydają się także wystarczająco perspektywiczne, a prawdziwy standard drugiej generacji, tj. TETRA, została wdrożona na potrzeby Policji w czterech ośrodkach miejskich Warszawa, Szczecin, Łódź i Kraków i ze względów finansowych nie była dalej rozwijana. Nadzieje na zbudowanie systemu TETRA w ramach *ofsetu* za zakup samolotów wielozadaniowych F-16 dla polskiej armii też okazała się złudna.

Opinie ekspertów dotyczące perspektyw rozwoju systemów trankingowych na świecie są podzielone. Głównym powodem tego jest szybkie rozprzestrzenianie się i poszerzanie wachlarza usług oferowanych przez systemy telefonii komórkowej. Z jednej strony, służby publiczne w każdym kraju mają tak specyficzne wymogi, że trudno sobie wyobrazić aby korzystały one z publicznych systemów komórkowych, nawet po uzupełnieniu ich o priorytetowanie rozmów, wywołania grupowe i rozbudowaną transmisję danych. Z drugiej strony, dla potencjalnych abonentów trankingowych systemów publicznych zmodyfikowane, masowe, a przez to bardzo tanie systemy komórkowe mogą stanowić w niedalekiej przyszłości atrakcyjną alternatywę. Odpowiada to ogólniejszej tendencji do tworzenia telekomunikacyjnych systemów zintegrowanych, w których ta sama infrastruktura oferuje możliwie szeroki zakres usług. Wydaje się więc, że przyszłość standardu TETRA jest bezdyskusyjna przynajmniej w zakresie jego zastosowania dla policji, służb ratowniczych itp. Na wyjaśnienie pytań dotyczących perspektyw rozwoju "cywilnych" systemów trankingowych, w tym systemów TETRA, przyjdzie nam jeszcze poczekać kilka lat. Oczywiście w ETSI trwały prace nad dalszym rozwojem standardu. Na przełomie lat dziewięćdziesiątych i dwutysięcznych opublikowany został standard TETRA2 znany pod akronimem TEDS *(TETRA Enhanced Data Service).* TEDS jest to część standardów TETRA Wydanie 2, wywodząca się od Wydania 1, z którym zachowuje zgodność wsteczną. TEDS zapewnia stopniową zmianę przepływności danych

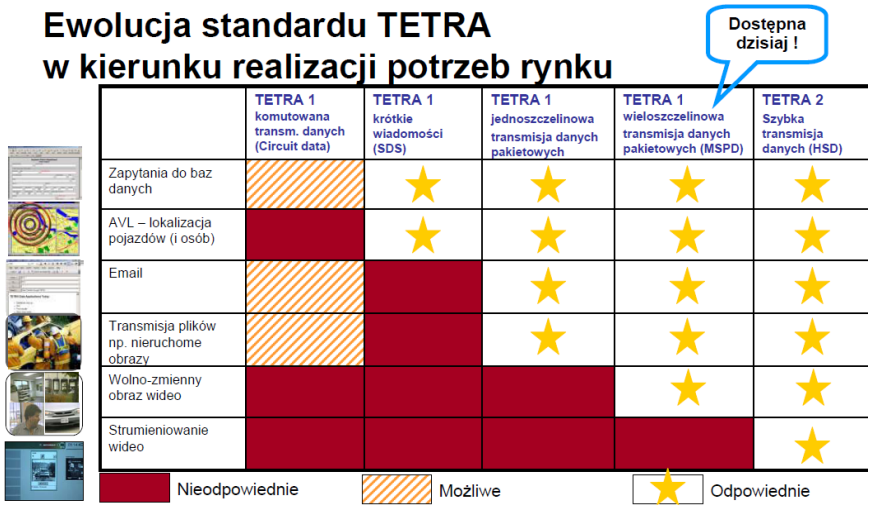
dostępnych poprzez TETRA, realizując w ten sposób potrzebę coraz szybszej transmisji danych. Główne zalety TEDS:

- Korzystanie z tych samych, zatwierdzonych przez władze mechanizmów zabezpieczeń, dzięki którym TETRA1 ma tak wysoki poziom bezpieczeństwa,
- Możliwość wprowadzenia do istniejącej sieci TETRA1 jako aktualizacja; w dużym stopniu upraszcza działanie i utrzymanie ze strony operatora sieci, dzięki czemu unika się ryzyka operacyjnego związanego z koniecznością wydzieleniem oddzielnej sieci łączności krytycznej dla szybkiej transmisji danych,
- Ekonomiczność wykorzystania spektrum oznacza, że TEDS można wpasować w dostępne pasma istniejącego zakresu częstotliwości TETRA, a nawet zastąpić obecne kanały przeznaczone dla danych i zapewnić znacznie większą przepustowość. Unika się kosztownego i czasochłonnego procesu wyszukiwania nowego spektrum dla oddzielnej szybkiej sieci danych.

Rozważając wdrożenie tego nowego rozwiązania należy rozważyć wyważenie wymagań w zakresie pokrycia i przepustowości. Przy określaniu co najmniej suboptymalnego rozwiązania należy uwzględnić stosunek pomiędzy szybkością przesyłu danych, pokryciem, spektrum i szerokością pasma (wielkością spektrum wykorzystywaną przez każdy kanał danych). Większa szerokość pasma umożliwia wyższą prędkość transmisji danych, ale wymagane jest większe spektrum, co prowadzi do zmniejszenia obszarów pokrycia. W rezultacie branża coraz bardziej kieruje się w stronę pasm 25 kHz i 50 kHz, które dają szerokie pokrycie, równoważne z TETRA1. Operator sieci może dla każdego miejsca podjąć decyzję, która szerokość kanału ma być używana, czyli TEDS oferuje dynamiczną zmianę szerokości pasma, rysunek 5.53 od standardowych 25 kHz do 150 kHz co decyduje o zasięgu i szybkości przesyłania danych, zaś na rysunku 5.54 przedstawiono ewolucję standardów TETRA w kierunku realizacji potrzeb rynku.



Rys.5.53. *Porównanie zasięgów standardówTETRA1 i TEDS*



Rys.5.54. *Ewolucja standardów TETRA*

W rozwiązaniu TEDS stosowana jest modulacja adaptacyjna dla uzyskania maksymalnej przepustowości danych. Schemat modulacji definiuje, w jaki sposób dane są przekazywane pomiędzy urządzeniem a stacją bazową. Modulacja adaptacyjna automatycznie zmienia wykorzystywany schemat modulacji w zależności od siły sygnału: schemat o wyższej przepustowości, kiedy sygnał jest dobry oraz układ wolniejszy i odporniejszy, gdy sygnał jest słaby. Zastosowanie, na przykład, przez Motorolę standardu TEDS wykorzystuje pełną adaptacyjną modulację i obsługuje wszystkie schematy modulacji QAM (4 QAM, 16 QAM oraz 64 QAM – najwyższy dostępny). Ponieważ schematy modulacyjne są wykorzystywane w takich technologiach

chociażby jak WiMax, to ten producent posiada potwierdzone doświadczenie w zakresie realizacji tych zaawansowanych technik zarówno w dziedzinie naszej infrastruktury jak i urządzeń. Często zadawane pytania to:

Jaką przepustowość danych zapewnia TEDS?

Przy założeniu szerokości kanału 50 kHz oraz schematu modulacji QAM 64 (maksymalnego dozwolonego), można teoretycznie uzyskać maksymalną przepływność IP netto 157 kb/s, ale zapewniony jest niski poziom ochrony przed błędami transmisji radiowej. Zamiast tego stosowany jest zwykle mechanizm wysokiego zabezpieczenia, mający zapewnić wysoką odporność transmisji danych, dający efektywną szybkość do 80 kbps, która jest dostępna dla aplikacji po uwzględnieniu narzutów.

Jakie aplikacje znajdują zastosowanie?

TEDS zapewnia wystarczającą szerokość pasma, by obsłużyć większość aplikacji wymaganych przez użytkowników krytycznych zastosowań, włączając w to bardziej złożone zapytania do baz danych, obrazy o większej rozdzielczości i streaming wideo. Gwarantowana jest także większa przepustowość jednoczesnego użycia danych przez wielu użytkowników współdzielących te same kanały danych oraz inteligentne mechanizmy dzielenia danych pomiędzy użytkownikami.

Takie zaawansowane aplikacje i usługi, jak jak lokalizacja pojazdów i użytkowników, wiadomości tekstowe, biuro mobilne czy pełny zakres usług pomocniczych, wykorzystują moc sieci komunikacji krytycznej dla zwiększenia skuteczności operacyjnej. Gwarantowane szerokopasmowe (wideband) transmisje danych zwiększa możliwości naszych głównych sieci, zapewniając odporność i bezpieczeństwo bezprzewodowego szerokopasmowego przesyłu danych, celem umożliwienia szerszego obszaru pokrycia i lepszego dostępu do sieci, grafiki oraz bogatszych aplikacji przetwarzania danych. Takie rozwiązania łączności krytycznej, bazujące na IP, umożliwiają rzeczywistą integrację z uzupełniającymi sieciami danych o wysokiej prędkości, dzięki czemu można wykorzystywać aplikacje wideo i multimedialne na obszarach docelowych, czyli rozwiązanie takie to:

Więcej niż głos - zapotrzebowanie na dane mobilne,

TETRA - większa skuteczność poprzez dane,

Rozszerzanie dostępu do danych krytycznych,

PROGRAM IMAGIN: Pełny wybór obrazów w terenie.

Porównanie parametrów systemów TETRA i TEDS zawiera tabela 5.4, a osiągane

Tabela 5.4. *Podstawowe parametry TETRA i TEDS.*

Parametr	TETRA	TEDS
Wielodostęp	FDMA/TDMA	
Odstęp między nośnymi	25kHz	25, 50, 100 lub 150kHz
Modulacja	π/4DQPSK π/8DQPSK	4-QAM, 16-QAM oraz 64-QAM
Kodowanie kanałowe	kod splotowy	turbo-kod
Sprawność kodowania	R=1/2 lub R=2/3	
Przepływność danych w kanale fizycznym	9 lub 13,5kb/s	od 38,4kb/s do 691,2kb/s

przepływności dla stosowanych rodzajów modulacji zawiera tabela 5.5.

Tabela 5.5. *Przepływności dla transmisji danych i obu rodzajów modulacji fazy.*

Modulacja	π/4 DQPSK			π/8 DQPSK
Kodowanie kanałowe	kod splotowy RCPC		brak	
Sprawność kodowania	R≈1/3	R≈2/3	-	
Przepływność danych	2,4kb/s	4,8kb/s	7,2kb/s	10,2 kb/s

System TETRA zyskał sobie w pełni zasłużone uznanie wśród wielu użytkowników. Dzięki jego specyficznym, cennym właściwościom, a w szczególności usługom specjalnym, jest doskonale przystosowany do roli systemu łączności dla wszelkiego rodzaju służb publicznych i firm. Publicznie dostępna specyfikacja oraz otwarty standard systemu sprawia, że jest on standardem międzynarodowym, a duża skala produkcji sprzętu do tego systemu i konkurencja między producentami przyczyniają się do znacznego obniżenia kosztów instalacji. Dużą i stale rosnącą popularność system TETRA zawdzięcza też nieustannemu rozwojowi np. TEDS który zapewnia nowe rodzaje usług, coraz większe przepływności dostępne dla użytkowników i wzrastającą jakość transmisji. To wszystko pozwala mieć nadzieję, że w niedługim czasie zostanie on wdrożony przynajmniej w służbach bezpieczeństwa publicznego.

5.6.4. Telefonia komórkowa

Telefonia komórkowa - infrastruktura telekomunikacyjna (oraz procesy związane z jej budową i eksploatacją), umożliwiająca abonentom bezprzewodowe połączenia na obszarze złożonym z tzw. komórek (ang. *cells*), obszarów

kontrolowanych przez poszczególne anteny stacji bazowych. Charakterystyczną cechą tego typu telefonii jest zapewnienie użytkownikowi mobilności, może on zestawiać połączenia (oraz połączenia mogą być zostawione do niego) na terenie pokrytym zasięgiem radiowym związanym ze wszystkimi stacjami bazowymi w danej sieci. Najpopularniejszym obecnie systemem telefonii komórkowej na świecie jest **GSM** *(Global System for Mobile Communications),* około 80% rynku telefonii mobilnej. Należy on do tzw. telefonii komórkowej drugiej generacji, która zaczyna być zastępowana przez telefonię 3G. Wśród wdrażanych obecnie systemów 3G najwięcej sieci (73%) zbudowanych jest na bazie standardu UMTS *(Universal Mobile Telecommunications System).* Konsorcjum standaryzacyjne 3rd Generation Partnership Project, które opublikowało specyfikacje systemu UMTS, pracuje obecnie nad nowym standardem - Long Term Evolution (LTE), który ma szanse stać się globalnym standardem sieci komórkowych na całym świecie.

Telefonia komórkowa pierwszej generacji - pierwsze systemy telekomunikacyjne na bazie których budowano telefonię komórkową, wykorzystywały w sieci radiowej transmisję analogową. Najpopularniejszymi standardami były NMT *(Nordic Mobile Telephone)* oraz AMPS (*Advanced Mobile Phone System*). Sieci w standardzie NMT (pierwsza sieć uruchomiona w 1981 roku) budowane były głównie w Europie. Większość wdrożeń systemów AMPS odbywała się w Ameryce Północnej. Istniała też europejska wersja tego systemu - TACS (*Total Access Communication System*) zaimplementowana w Wielkiej Brytanii i Irlandii.

Telefonia komórkowa drugiej generacji - wraz ze wzrostem liczby użytkowników sieci komórkowych używana w nich sieć radiowa stawała się coraz bardziej przeciążona. Nie można było rozwiązać tego problemu na bazie istniejących systemów analogowych. Nowe standardy sieci zaczęły wykorzystywać transmisję cyfrową co znacznie zwiększyło pojemność sieci. Sieci wykorzystujące ten rodzaj transmisji określane były jako telefonia komórkowa drugiej generacji. Do najpopularniejszych systemów należały wynaleziony w USA cdmaOne oraz bazujący na specyfikacjach Europejskiego Instytutu Norm Telekomunikacyjnych - GSM. GSM był pierwotnie projektowany jako system, który ma być zbudowany na obszarze Europejskiej Wspólnoty Gospodarczej (EWG), ale obecnie sieci w tym standardzie znajdują się na wszystkich kontynentach. Systemy drugiej generacji są obecnie najpopularniejszymi

sieciami komórkowymi, ciągle są rozbudowywane - zaimplementowano w nich na przykład przesyłanie danych na bazie komutacji pakietów (w systemach cdmaOne – specyfikacja IS-95B, w systemach GSM - technologie GPRS *(General Packet Radio Service)* i EDGE *(Enhanced Data rates for GSM Evolution*).

Telefonia komórkowa trzeciej generacji - Międzynarodowy Związek Telekomunikacyjny ITU, *(International Telecommunication Union*) na początku lat 90. rozpoczął pracę nad IMT-2000 - wspólną platformą, na której miały być oparte systemy 3G. Nie były to specyfikacje konkretnego systemu, ale zbiór wymagań, które pozwalały ujednolicić usługi oferowane przez różne standardy oraz umożliwić współpracę pomiędzy różnymi systemami. Obecnie najpopularniejszymi standardami zaaprobowanymi przez ITU jako systemy opisywane przez IMT-2000 są UMTS *(Universal Mobile Telecommunications System)* i systemy z rodziny CDMA2000.

Telefonia komórkowa czwartej generacji - Nazwa „4G" nie jest formalnym terminem wykorzystywanym w oficjalnych dokumentach opisujących standardy telekomunikacyjne, niemniej jest ona często używana jako określenie systemów, których specyfikacje opisują przesyłanie danych z przepływnością większą niż ta oferowana przez obecne systemy 3G. Najczęściej określa się tak systemy oparte na standardach WiMAX i Long Term Evolution. **LTE** jest zdecydowanie częściej wybierany przez operatorów jako przyszły element ewolucji, której podlegają zarządzane przez nich sieci i ma szanse stać się przyszłym globalnym standardem telefonii komórkowej.

Na koniec 2010 roku penetracja rynku telefonii komórkowej w Polsce wyniosła 123%, co oznacza, że w kraju jest ok. 47 milionów numerów telefonii mobilnej. Wartość rynku telekomunikacyjnego (mierzona wielkością przychodów ze sprzedaży) wyniosła ponad 42,8 mld zł. i była o prawie 2% wyższa w porównaniu z rokiem 2009.

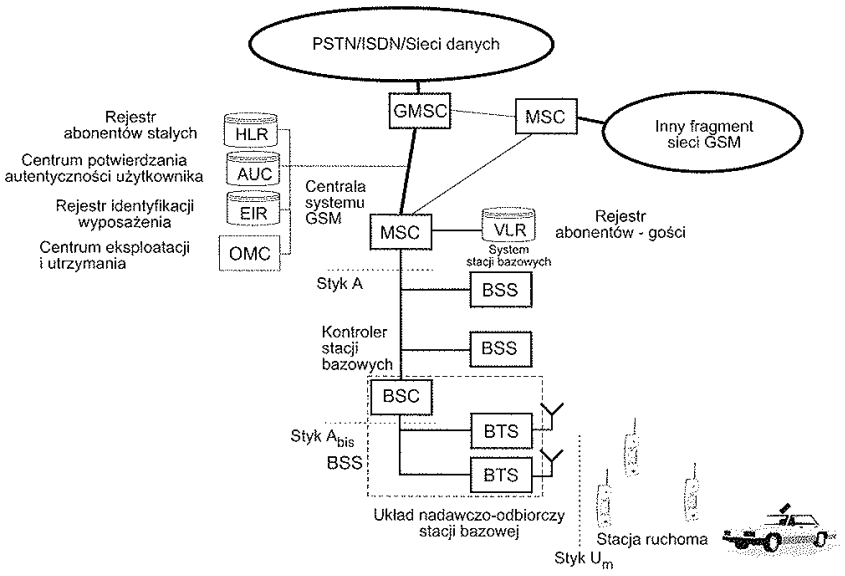
Standardy GSM. Istnieje pięć głównych standardów GSM, różniących się przede wszystkim używanym pasmem radiowym i rozmiarami komórek: GSM 400, GSM 850, GSM 900, GSM-1800 (nazywany także DCS), i GSM 1900 (nazywany także PCS). GSM 850 i GSM 1900 wykorzystywane są w większości państw Ameryki Północnej i Południowej. W pozostałej części świata, używany jest standard GSM 900/1800. GSM 400 jest rozwiązaniem dla operatorów posiadających sieci NMT 450, którzy są

już posiadaczami prawa do używania wykorzystywanych przez ten system częstotliwości, a w okresie przejściowym oba systemy mogą działać razem. Jest też technologią, którą można zastosować do pokrycia dużych niezamieszkanych obszarów.

Cecha \ System	GSM 400	GSM 850	GSM 900	GSM 1800	GSM 1900
Uplink [MHz]	450.4 - 457.6 lub 478.8 - 486	824 - 849	880 - 915	1710 - 1785	1850 - 1910
Downlink [MHz]	460.4 - 467.6 lub 488.8 - 496	869 - 894	925 - 960	1805 - 1880	1930 - 1990
Liczba częstotliwości	35	124	174	374	299

Architektura systemu GSM - sieć GSM to zespół elementów współpracujących ze sobą w celu świadczenia usług telekomunikacyjnych dla abonentów mobilnych (ruchomych). Elementy sieciowe komunikują się ze sobą za pomocą określonych interfejsów, rysunek 5.55.

Obszar działania systemu jest podzielony na fragmenty zarządzane przez centrale radiokomunikacyjne **MSC** *(Mobile Switching Centre).* Są to specjalizowane centrale elektroniczne z dołączonymi blokami , które pełnią funkcje właściwe radiokomunikacji ruchomej. Do centrali dołączona jest baza danych określana jako **VLR** – *(Visitor's Location Register), rejestr stacji obcych.* Jest to rejestr stacji ruchomych chwilowo przebywających w obszarze obsługiwanym przez daną centralę radiową. Oprócz tej bazy system zarządzany przez konkretnego operatora ma jeszcze trzy inne bazy danych: **HLR** – *(Home Location Register),rejestr stacji własnych.* Jest to rejestr stacji ruchomych na stałe zarejestrowanych w systemie zarządzanym przez danego operatora;

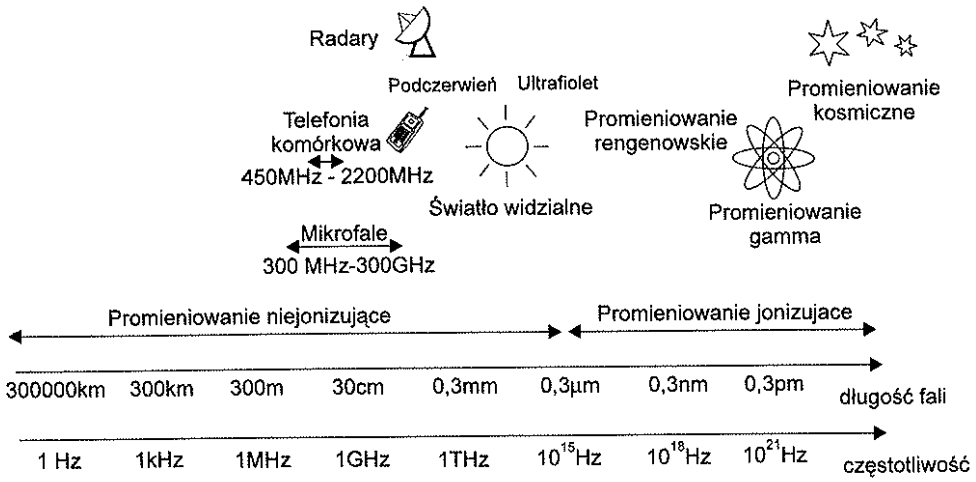


Rys.5.55. *Ogólna architektura systemu GSM*

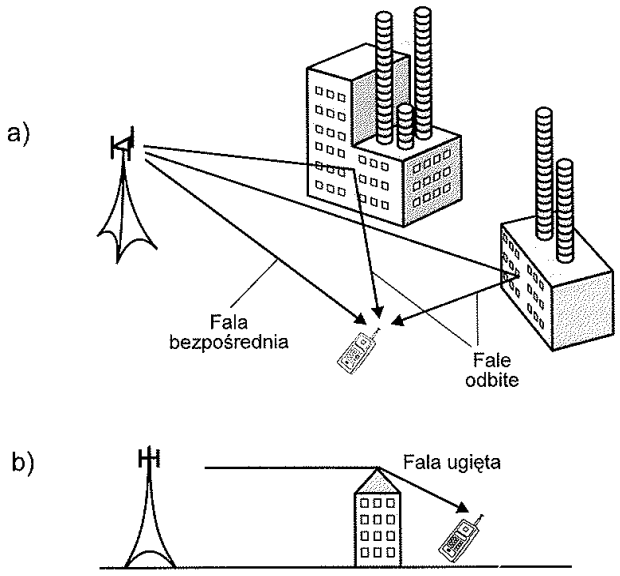
AUC – *(Autentication Centre), centrum identyfikacji.* Jest to baza danych służąca do sprawdzania, czy abonent posiadający indywidualną kartę identyfikacyjną **SIM –** *(Subscriber Identity Module)* jest dopuszczony do realizacji połączenia; **EIR** – *(Equipent Idetification Register), rejestr identyfikacji wyposażenia.* Jest to baza danych z informacjami dotyczącymi numerów seryjnych używanych stacji mobilnych, telefony skradzione lub zagubione są na „czarnej liście" i nie mogą być wykorzystane. Centrale **MSC** obsługujące przydzielone im obszary połączone są między sobą poprzez centralę wejściową **GMSC** *(Gateway Mobile Switching Centre)* z publiczną komutowaną siecią telefoniczną PSTN, siecią ISDN oraz ewentualnie innymi sieciami np. transmisji danych. Każda centrala MSC zarządza co najmniej jednym systemem stacji bazowych **BSS** – *(Base Station System),* w skład którego wchodzą sterownik (kontroler) stacji bazowych **BSC** – *(Base Station Controller)* oraz kilka transciverów (urządzeń nadawczo – odbiorczych) stacji bazowych **BTS** – *(Base Transceiver Station)* wraz z układami realizującymi podstawowe funkcje sterujące na poziomie pojedynczego transceivera. Te transceivery w uproszczeniu nazywa się stacjami bazowymi **BS.** Są one rozmieszczone w środkach komórek pokrywającymi obszar działania systemu. W każdej komórce może znajdować się pewna liczba stacji ruchomych **MS** – (Mobile Station), z którymi nawiązywana jest łączność. Centrum eksploatacji i utrzymania **OMC** – *(Operational and Maintenance Center),* nadzoruje działanie poszczególnych elementów systemu GSM. Jest ono połączone z wszystkimi elementami części komutacyjnej systemu GSM i wykonuje funkcje administracyjne,

takie jak taryfikacja, monitorowanie ruchu telekomunikacyjnego, zarządzanie w przypadku uszkodzeń elementów sieci a zwłaszcza zarządzanie rejestrem HLR.

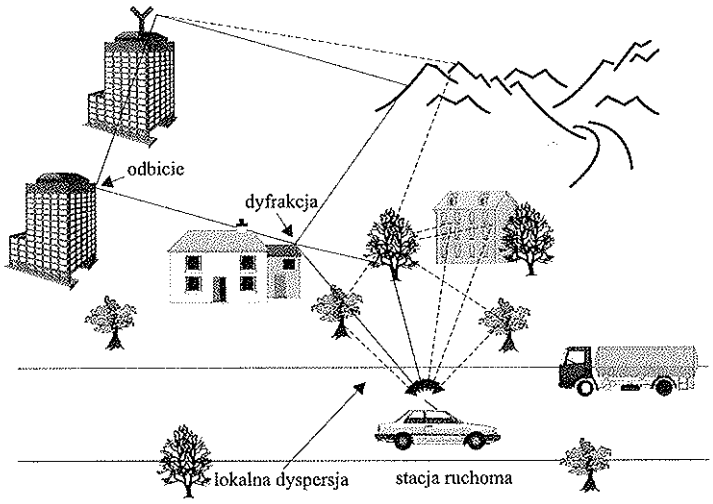
Położenie zakresów częstotliwości wykorzystywanych przez systemy komórkowe, na tle pełnego spektrum częstotliwości przedstawia rysunek 5.56 a typowe zjawiska propagacyjne występujące rzeczywistych kanałach radiowych przedstawiają rysunki 5.57 (warunki stworzone przez działania ludzkie) i 5.58 (warunki „naturalne").



Rys.5.56. *Widmo fal radiowych*

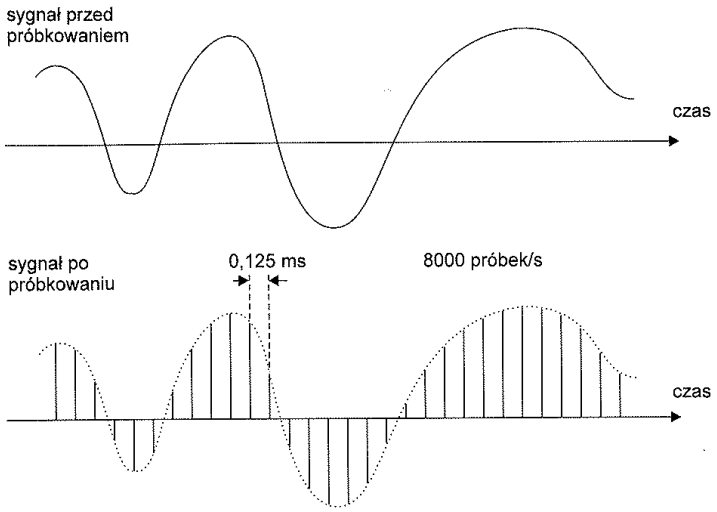


Rys.5.57. *Typowe zjawiska propagacyjne występujące w rzeczywistych kanałach radiowych a) transmisja wielodrogowa b) uginanie się fal na przeszkodach.*



Rys.5.58. *Przykłady propagacji sygnału w systemie radiokomunikacji ruchomej*

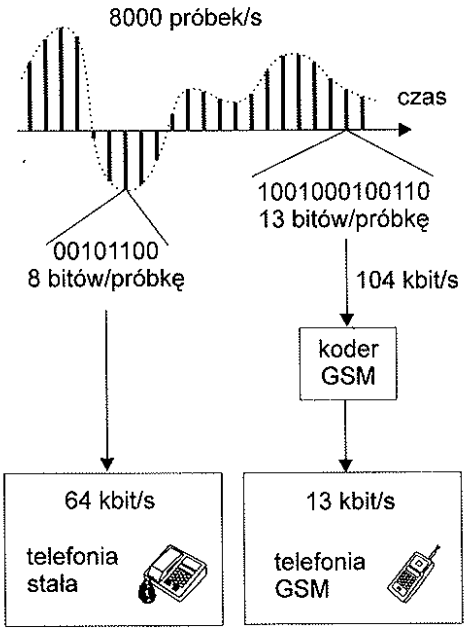
System GSM jest systemem cyfrowym, czyli pracuje w oparciu o sygnały cyfrowe a sygnał mowy jest sygnałem analogowym. Aby przekształcić sygnał analogowy na sygnał cyfrowy musimy, podobnie jak to było w omawianym w punkcie 3.3 systemie ISDN, próbkowaniu, rysunek 5.59.



Rys.5.59. *Zasada próbkowania sygnału mowy*

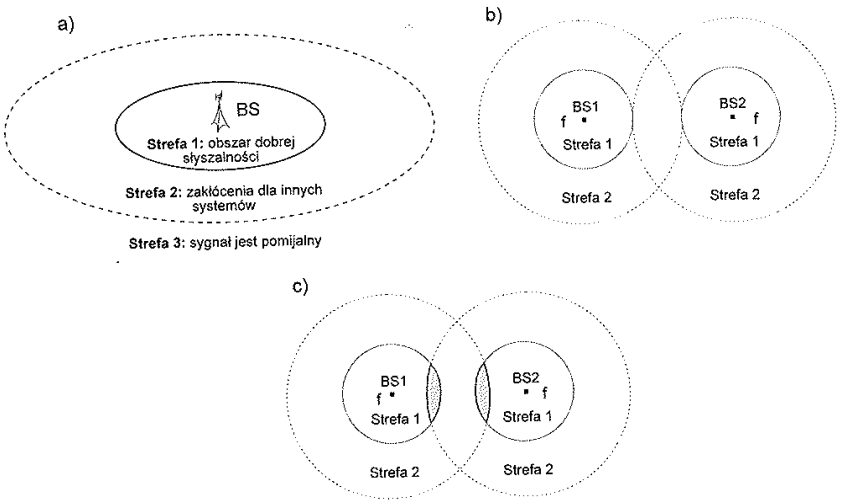
Sposób kodowania stosowany w systemie ISDN to 8000 próbek sygnału w każdej sekundzie kodowane ośmioma bitami, czyli 8000 x 8 daje przepływność binarną 64 kb/s. Ponieważ kanały radiowe są gorszej jakości niż łącza przewodowe to nie są w stanie przenieść takiej dużej przepływności. Poza tym, im większa przepływność strumienia binarnego tym droższe jest przesłanie sygnału. W związku z tym

w standardzie GSM stosujemy dwuetapowe kodowanie. Wartość próbki zapisujemy 13 bitami co daje przepływność 104 kb/s a następnie w układzie specjalnego **kodera GSM** kodujemy drugi raz aby osiągnąć przepływność możliwą do przeniesienia przez kanał radiowy czyli zaledwie 13 kb/s (rysunek 5.60).



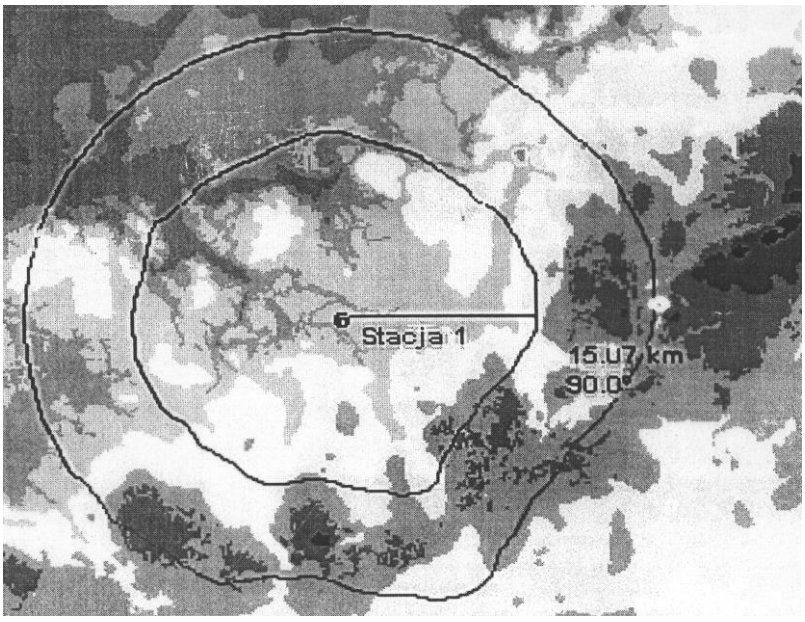
Rys.5.60. *Zamiana próbek sygnału na ciąg bitów*

Bardzo ważnym problemem jest poprawne rozmieszczenie stacji bazowych w terenie. Wokół każdej stacji bazowej (nadajnika) mamy trzy strefy: strefa 1 - obszar dobrej słyszalności, strefa 2 - w której występują zakłócenia dla innych systemów radiowych i strefa 3 w której sygnał zakłócający jest pomijalnie mały czyli możemy wykorzystać tą samą częstotliwość (rysunek 5.74). Problem ten (właściwe rozmieszczenie nadajników) dotyczy wszystkich systemów radiokomunikacyjnych a nie tylko telefonii komórkowej. Czyli musimy tak planować rozmieszczenie nadajników aby **strefa zakłócająca jednego nadajnika (stacji bazowej) nie wchodziła w strefę dobrej słyszalności innej stacji.**

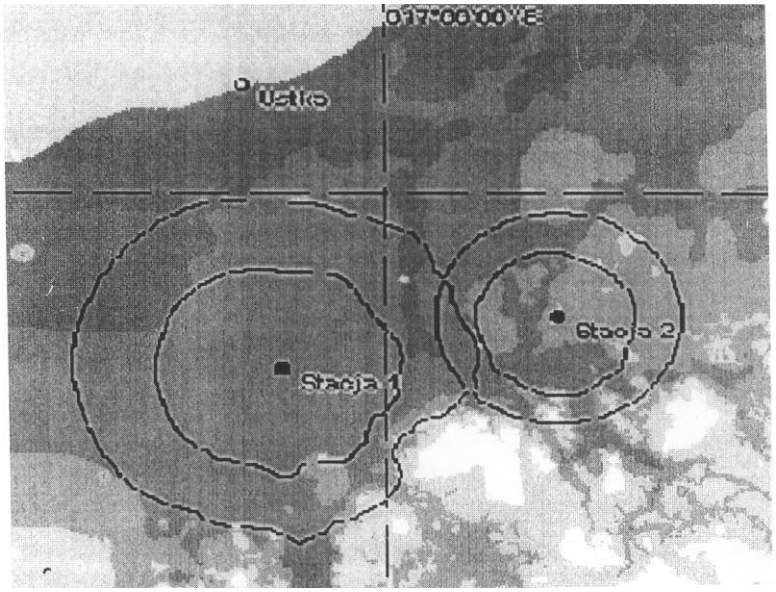


Rys.5.61. *Strefy wokół nadajnika radiowego; a) podział b) poprawne wykorzystanie tej samej częstotliwości w różnych kanałach c) nieprawidłowe konfigurowanie komórek*

W praktyce strefy nie są okręgami lecz są pewnymi zamkniętymi liniami krzywymi, zależnymi od ukształtowania terenu, obszarami (rysunki 5.75 i 5.76 obraz z rzeczywistych pomiarów).

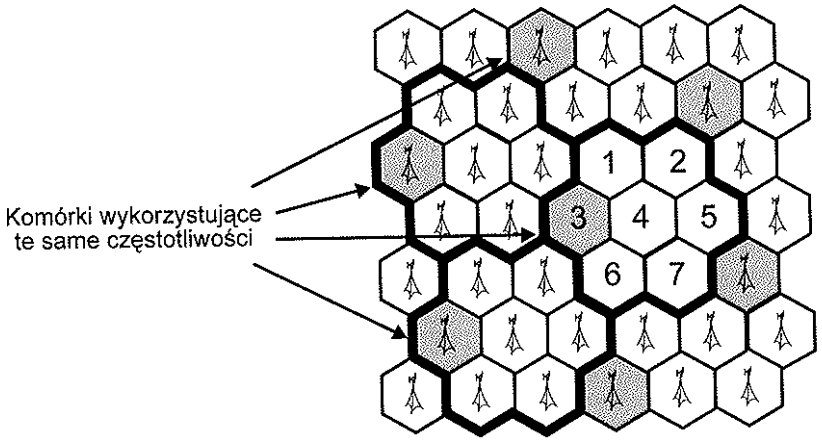


Rys.5.62. *Strefy wokół BS dla pojedynczej komórki*



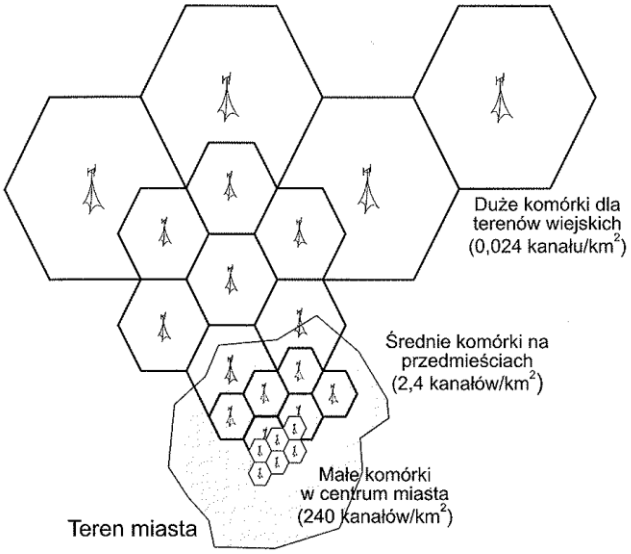
Rys.5.63. *Strefy dla przypadku dwóch komórek*

Idea systemu komórkowego polega więc na podzieleniu całego obszaru na mniejsze fragmenty, tzw. komórki, z których każdy wyposażony jest w nadajnik stacji bazowej o stosunkowo niewielkiej mocy. Pozwala na wykorzystanie tej samej częstotliwości w wielu komórkach (rysunek 5.64).



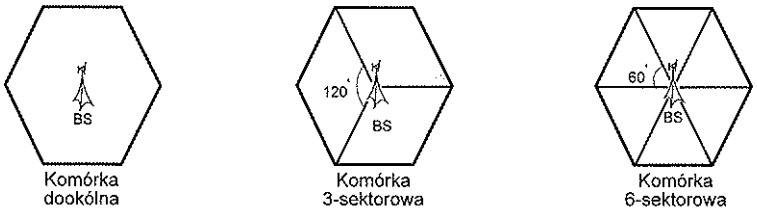
Rys.5.64. *Regularna struktura komórkowa wykorzystująca komórki tej samej wielkości (przyjmuje się współczynnik ponownego wykorzystania tej samej częstotliwości równy 1/7)*

Ze względu na zapotrzebowanie na usługi telekomunikacyjne komórki systemu mają różną wielkość. Na terenach wiejskich o niedużym ruch będą one dużo większe niż komórki w centrum dużego miasta gdzie generowany jest dużo większy ruch (rysunek 5.65).



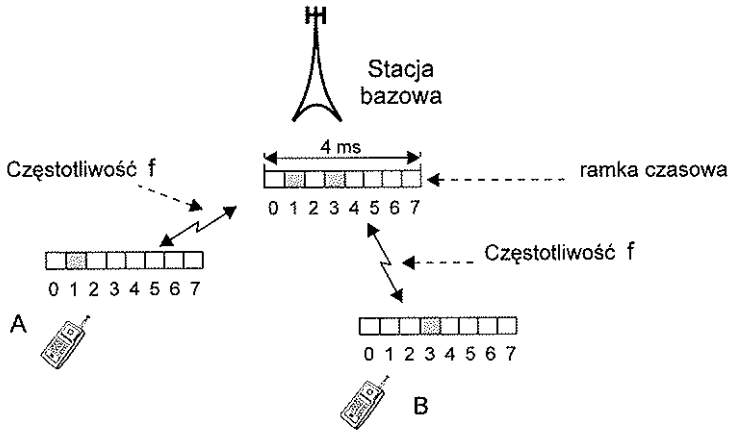
Rys.5.65. *Praktyczna struktura sieci komórkowej odzwierciadlająca zróżnicowane zapotrzebowanie na usługi telekomunikacyjne*

Pamiętać jednak trzeba, że procedura podziału komórek na mniejsze ograniczona jest wysokim kosztem wynikającym z instalacji dużej liczby stacji bazowych, poziomem zakłóceń współkanałowych , które w praktycznych systemach zwiększają się w miarę zagęszczania komórek. Planowanie więc, systemu komórkowego jest zadaniem trudnym i złożonym polegającym na znalezieniu kompromisu pomiędzy: kosztem systemu, jego pojemnością, wielkością obszaru objętego zasięgiem systemu oraz jakością usług. Innym sposobem na zwiększenie pojemności sytemu jest sektoryzacja komórek (inny sposób zmniejszania rozmiarów komórek , w którym maleje obszar obsługiwany przez komórkę, ale nie zmienia się maksymalna odległość stacji bazowej od stacji ruchomej. W porównaniu z poprzednim (stosowanie mniejszych komórek) z antenami dookólnymi mniejsza jest liczba masztów antenowych, znacząco zmniejsza koszty infrastruktury (rysunek 5.66).



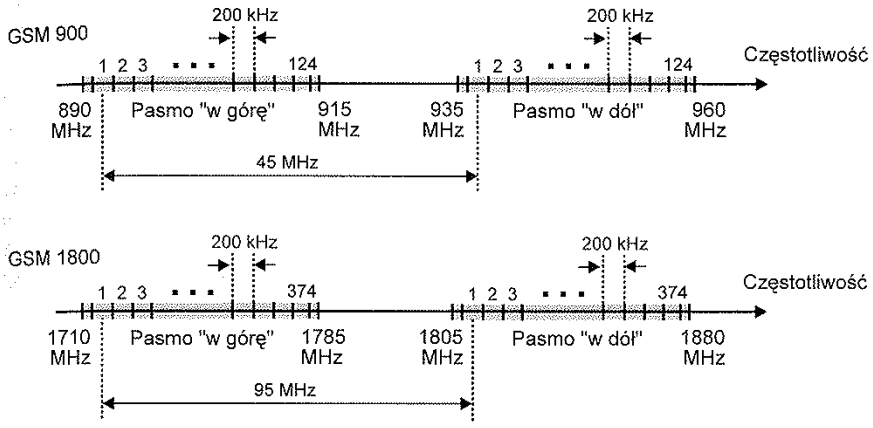
Rys.5.66. *Komórka dookólna oraz komórki sektorowe*

Jeszcze innym sposobem powiększenia pojemności systemu jest wtórne zwielokrotnienie każdego kanału częstotliwościowego ośmiokrotnie zwielokrotnieniem czasowym (rys.5.67).



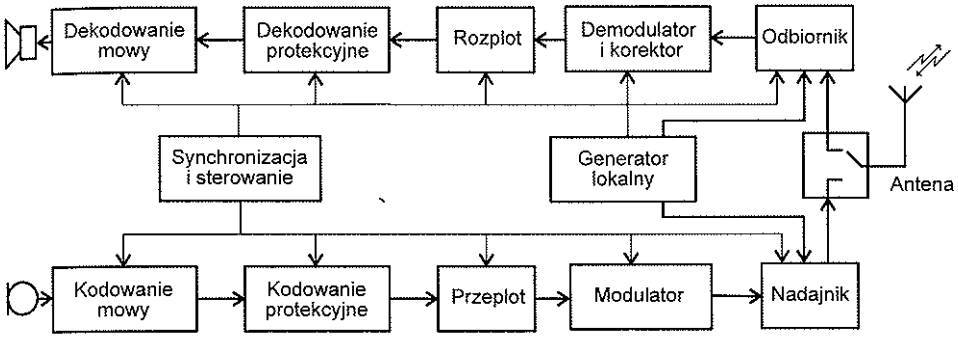
Rys.5.67. *Transmisja na jednej częstotliwości sygnałów generowanych przez różnych użytkowników*

Znormalizowane pasma częstotliwości wykorzystywane w sieciach GSM przedstawia rysunek 5.68.



Rys.5.68. *Pasma częstotliwości wykorzystywane w sieciach GSM*

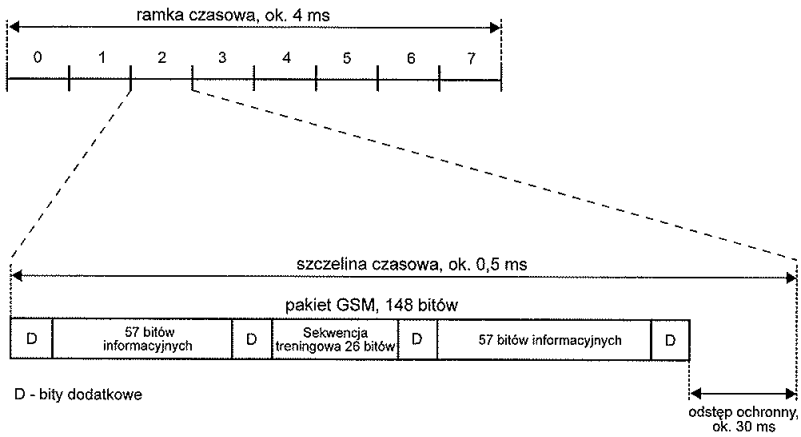
Schemat funkcjonalny typowego telefonu komórkowego przedstawia rysunek 5.69. Z tego rysunku wynika, że telefon komórkowy składa się standartowego nadajnika radiowego (patrz punkt 5.3) i superheterodynowego odbiornika radiowego (patrz punkt 5.4) zamkniętych w jednej obudowie.



Rys.5.69. *Schemat funkcjonalny telefonu komórkowego GSM*

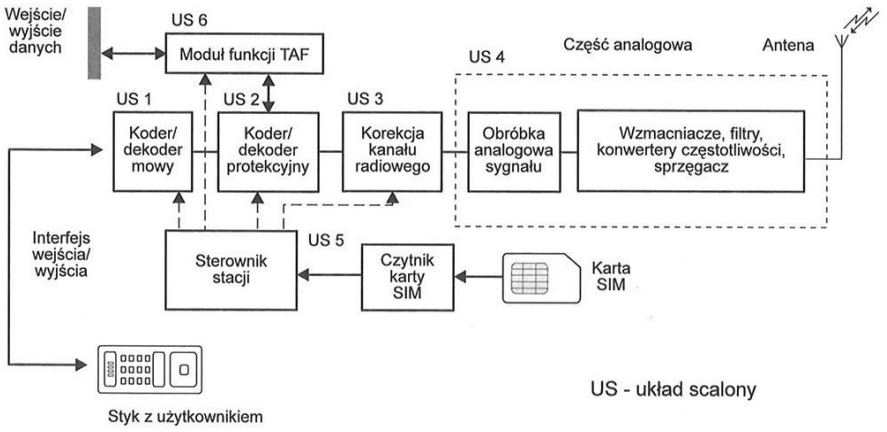
Istotnym elementem w torze odbiorczym jest blok demodulatora i korektora. O ile rola demodulatora jest oczywista to element zwany korektorem jest pewnym nowum w torze odbiorczym. Na podstawie przesyłanej z nadajnika tak zwanej sekwencji treningowej (rys.5.70) odbiornik ma prognozę stanu kanału radiowego na najbliższe 0,5 ms i stosownie do tej prognozy „ustawia" parametry toru odbiorczego.

Schemat elektryczny telefonu komórkowego przedstawia rysunek 5.71. Jak widać telefon komórkowy składa się z kilku układów scalonych (US 1 do US 6). Nie oznacza to, że nie można by było zbudować telefonu komórkowego w oparciu o jeden układ scalony bardzo dużej skali integracji – VLSI. Nie praktykuje się takiego rozwiązania, gdyż wtedy tak zwana „podatność naprawcza" byłaby bardzo mała (nie opłacałoby się naprawiać takiego telefonu).



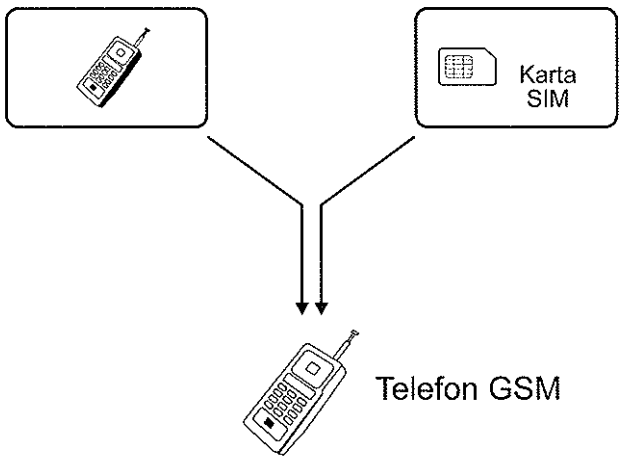
Rys.5.70. *Struktura pakietu przesyłanego w kanale radiowym*

W praktyce więc obecnie budowane telefony komórkowe, aby poprawić wspomnianą podatność naprawczą, złożone są z wspomnianych kilku układów scalonych a ich ilość zależy od konkretnego modelu telefonu.



Rys.5.71. *Uproszczony schemat elektryczny przykładowego telefonu komórkowego*

W standardzie GSM stacja ruchoma (telefon komórkowy) podzielona została na dwie części. Część pierwsza zawiera wszystkie funkcje sprzętowe oraz oprogramowanie związane z transmisja sygnałów w kanale radiowym, współpracą telefonu komórkowego z urządzeniami zewnętrznymi rysunek 5.72. Część druga jest zawiera dane identyfikujące użytkownika. Część pierwsza jest więc kompletnym telefonem systemu GSM, który jednak wymaga do swojej pracy „klucz" związanego z użytkującym go abonentem. Tym kluczem jest karta identyfikująca abonenta zwana kartą **SIM** *(Subsciber Identity Module)*. Oddzielenia karty SIM od pozostałych funkcji telefonu komórkowego daje nam wiele korzyści, pozwala na wymianę telefonu na inny bardziej nowoczesny, umożliwia wypożyczanie telefonów oraz świadczenia usług przedpłaconych (prepaid).



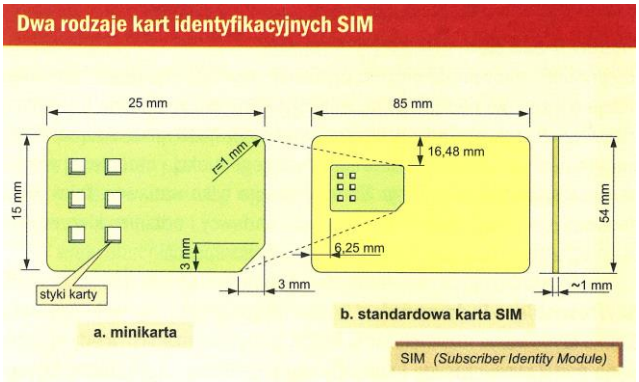
Rys.5.72. *Telefon GSM a karta SIM*

Zadania karty SIM opisuje poniższa tabela.

Parametry karty identyfikacyjnej SIM

Właściwości	Parametry i usługi
Funkcje użytkowe	● identyfikacja abonenta ● przechowywanie informacji używanych przez operatora ● generowanie klucza szyfrującego informacje wysyłane w kanał radiowy ● przechowywanie bieżących informacji definiowanych przez użytkownika ● pamiętanie krótkich wiadomości SMS (*Short Message System*)
Pamięć danych	● międzynarodowy numer abonenta ruchomego IMSI (*International Mobile Subsciber Identity*) ● tymczasowy numer abonenta ruchomego TMSI (*Temporary MSI*) ● numer obszaru przywołań LAI (*Local Area Identity*) ● uprawnienia abonenta do usług ● kod dostępu PIN (*Personal Identity Number*) ● kod odblokowujący PUK (*Personal Unblocking Key*) ● klucz identyfikacyjny Ki ● algorytmy szyfrujące dla procedur kryptograficznych (A3, A8) ● indeksowana lista numerów skróconych ● krótkie wiadomości tekstowe SMS odebrane pod nieobecność abonenta ● preferencje abonenta co do wyboru sieci GSM
Tryby dostępu do karty	● NEVER - zabronienie użytkownikowi wykonania operacji ● ALWAYS - zezwolenie na operacje przez użytkownika ● ADM - administracyjny dostęp do karty przez operatora systemu ● PIN-PUK - ochrona zawartości karty ● PIN2-PUK2 - nowy typ ochrony karty (GSM faza 2)
Funkcje dodatkowe (faza 2)	● wybór języka komunikatów prezentowanych na ekranie ● nowy poziom zabezpieczeń (PIN 2) ● przechowywanie informacji sterujących nowymi usługami dodatkowymi ● rozszerzenie kontroli krótkich wiadomości SMS ● rozszerzenie pamięci dla książki telefonicznej
Wymiary	● 85x54x1 [mm] dla karty standardowej ● 25x16x1 [mm] dla minikarty

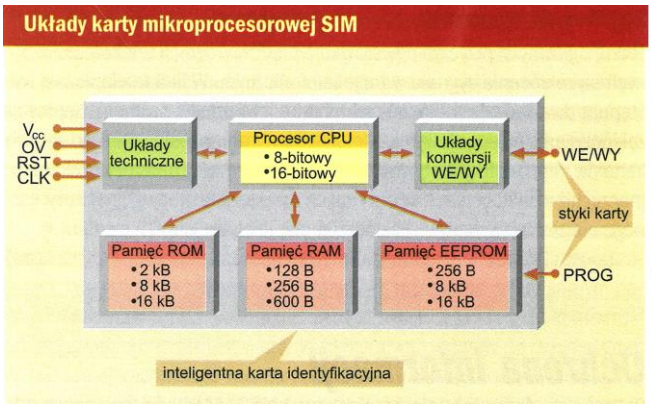
Występują dwa typy kart SIM mini karta i karta standardowa o wymiarach typowej karty bankomatowej (rysunek 5.73). Układy karty SIM przedstawia rysunek 5.74. Moduł SIM składa się z procesora CPU, układów technicznych (zasilanie), układów konwersji WE/WY



Rys.5.73. *Rodzaje kart SIM*

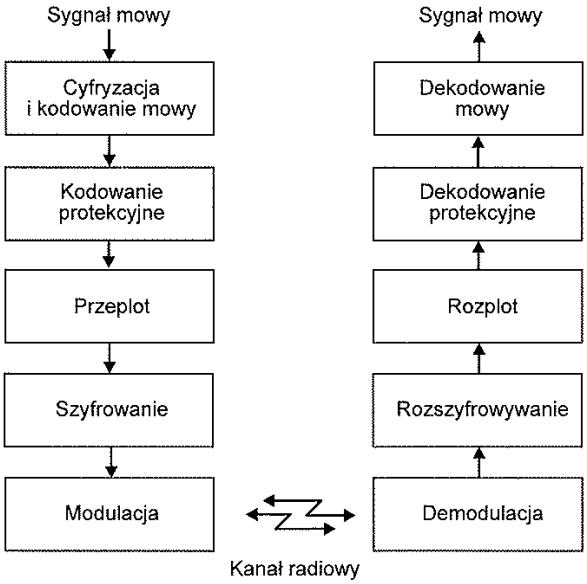
oraz trzech pamięci: ROM *(Read Only Memory) - tylko do odczytu,* RAM *(Random Acces Memory) - pamięć o dostępie swobodnym,* EEPROM *(Electrically-Erasable Programmable Read-Only Memory*) - *programowalna pamięć nieulotna.* Pamięci wykorzystywane są do realizacji głównych zadań modułu: przechowywania zapisanych

przez operatora tajnych parametrów i haseł wykorzystywanych w procedurach związanych z zabezpieczaniem systemu przed nadużyciami, przechowywanie informacji bieżących wprowadzanych przez użytkownika oraz przychodzących do niego krótkich wiadomości.



Rys.5.74. *Układy modułu SIM*

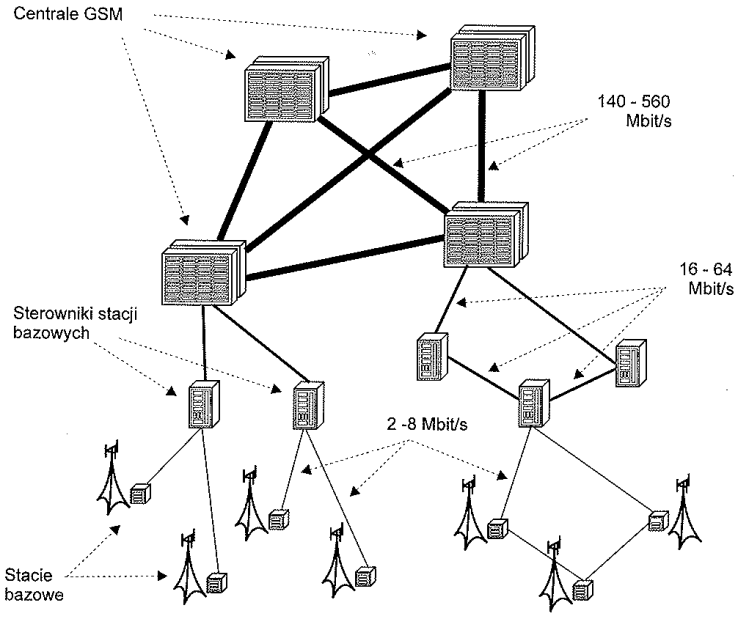
Etapy obróbki sygnału mowy w telefonie komórkowym przedstawia rysunek 5.75. Głównym zadaniem nadajnika jest zamiana sygnału informacyjnego pochodzącego od użytkownika (najczęściej jest sygnał mowy, czasem sygnał danych) na postać dogodną do wysłania w kanał radiowy. Cyfryzacja i kodowanie mowy zamienia sygnał analogowy generowany w mikrofonie na sygnał cyfrowy o przepływności 13 kb/s możliwy do przesłania w kanale radiowym. Kodowanie protekcyjne uzupełnia ucyfrowione fragmenty frazy sygnału



Rys.5.75. *Etapy obróbki sygnału mowy w telefonie komórkowym*

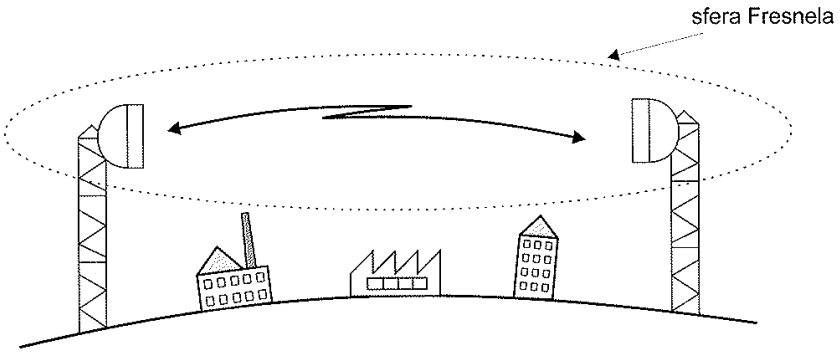
mowy o pewne bity nadmiarowe, wypracowywane wg określonej reguły (np. kody Reeda – Salomona) pozwalające stwierdzić czy w trakcie transmisji wystąpiły błędy i zasygnalizowanie tego faktu, kodowanie detekcyjne lub wykrywanie i korygowanie błędu, kodowanie korekcyjne. Przeplot zabezpiecza przed zanikami w kanale radiowym. Polega to na wprowadzaniu po stronie nadawczej do pamięci nadawczej (bufora) fragmentów ucyfrowionej frazy sygnału mowy wierszami a wyprowadzanie do nadajnika kolumnami. Po stronie odbiorczej do odpowiedniej pamięci odbiorczej wprowadzamy kolumnami a wyprowadzany wierszami. Ten zabieg powoduje, że krótkotrwałe zaniki nie „wytną" fragmentu frazy a spowodują w nich pojedyncze błędy z którymi poradzi sobie kodowanie protekcyjne. Szyfrowanie zabezpiecza przed podsłuchem przesyłanych w kanale radiowym informacji.

Pamiętać należy, że na drodze radiowej realizowane jest tylko połączenie stacja mobilna i najbliższa stacja bazowa. Stacjonarna część sytemu zbudowana jest w oparciu o system telekomunikacyjny Państwa wykorzystujący łącza przewodowe a gdy tych brakuje poprzez dedykowane łącza radioliniowe o stosownych przepływnościach (rysunek 5.76).



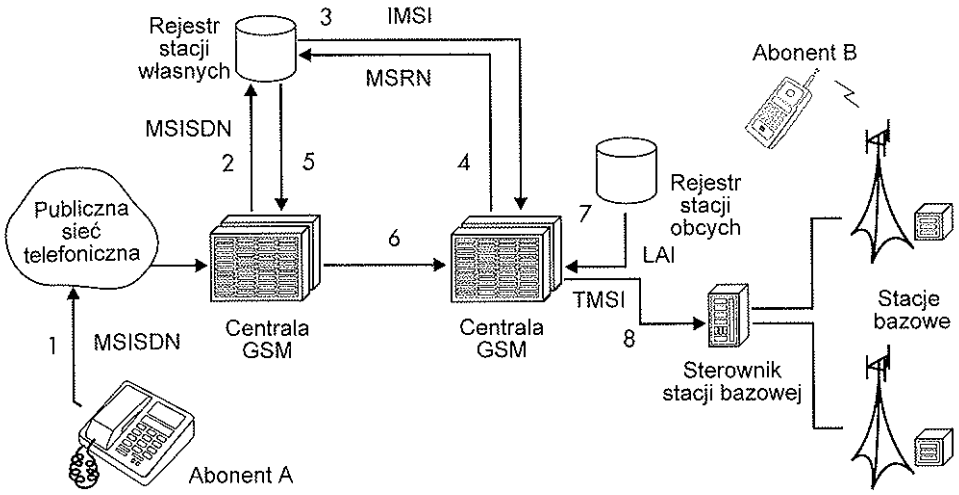
Rys.5.76. *Uproszczony schemat sieci telefonii komórkowej z zaznaczonymi przepływnościami łączy stałych*

W przypadku uzupełniania systemu radioliniami pojawia się nowy trudny problem projektowania horyzontowych linii radiowych. Rozmieszczając stacje radioliniowe w terenie musimy uwzględniać krzywiznę Ziemi i przeszkody pomiędzy antenami stacji radioliniowych (anteny muszą się „widzieć") oraz zasięgi tych stacji. Praktycznie sprowadza się to do określenia tzw. strefy Fresnela (rys.5.77) i sporządzenie bilansu łącza.



Rys.5.77. *Przykładowy przekrój terenu odpowiadający projektowanej linii radiowej*

System numeracji stosowany w standardzie GSM jest skomplikowany i trudny do omówienia dla przeciętnego użytkownika systemu. Aby wyjaśnić problem na rysunku 5.78 pokazano przykładową sekwencję kroków w procedurze zestawiania połączenia, w trakcie której wykorzystywane jest kilka różnych numerów związanych z tym samym abonentem.

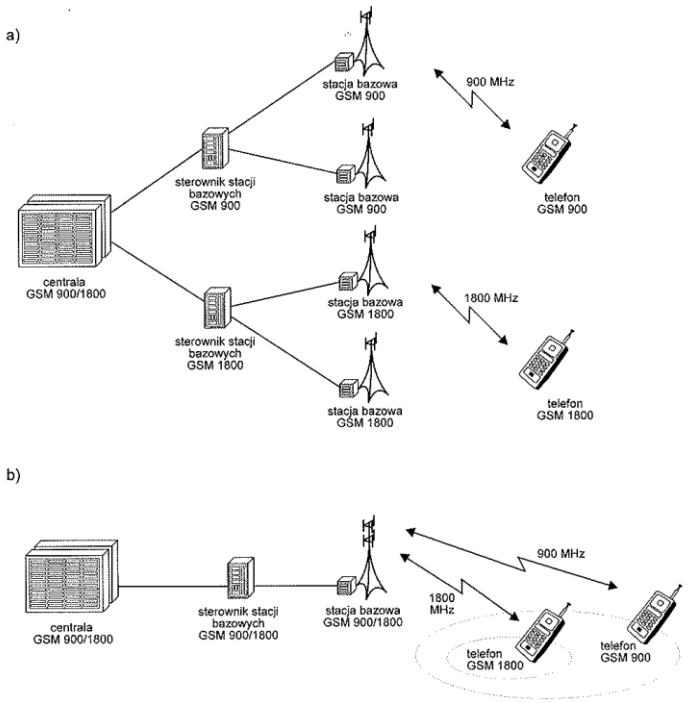


Rys.5.78. *Przykładowa procedura zestawiania połączenia w systemie GSM*

W pierwszym kroku abonent A w sieci stacjonarnej wybiera na klawiaturze aparatu telefonicznego numer katalogowy MSISDN *(Mobile Station International ISDN Number - międzynarodowy numer abonenta sieci komórkowej wg standardu ISDN)* abonenta B sieci GSM. Jest to jedyny numer abonenta B znany abonentowi A (także jedyny numer podany abonentowi B przez operatora sieci). Numer katalogowy MSISDN zostaje następnie zamieniony w rejestrze stacji własnych na odpowiadający mu wewnętrzny numer IMSI *(International Mobile Subscriber Identity - międzynarodowy numer abonenta sieci komórkowej)* będący w pewnym sensie odpowiednikiem numeru sprzętowego w telefonii stacjonarnej z tym, że nie podaje on informacji co do aktualnego położenia abonenta (krok 2). Na podstawie adresu przechowywanego w rejestrze stacji własnych, numer IMSI zostaje w kroku 3 przesłany do centrali, na której obszarze aktualnie znajduje się abonent B, gdzie zostaje wygenerowany numer MSRN *(Mobile Station Roaming Number - chwilowy numer telefonu komórkowego)* zawierający informacje potrzebne do zestawienia drogi połączeniowej (kroki 4 i 5). W kroku 6 zostaje utworzona droga połączeniowa, a w kroku 7 z rejestru stacji obcych centrali GSM pobierany jest identyfikator obszaru przywoławczego LAI *(Local Area Identity - numer obszaru przywołań)*. Następnie abonentowi B nadawany jest tymczasowy identyfikator TMSI *(Temporary Mobile Subscriber Identity - tymczasowy numer abonenta ruchomego),* którym system będzie się odtąd posługiwał się w trakcie trwania połączenia. W wyniku tego, nawet gdyby ktoś niepowołany zdołał przechwycić informacje sygnalizacyjne przesyłane w komórce GSM nie mógłby on zidentyfikować abonenta B uczestniczącego w rozmowie. W tym momencie pozostaje już tylko rozpocząć wymianę informacji rozmownych (krok 8).

Jeśli w tym przykładzie występowała procedura identyfikacji abonenta, na przykład w przypadku, gdy abonent sieci GSM inicjuje połączenie wtedy będziemy mieli do czynienia dodatkowo ze ściśle poufnym identyfikatorem użytkownika, przechowywanym jedynie w centrum identyfikacyjnym jego macierzystej sieci oraz na jego karcie SIM, a także z hasłem będącym chwilową wersją tego parametru dopuszczoną do przesyłania w sieci. Pamiętać trzeba również, że każdy telefon komórkowy posiada swój własny identyfikator (numer) sprzętowy IMEI *(International Mobile Equipment Identity - międzynarodowy numer identyfikacyjny telefonu komórkowego).*

Obecnie eksploatowane systemy telefonii komórkowej są systemami zintegrowanymi to znaczy pracują w tzw. roamingu wewnętrznym zarówno paśmie 900 MHz jak i 1800 MHz. Abonent nie wie czy aktualnie prowadzona rozmowa odbywa się w systemie GSM 900 czy w systemie DCS *(Digital Cellurar System)* obecnie nazywanym GSM 1800. Budowa zintegrowanych „dwupasmowych" sieci znacząco obniża koszty infrastruktury sieci (wiele elementów wspólnych). Taką integrację można zrealizować dwoma sposobami; integracja na poziomie central GSM i integracja na poziomie stacji bazowych (rysunek 5.79).



Rys.5.79. *Realizacja zintegrowanych sieci GSM 900/1800;*
a) integracja na poziomie central GSM
b) integracja na poziomie stacji bazowych

W tabeli 5.6 przedstawiono podstawowe różnice pomiędzy dwoma najpopularniejszymi systemami telefonii komórkowej GSM 900 i DCS 1800.

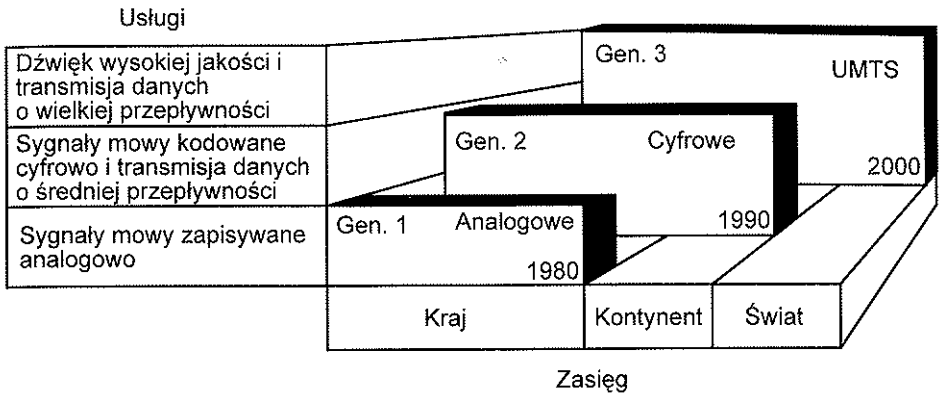
Tabela 5.6. Zasadnicze różnice między systemami GSM i DCS 1800

Cecha	GSM	DCS1800
Zakres częstotliwości: „w górę" (MS → BS) „w dół" (BS → MS)	 890 ÷ 915 MHz 935 ÷ 960 MHz	 1710 ÷ 1785 MHz 1805 ÷ 1880 MHz
Liczba kanałów dupleksowych	992 (FR) 1984 (HR)	2976 (FR) 5952 (HR)
Liczba częstotliwości nośnych	124	374
Odstęp częstotliwości między kierunkami transmisji	45 MHz	95 MHz
Maksymalna moc stacji BS	320 W (55 dBm)	20 W (43 dBm)
Maksymalna moc stacji MS	8 W (39 dBm)	1 W (30 dBm)
Minimalna moc stacji MS	0,02 W (13 dBm)	0,0025 W (4 dBm)
Klasy stacji ruchomych MS	20 W (nie realizowana) 8 W (telefon sam./przenośny) 5 W (j.w.) 2 W (tel. ręczny) 0,8 W (tel. ręczny)	1 W (tel. ręczny) 0,25 W (tel. ręczny)
Maksymalna szybkość pojazdu	250 km/h	130 km/h

Objaśnienia: FR — kodowanie mowy z pełną szybkością, HR — kodowanie mowy z szybkością połówkową

Jak widać z powyższej tabeli w systemie DCS mamy około trzykrotnie większą liczbę nośnych, tak więc znacznie wzrasta liczba dostępnych kanałów ale mamy dwukrotny spadek dopuszczalnej prędkości pojazdu.

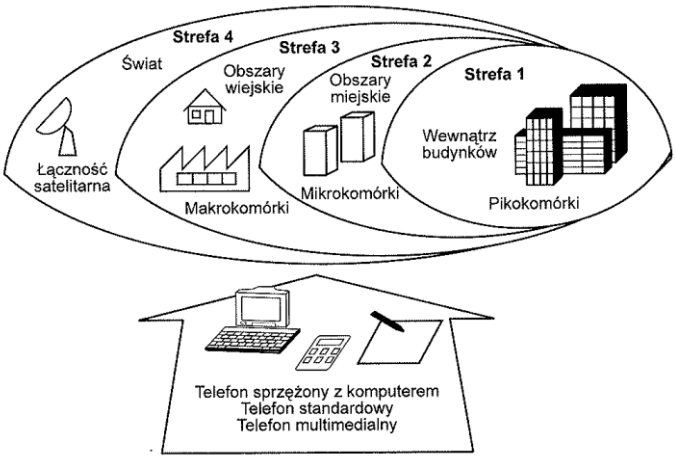
Zakres usług i obszar działania kolejnych generacji telefonii komórkowej przedstawia rysunek 5.80.



Rys.5.80. *Zakres usług i obszar działania kolejnych generacji telefonii komórkowej*

Ponieważ usługi przewidziane dla systemów 3G np.. protokół WAP *(Wireless Aplication Protocol)* wywołał zainteresowanie abonentów systemów 2G to został zaimplementowany w tych systemach (usługa Omnix w Erze; obecnie T – Mobile) i mówimy, że obecnie mamy generację 2,5 G. Mimo opóźnienia, wdrażane są do

eksploatacji systemy trzeciej generacji UMTS *(Universal Mobile Telecommunications System)*. Środowisko tego systemu przedstawia rysunek 5.81.



Rys.5.81. *Środowisko systemu telefonii komórkowej trzeciej generacji*

Jak widać w systemach trzeciej generacji bardzo dużą rolę odgrywają systemy łączności satelitarnej jako nieodłączna część systemu UMTS.

5.6.5. Satelitarne systemy łączności osobistej

Pomysł telekomunikacji satelitarnej liczy już sobie ponad pół wieku. W roku 1959 International Telecommunications Union przyznała pierwsze częstotliwości dla transmisji satelitarnej. Rok później na orbicie umieszczono pierwszego satelitę o zastosowaniu telekomunikacyjnym, Echo 1 - tylko odbijającego sygnały radiowe. Od tego czasu powstało wiele pomysłów systemów satelitarnych, wiele projektów zrealizowano, powstały też nowe standardy, a transmisji satelitarnej przydzielano nowe częstotliwości. Co wyróżnia systemy satelitarne od innych systemów transmisji danych? Przede wszystkim osoba chcąca się połączyć z siecią nie jest do niej podłączona żadnymi kablami i nie jest tutaj istotna odległość od najbliższej infrastruktury sieciowej. Dane wysyłane są bezpośrednio do satelity kanałem radiowym, a stamtąd wędrują do punktu docelowego przez inne satelity lub przez sieć naziemną. W większości sieci terminal abonenta może być też przenośny.

Budowa systemu satelitarnego

Generalnie, w każdym systemie satelitarnym można wyróżnić trzy elementy składowe:

- moduł naziemny
- moduł kosmiczny

- kanał radiowy.

Moduł naziemny

Moduł naziemny stanowią terminale abonenckie - ruchome lub stacjonarne, szkieletowa sieć naziemna ze stacjami bazowymi, adaptery sieciowe i stacje kontrolne. Terminale abonenckie są zaopatrzone w antenę do nadawania i odbierania danych z satelity oraz urządzenia do przetwarzania sygnałów radiowych wysokiej częstotliwości na sygnały mowy, ramki określonego protokołu, itp. **W satelitarnych systemach komunikacji osobistej S-PCN (*Satellite Personal Communication Network*)** - zakładających możliwość przemieszczania się abonenta z terminalem dąży się do minimalizacji terminali abonenckich, a więc jak najwięcej koniecznego przetwarzania sygnału przerzuca się na inne elementy sieci. W systemach z terminalami stacjonarnymi również istnieje tendencja do zmniejszania rozmiarów terminali, lecz nie jest to w tym przypadku aż tak istotne. Terminalem abonenckim może być również telefon przenośny z możliwością łączenia się z innymi sieciami, nie tylko telefonicznymi, np. GSM czy Internet. Takim terminalem może być też stacjonarny moduł dołączony do komputera, dla abonenta będący po prostu łączem sieciowym na świat. Na ten terminal mogą być wysyłane inne typy danych związane z innymi usługami multimedialnymi - przykładowo transmisja filmu video, telekonferencja, faksy i inne. Generalnie nie ma żadnego ograniczenia, które powodowałoby, że usługi dostępne w sieciach stacjonarnych nie są dostępne przez sieci satelitarne. Terminale abonenckie, chcąc przesłać dane, wysyłają je do najbliższego, w danej chwili dostępnego satelity. Ten przesyła dane dalej przez następne satelity, a często od razu do najbliższej lub po prostu odpowiadającej mu naziemnej stacji bazowej. Jeżeli przeznaczeniem tej wiadomości jest miejsce na Ziemi, w jednej z naziemnych sieci telekomunikacyjnych (np. abonencka sieć telefoniczna lub Internet), stacja bazowa przesyła tą wiadomość dalej przez naziemną sieć szkieletową do punktu będącego połączeniem z tą naziemną siecią telekomunikacyjną. Punkt taki zwany jest adapterem sieciowym (*gateway*). Od tego punktu wiadomość przesyłana jest już według zasad obowiązujących w owej sieci naziemnej. Jeżeli jednak wiadomość ma być przesłana do innego posiadacza terminala abonenckiego sieci satelitarnej, wędruje ona przez naziemną sieć szkieletową do stacji bazowej najbliższej satelity, który z kolei będzie w stanie przetransmitować ją do owego terminala abonenckiego. W tym przypadku wiadomość musi 4 razy przebyć drogę Ziemia - satelita, w porównaniu z dwukrotną taką drogą dla

poprzedniego przypadku. W niektórych systemach (zwłaszcza systemy **S-PCN**) możliwe jest połączenie między dwoma terminalami abonenckimi sieci satelitarnej poprzez kanały transmisyjne między satelitami. Pozwala to na zredukowanie ilości transmisji Ziemia - satelita z czterech do dwóch. Fakt ten jest bardzo istotny ze względu na duże opóźnienia w transmisji wynikające z dużych odległości między Ziemią a satelitami. Stacje kontrolne czuwają nad działaniem całego systemu, m.in. wykonują pomiary położenia satelitów na orbitach i wysyłają im informacje o koniecznych do wykonania manewrach.

Moduł kosmiczny, orbity

Na ten człon systemu składa się określona liczba satelitów umieszczonych na orbitach okołoziemskich. Satelity te do poprawnego działania potrzebują oczywiście energii, co zwykle rozwiązywane jest poprzez posiadane przez nie baterie słoneczne i paliwo dla silników rakietowych. W większości systemów wszystkie satelity krążą po orbitach tego samego typu, ta sama odległość od Ziemi i kąt nachylenia orbity, lecz nie jest to regułą: projekt Motoroli - Celestri był systemem hybrydowym, łączącym satelity różnych typów. Satelity można klasyfikować właśnie ze względu na typy orbit (sygnalizowane już w punkcie 2.3). Jak pamiętamy, wyróżnia się orbity :

- LEO (*Low Earth Orbit*) - orbity o wysokości od 500 do 2000 km nad powierzchnią Ziemi. Poniżej 500 km atmosfera jest zbyt gęsta i występowałyby zbyt duże tarcia w ruchu satelity, natomiast powyżej 2000 km zaczyna się pierwsza ze stref (pasów) Van Allena - obszarów występowania cząstek (protonów i elektronów) o bardzo dużych energiach, mogących spowodować uszkodzenie elektronicznych elementów satelity przebywającego w niej przez dłuższy czas. Mała wysokość lotu satelity oznacza jego dużą prędkość (siła odśrodkowa musi zrównoważyć siłę grawitacji), tak więc satelita przez krótki okres czasu pozostaje w zasięgu stacji naziemnej - czy to bazowej czy abonenckiej - około 10-30 minut. W przypadku transmisji danych czasu rzeczywistego (transmisja rozmowy telefonicznej lub filmu video) kluczowym staje się problem przełączeń dróg transmisji. Jednocześnie duża prędkość satelity rodzi problem proporcjonalnie dużych dopplerowskich zmian częstotliwości. Pojedynczy satelita krążący na tej wysokości ma w swoim zasięgu obszar na powierzchni Ziemi o promieniu nie większym niż 4000 km. Stworzenie systemu globalnego wymaga umieszczenia na orbicie wielu

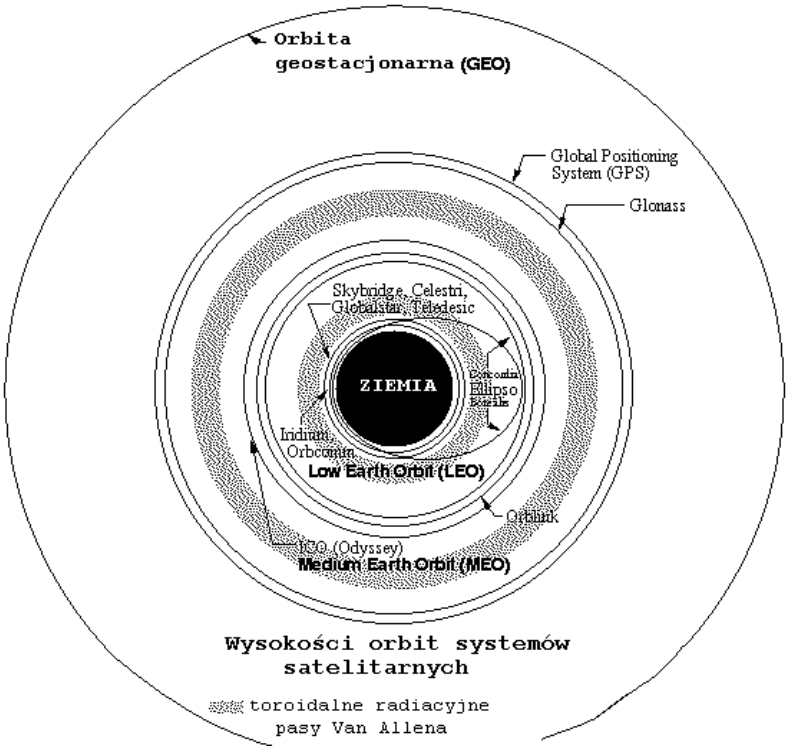
satelitów - np. kilkudziesięciu, krążących po różnych orbitach. Orbity LEO mogą być kołowe lub eliptyczne, jednak najczęściej stosowane są te pierwsze. Mogą mieć też różne odchylenie od powierzchni równika, inklinację, od 0 do 90 stopni.

- MEO (*Medium Earth Orbit*) - wysokość nad powierzchnią Ziemi od 8 do 12 tys. km (a nawet 20 tys.km – systemy nawigacyjne). Ograniczenia zarówno od góry jak i od dołu wynikają z istnienia pierwszej i drugiej strefy Van Allena. Pojedynczy satelita pozostaje nad horyzontem danego punktu kuli ziemskiej przez parę godzin. Budowa systemu globalnego wymaga od 10 do 20 satelitów krążących po kilku różnych orbitach. Czasy transmisji Ziemia - satelita odpowiednio większe w porównaniu z orbitami LEO. Podobnie jak w ich przypadku, MEO mogą być kołowe i eliptyczne, inklinacja od 0 do 90 stopni.

- HEO (*Highly Eliptical Orbit* lub *Helical Earth Orbit*) - orbity silnie eliptyczne: perygeum - odległość najbliższa Ziemi, od ok. 500 km, apogeum odległość najdalsza od Ziemi - do około 50 tys. km. Dzięki takim parametrom orbity satelita jest widoczny z danego obszaru na kuli ziemskiej jako prawie nieruchomy przez pewien okres czasu. Pozwala to na tworzenie systemów o podobnych cechach jak systemy oparte na satelitach geostacjonarnych, ale są to systemy regionalne. Jednocześnie satelita jest widoczny z Ziemi pod dużym kątem elewacji (kątem między kierunkiem z danego punktu powierzchni Ziemi na satelitę a powierzchnią Ziemi), co sprawia, że systemy takie dobrze się sprawdzają również w terenach górskich lub silnie zurbanizowanych. Dla stworzenia systemu regionalnego bazującego na orbitach HEO wystarcza od 2 do 10 satelitów. Obecnie, właściwie nie planuje się nowych systemów HEO a eksploatuje wcześniej zbudowane np. Mołnia i Tundra.

- GEO (*GEOstationary orbit*) - orbity o wysokości 35 786 km w płaszczyźnie równikowej. Satelita krążący po takiej orbicie ma tą samą prędkość kątową co obracająca się Ziemia, dzięki czemu z jej powierzchni widziany jest cały czas w jednym miejscu. Do stworzenia systemu globalnego - nie obejmującego jednak swym zasięgiem obszarów podbiegunowych - wystarczają trzy satelity. Z drugiej strony duża odległość od powierzchni Ziemi oznacza duże opóźnienia w transmisji i konieczność stosowania dużych mocy sygnałów. Orbita ta jest

jednak bardzo popularna i jednocześnie coraz bardziej eksploatowana - korzystają z niej m.in. systemy VSAT, Inmarsat i satelity transmitujące kanały telewizyjne.



Rys.5.82. *Porównanie orbit różnych typów (rysunek ze strony Lloyd's satellite constellation)*

Utrzymanie satelitów na wyznaczonych dla nich orbitach nie jest proste. Często to stacje bazowe pełnią jednocześnie rolę stacji kontrolnych. Wśród informacji sygnalizacyjnych wymienianych z każdym satelitą są dane dotyczące toru jego lotu. Na ich podstawie dokonywane są decyzje o ewentualnej korekcji trasy satelity, co jest możliwe, jako że każdy satelita posiada silnik i zapas paliwa. Czas życia różnych satelitów ocenia się zwykle na kilka do kilkunastu, maksymalnie 20 lat. Ich naprawy nie bierze się pod uwagę. Właśnie paliwo jest jednym z głównych czynników decydujących o czasie życia satelity.

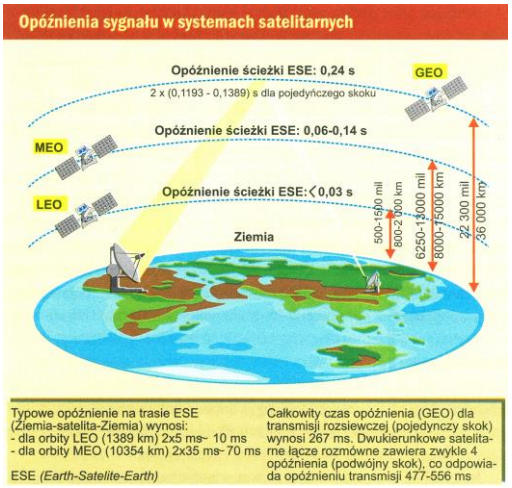
Wysokość orbity ma kluczowe znaczenie dla opóźnienia wiadomości przechodzącej przez system satelitarny. Opóźnienie to największe jest dla orbit geostacjonarnych i silnie eliptycznych. Przykładowo, transmisja sygnału z satelity geostacjonarnego do punktu na Ziemi leżącego dokładnie pod satelitą na równiku, a więc najbliżej satelity na powierzchni Ziemi, trwa: 35786 km / 300000 km/s = 120 ms. Przy tak wysokiej orbicie

zmiana punktu docelowego na powierzchni Ziemi nie wpływa już znacząco na rozmiar opóźnienia. Np. odległość między Krakowem; φ=50° N, λ=20° E, a satelitą geostacjonarnym umieszczonym nad południkiem 0°, a więc "zawieszonym" nad punktem φ=0°, λ=0° to 38644 km, a więc czas transmisji to 129 ms. Odległość satelita - Ziemia jest jednak zawsze pokonywana przez sygnał dwukrotnie, a w przypadku połączenia dwóch terminali abonenckich systemu satelitarnego poprzez naziemną sieć szkieletową - czterokrotnie. W tym przypadku opóźnienie sygnału rośnie do ok. 0.5 s, do czego należy jeszcze doliczyć czas przetwarzania sygnału w różnych punktach trasy oraz opóźnienie jego przejścia przez sieć naziemną. Z jeszcze większymi czasami transmisji należy się liczyć w systemach z satelitami na orbitach HEO. Przy apogeum orbity do 50000 km, pojedynczy czas przesłania wiadomości satelita - Ziemia to okres nawet do 170 ms. Problem opóźnień jest nieco mniejszy w przypadku satelitów krążących po niższych orbitach. Rozważmy system z orbitami na wysokości 1200 km. Gdy satelita znajduje się dokładnie nad stacją na Ziemi, z którą prowadzi transmisję, opóźnienie wynosi 4 ms. W przypadku gdy satelita jest widoczny np. 20° nad horyzontem, odległość do niego wynosi 2455 km, a więc opóźnienie to ok. 8 ms. Tak więc w systemach z satelitami krążącymi po niskich orbitach opóźnienia są wyraźnie mniejsze, ale ich zmiany względne są większe. Dla satelity krążącego po orbicie kołowej o danej wysokości można w prosty sposób obliczyć jego prędkość. Na satelitę działają dwie siły: przyciąganie ziemskie i siła odśrodkowa. Aby satelita krążył po orbicie kołowej, siły te muszą być sobie równe: $\mathbf{G \cdot M \cdot m / r^2 = m \cdot v^2 / r}$ gdzie,

G - stała grawitacji, M - masa Ziemi, m - masa satelity, r - odległość satelity od środka Ziemi (suma promienia Ziemi i wysokości orbity), v - prędkość satelity.

Po przekształceniu tej zależności można otrzymać: $\mathbf{v = (G \cdot M / r)^{1/2}}$

Znając prędkość satelity można również obliczyć okres obiegu orbity: $\mathbf{T = 2 \cdot \pi \cdot r / v}$



Rys.5.83. *Typowe opóźnienia sygnału w systemach satelitarnych*

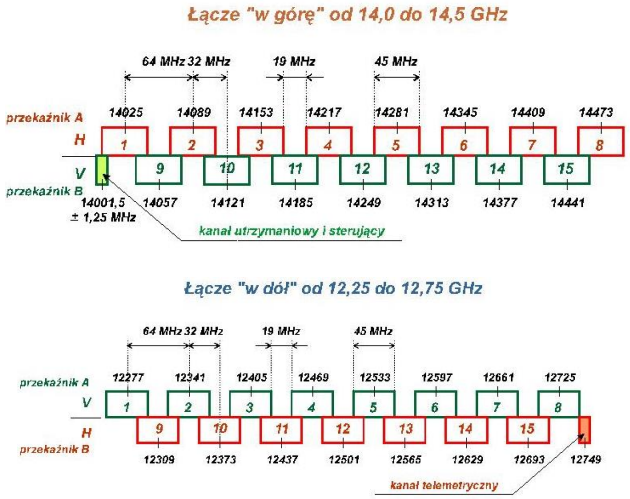
Kanał radiowy

Kanał radiowy przewidziany do transmisji Ziemia - satelita nosi nazwę "*uplink*", zaś kanał do transmisji satelita - Ziemia to "*downlink*". W miarę rozwoju telekomunikacji satelitarnej wzrastały potrzeby na pasmo częstotliwości przydzielone tym kanałom. W związku z tym, na kolejnych światowych konferencjach radiowych WRC (*World Radiocommunication Conference*) przyznawane były coraz to nowe częstotliwości. Przyjęto następujący podział :

- pasmo L - 1-2 GHz
- pasmo S - 2-4 GHz
- pasmo C - 4-8 GHz
- pasmo X - 8-12 GHz → przeznaczone głównie dla organizacji rządowych i wojska
- pasmo Ku - 12-18 GHz
- pasmo K - 18-27 GHz
- pasmo Ka - 27-40 GHz → pasma K i Ka czasem określa się jedną nazwą Ka
- pasmo V - powyżej 40 GHz

Nie oznacza to, że cały zakres 1-40 GHz przewidziano dla łączności satelitarnej. W ramach każdego pasma tylko wybrane zakresy częstotliwości przeznaczono dla transmisji przez satelity - np. w paśmie L są to m.in. 1.215-1.240 GHz (GPS), 1.530-1.559 GHz i 1.6265-1.6605 GHz. W większości przypadków, zakresy częstotliwości przeznaczone na uplink i downlink mają taką samą szerokość.

Wyjątkiem są systemy nawigacyjne, tam kanał "*uplink*" potrzebny jest jedynie do przesyłania informacji sterujących i nie musi mieć dużej przepustowości. Przykłady planów kanałów 500 MHz „w górę” (*uplink*) i „w dół” (*downlink*) w paśmie Ku przedstawia rysunek 5.84.



Rys.5.84. *Przykładowe plany 500 MHz kanałów w paśmie Ku*

Architektura

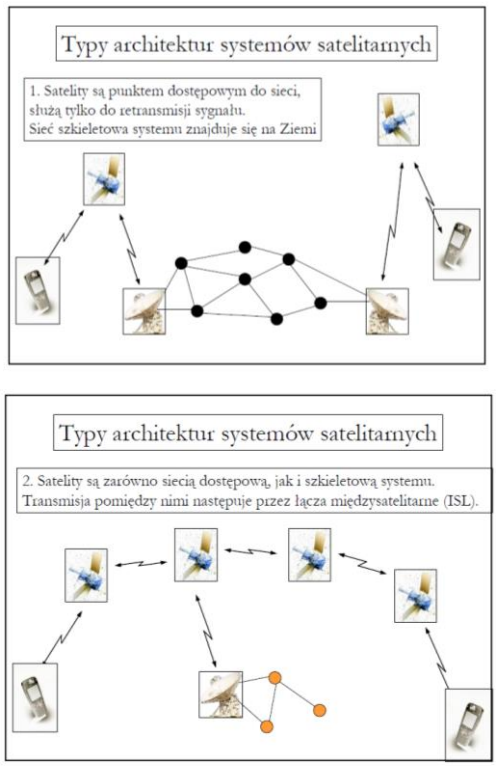
Istnieją dwa typy architektur systemów satelitarnych i oczywiście wersje pośrednie. W pierwszym przypadku satelity są tylko siecią dostępową. Sygnał z terminala abonenckiego jest transmitowany do satelity i zaraz z powrotem na Ziemię - do stacji bazowej. Dalej jest odpowiednio przetwarzany i przesyłany już w szkieletowej sieci naziemnej. W takim układzie satelita tylko retransmituje sygnał na Ziemię, nie przekształca go, jako że nie zna jego typu, nie jest też w stanie wzmocnić sygnału. W tym sygnale nie mogą być też przesyłane żadne informacje sterujące, potrzebny jest do tego osobny kanał od stacji bazowej do satelity. Większy ciężar położony jest na segment naziemny sieci. Większe też muszą być anteny terminali i stacji bazowych i moce sygnałów, jako że muszą uwzględnić wpływ szumów na drodze Ziemia - satelita i satelita - Ziemia.

Taka architektura jest bardzo popularna i chętnie stosowana z dwóch powodów:

1. konstrukcja satelitów jest uproszczona, pozbawione są one elementów wzmacniających, przetwarzających i komutujących wiadomości. Prosta konstrukcja oznacza większą niezawodność.
2. transmisja sygnału przez satelitę jest przeźroczysta. Satelita nie zna typów przesyłanych wiadomości, nie ingeruje w nie. Oznacza to, że można przesyłać

wiadomości dowolnego typu, nie ma konieczności zgodności protokołów transmisyjnych.

W drugim przypadku satelity stanowią zarówno sieć dostępową jak i szkieletową. Może również występować naziemna sieć szkieletowa (albo przynajmniej jej część) uzupełniająca działanie jej satelitarnego odpowiednika. Generalnie przetwarzanie i komutacja wiadomości następuje już w satelitach. Do przesyłania wiadomości bezpośrednio między nimi służą łącza międzysatelitarne ISL (*Inter Satellite Links*). Pomysł architektury tego typu wynika z dążenia do maksymalnego uproszczenia i zmniejszenia rozmiarów terminali abonenckich. W tym przypadku konieczne wielkości anten i moce transmitowanych sygnałów będą mniejsze. Jest to sprawa kluczowa przy projektowaniu sieci osobistych; S - PCN. Jednocześnie dzięki przesyłaniu wiadomości bezpośrednio między satelitami zmniejszają się opóźnienia w transmisji. Taka konstrukcja systemów satelitarnych stała się możliwa dopiero niedawno, wraz z postępem techniki. Konieczne jest bowiem wyniesienie na orbitę satelitów zbudowanych w sposób dużo bardziej skomplikowany i zapewnienie im odpowiedniej niezawodności działania.



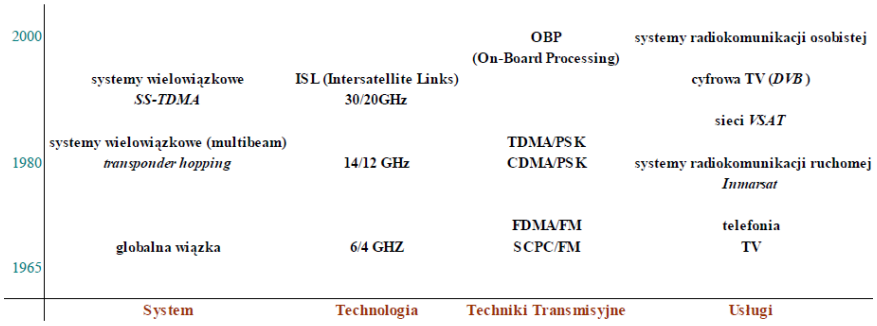
Rys.5.85. *Architektura sieci satelitarnej: jako sieć dostępowa (rysunek górny) i sieć szkieletowo-dostępowa (rysunek dolny).*

Zalety i wady systemów satelitarnych, ich możliwości i perspektywy.

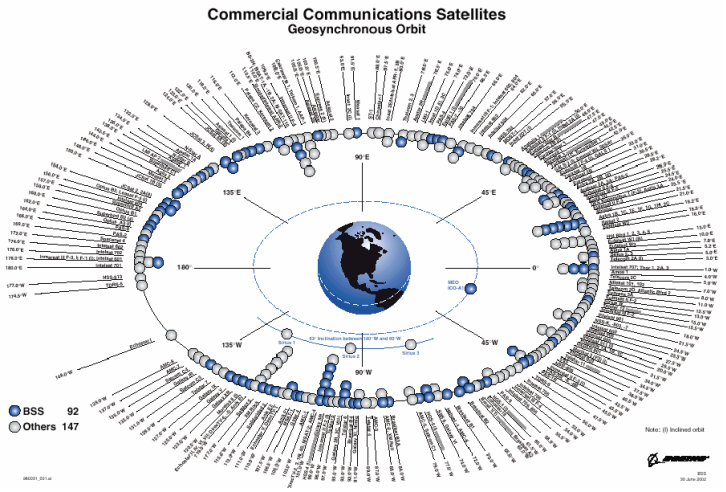
Niezaprzeczalną zaletą łączności satelitarnej jest jej dostępność. Instalacja terminala abonenckiego pociąga za sobą pewne, czasem spore koszty, jednak jest dużo prostsza i szybsza niż kładzenie kabli, zwłaszcza na terenach o małej gęstości zaludnienia. Podobną przewagę mają systemy osobiste (S-PCN) - rozmowę telefoniczną w systemie o zasięgu globalnym można prowadzić z dowolnego zakątka świata, nie przejmując się jakimkolwiek łączem z siecią kablową. W ostatnich projektach sieci satelitarnych przewidywano transmisję szerokopasmową, czyli przepustowości 2 Mbit/s i większe. Planowano kanały 20 Mbit/s i jego krotności (Skybridge), a także 155 Mbit/s (pierwotny projekt Celestri). Pojemności największych sieci szacowano na miliony i dziesiątki milionów użytkowników. Niestety, praktycznie wszystkie projekty sieci telefoniczne czy transmisji danych oparte na satelitach LEO lub MEO zostały zawieszone lub zakończyły się porażką. Słychać było raczej o spektakularnych klapach wielkich konsorcjów satelitarnych niż o ich szybkim rozwoju. Bankructwa dotknęły Iridium, Globalstar, ICO i Odyssey. Projekt Skybridge został wstrzymany. Teledesic ogłaszał kolejne redukcje liczby satelitów, w końcu z niego zrezygnowano. Dobrze funkcjonują systemy VSAT, jednak proponowane w tych sieciach usługi są dość ograniczone. Z pewnością decydujący jest tutaj czynnik finansowy. Uruchomienie globalnej sieci satelitarnej to koszt od kilku do kilkunastu mld $. Pieniądze te muszą się później zwrócić, co oznacza wysokie ceny usług oferowanych użytkownikom. Ceny te mogłyby spaść przy dużej liczbie klientów, ale kwoty, które są z początku wysokie, zniechęcają firmy i indywidualnych odbiorców do korzystania z łączności przez satelitę. Jednocześnie sieci satelitarne mają ostrą konkurencję, nawet w terenach słabo zurbanizowanych, a zwłaszcza w dużych miastach. W dziedzinie telefonii ruchomej dominują sieci GSM, dużo tańsze w budowie. Dostęp do Internetu oferuje wielu operatorów bazujących na sieciach naziemnych i radiowych, dzięki technice światłowodowej dostęp ten jest coraz szybszy, możliwy w nowych regionach, a oferty są coraz bardziej konkurencyjne. W takiej sytuacji przetrwać mogą przede wszystkim te systemy, które etap rozwoju mają już za sobą i ich pozycja na rynku jest ustalona. Są również pewne specyficzne funkcje i usługi, które zdecydowanie najprościej jest zrealizować właśnie przez satelitę. Przykładem może być tworzenie sieci prywatnej z jednostek rozproszonych po dużych obszarze - w czym świetnie sprawdzają się VSAT-y lub zapewnianie podstawowej łączności morskiej, co stało się domeną

konsorcjum Inmarsat. Istnieją też miejsca, gdzie dostęp do sieci telefonicznych czy Internet nie jest możliwy w inny sposób niż przez satelitę ze względu na specyficzne położenie geograficzne. Jednak przypadków takich nie jest wiele, dlatego jest to raczej rynek dla mniejszych firm dzierżawiących łącze satelitarne i świadczących określone usługi.

Czy w takiej sytuacji globalne satelitarne systemy multimedialne są z góry skazane na porażkę? Byłoby to chyba przedwczesne stwierdzenie. Ważne jest jednak, aby za projektem sieci satelitarnej stał inwestor ze sporym zapasem cierpliwości i gotówki w kieszeni. Projektowany system musi być konkurencyjny cenowo do istniejących rozwiązań naziemnych, musi dostosowywać się do oczekiwań klientów i być przygotowany na początkowy okres małego zainteresowania swoimi usługami. Mimo tych problemów systemy satelitarne mają swoich zwolenników i ciągle się rozwijają, a zwłaszcza systemy rozsiewcze (broadcastingowe) radiofonii (DSR – *Digital Sattelite Radio*) i telewizji (DVB – S, *Digital Video Broadcasting*). Rozwój systemów satelitarnych przedstawia rysunek 5.86 zaś na rysunku 5.87 poglądowo przedstawiono rozmieszczenie satelitów komercyjnych na orbicie geostacjonarnej.



Rys.5.86. *Rozwój komunikacji satelitarnej*



Rys.5.87. *Komercyjne satelity komunikacyjne na orbicie geostacjonarnej*

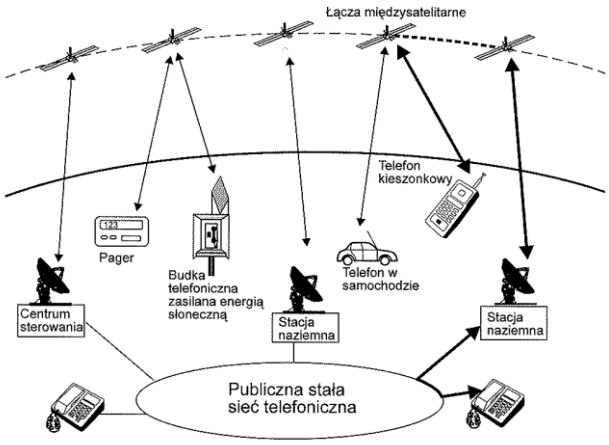
Idea sieci **S-PCN** (*Satellite Personal Communication Network*) polega na zapewnieniu globalnej łączności klientom indywidualnym. Zakłada się, że abonent takiej sieci może się poruszać. Podstawowymi usługami są telefonia, transmisja danych, faks i łączność z publiczną siecią telekomunikacyjną (telefoniczna, Internet). W porównaniu z innymi sieciami satelitarnymi bardziej istotne są :

- małe opóźnienia w transmisji - z tego powodu sieci S-PCN projektuje się w oparciu o satelity LEO, ewentualnie MEO. Satelity takie szybko okrążają Ziemię, mają duże prędkości względem jej powierzchni - siła odśrodkowa ruchu musi zrównoważyć siłę grawitacji, która blisko Ziemi jest większa niż w przypadku orbit geostacjonarnych. Oznacza to, że właściwie nie ma różnicy między abonentami ruchomymi i stacjonarnymi - wszyscy są w ruchu względem satelitów z bardzo dużą prędkością. Mały czas widzialności satelity z Ziemi oznacza też, że często muszą występować przełączenia połączeń z terminalami abonenckimi na innego satelitę.
- mała waga i rozmiary terminali abonenckich - terminale z zasady mają być przenośne.

Poniżej opisanych jest kilka z wielu systemów S-PCN. Jednak obecnie funkcjonują tylko Iridium i Globalstar, zresztą po wcześniejszym zbankrutowaniu. Generalnie, firmy planujące sieci S-PCN albo zbankrutowały, albo realizacja ich projektów została wstrzymana. Wstrzymana została również dalsza rozbudowa systemu

Skybridge – czyli projektowi satelitarnej sieci szkieletowej o dużej przepustowości łączącej stacjonarne węzły naziemne.

Zasadę pracy przykładowego niskoorbitowego systemu łączności satelitarnej przedstawia rysunek 5.88.



Rys.5.88. *Zasada działania przykładowego niskoorbitowego systemu łączności satelitarnej*

Ograniczenia i wymagania na systemy satelitarne:

- Przeciążenia i wibracje w czasie wynoszenia satelity na orbitę
  - wszystkie systemy satelity muszą pracować poprawnie po takich narażeniach.
- Próżnia
  - problem z odprowadzaniem ciepła
  - odgazowywanie niektórych materiałów
- Promieniowanie (cząstki o dużej energii: elektrony, protony, ciężkie jony; promieniowanie elektromagnetyczne)
  - błędy w układach elektronicznych, zwłaszcza półprzewodnikowych (SEL, SEU)
  - całkowita dawka promieniowania
  - poziom promieniowania zależy od wysokości orbity
  - pasy van Allena
- Szeroki zakres zmian teperatury
- Brak możliwości napraw

- Ładunek użyteczny – zawierający instrumenty, aparaturę, przekaźniki niezbędne do realizacji misji systemu satelitarnego

- Platforma satelitarna
  - struktura nośna; mocowanie systemów, ekranowanie, odprowadzanie ciepła, połączenie z rakietą nośną;
  - system komunikacyjny (COMM); realizacja łączności z naziemną stacją kontrolno - sterującą;
  - system sterowania (OBDH); kontrola i sterowanie pracą wszystkich systemów satelity;
  - system kontroli orientacji (ACS); kontrola orientacji satelity na orbicie;
  - system zasilania (EPS); generacja napięć zasilania wszystkich systemów satelity;
  - system termiczny (THERMAL); kontrola temperatury wewnątrz satelity;
  - system silników korekcyjnych (PROPULSION); utrzymanie satelity na właściwej orbicie

Zestawienie parametrów wybranych komórkowych systemów satelitarnych przedstawia tabela 5.7, a parametry stosowanych obecnie satelitów tabele od 5.8 do 5.12.

Tabela 5.7. *Zestawienie parametrów wybranych satelitarnych systemów komórkowych*

System	Data uruchomienia	Rodzaj orbity	Wysokość orbity	Liczba satelitów
Globalstar	1998 - 1999	niska	1414 km	48
ICO	1999 - 2000	średnia	10400 km	10
Irydium	1999	niska	780 km	66
Odyssey	1998 - 2000	średnia	10373 km	123
Teledesic	2001	niska	700 km	924

Tabela 5.8. *Zakresy częstotliwości przyznane satelitarnym systemom telekomunikacyjnym.*

Pasmo	Zakres częstotliwości [GHz]
L	1,530 – 2,700
S	2,700 – 3,500
C (łącze do abonenta)	3,700 – 4,200
C (łącze od abonenta)	5,925 – 6,4,25
X (łącze do abonenta)	7,250 – 7,745
X (łącze od abonenta)	7,900 – 8,395
Ku (łącze od abonenta)	10,700 – 12,750
Ku (łącze od abonenta)	12,750 – 14,500 17,300 – 18,100
Ka	17,700 – 31,000
Q – V	36,000 – 51,400

Tabela 5.9. *Podstawowe parametry satelity ASTRA – 1K.*

Parametr	Wartość przeciętna dla istniejących satelitów	Wartość dla satelity ASTRA 1K
Masa startowa	3500 – 4100 kg	5250 kg
Moc baterii słonecznych	6 – 10 kW	13 kW
Wysokość	5,2 m	7,6 m
Czas życia	10 – 15 lat	13 – 19 lat
Masa ładunku użytkowego	500 kg	680 kg
Liczba LFB*) (110 W)	40 (zakres Ku)	58 (zakres Ku)
Liczba kanałów	60	112
Liczba anten	3 - 4	10
Rakieta nośna	Ariane 4/5; Atlas IIA; LM 2	Proton d-1-E**)

*) Lampa z falą bieżącą **) Przewidywana przez SES

Tabela 5.10. *Parametry terminala systemu ARCS* *)

Parametr	Wartość
Pasmo nadawcze (Tx)	29,50 – 30 GHz
Pasmo odbiorcze (Rx)	10,70 12 – 12,75 GHz
Polaryzacja	liniowa
Średnica anteny	0,6 – 1,2 m
Moc nadajnika	0,5 – 2 W
Maksymalna szybkość transmisji danych użytkownika	144 – 2048 kb/s

*) ARCS *(Astra Radio Communication System)* obecnie Astra Broadband Interactive System.

Tabela 5.11. *Parametry kanału podstawowego*

Parametr	Wartość
System transmisji	Zgodny z DVB-S (ETS 300 421)
Sygnalizacja	Zgodna z DVB DB
Częstotliwość p. cz.	950 – 2150 MHz
Synchronizacja	10 MHz z ODU*)

*) ODU *(Out Door Unit)*

Tabela 5.12. *Parametry kanału zwrotnego*

Parametr	Wartość
Modulacja	QPSK
Kodowanie	Kod RS*) + kod splotowy
Dostęp	MF - TDMA
Protokoły	IP**) przez ATM i ATM***)
Synchronizacja	Z kanału podstawowego
Sterowanie transmisji	Blokada transmisji, gdy: 1. brak odbioru kanału podstawowego i autoryzacji, 2. człowiek w pobliżu anteny (detektor).
Częstotliwość p.cz.	2500 – 3000 MHz
Kontrola nadawanej mocy	Na podstawie poziomu sygnału odbieranego

*) RS kod Reeda – Salomona, **) IP Internet Procotol, ***) ATM Asynchronous Transfer Mode

Omówimy przykładowe systemy satelitarnej łączności osobistej wymienione w tabeli 5.7.

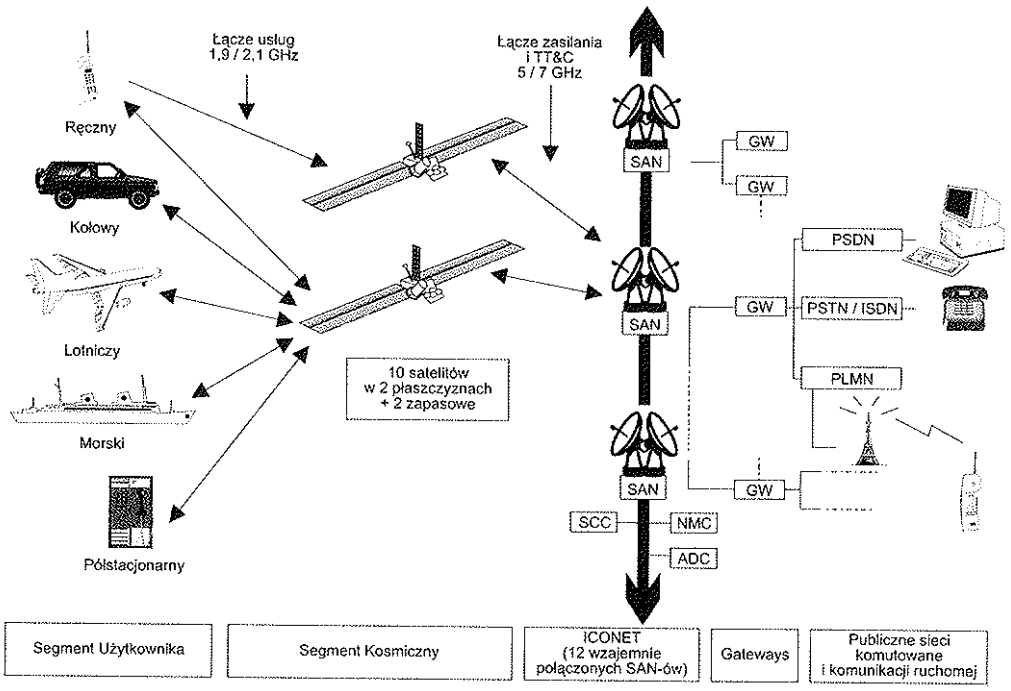
5.6.5.1. System ICO (Intermediate Circular Orbit)

Inne nazwy tego systemu to Inmarsat P, Project 21 lub Inmarsat P-21. Początkowo projekt planowany był przez konsorcjum Inmarsat, potem przejęty przez niezależną firmę, stąd zmiana nazwy. Plan systemu jest dość podobny do planu Odyssey, z którym zresztą toczono spór prawny o wysokość orbity. Bazuje na 10 i 2 zapasowych satelitach MEO. Wysokość orbity to 10355 km, potem zmienione na 10390 km, inklinacja wynosi 45°. Satelity odbierają sygnał od terminali ruchomych, zmieniają jego częstotliwość i transmitują do stacji naziemnych, bez przetwarzania informacji na orbicie (przekaźniki bierne). Techniką wielodostępu jest TDMA.
Wykorzystane są częstotliwości :

- łącze od satelity do terminala abonenckiego: 1980÷2010 MHz
- od terminala do satelity: 2170÷2200 MHz
- od stacji naziemnej do satelity: 5150÷5250 MHz
- od satelity do stacji naziemnej: 6975÷7075 MHz

Terminale abonenckie mają rozmiary telefonów komórkowych. Umożliwiają łączność telefoniczną, przesyłanie faksów, transmisję danych i paging. ICO, jako członek grupy GSM Memorandum of Understanding, wykorzystał wiele z techniki GSM przy projektowaniu systemu. Zakładano zresztą, że terminale ICO będą działać jako dwusystemowe w połączeniu z siecią komórkową - najpierw podejmowana będzie próba połączenia przez sieć komórkową, a gdy to nie będzie możliwe - przez sieć satelitarną.

Pieniądze na budowę systemu skończyły się 27 sierpnia 1999 roku i firma ICO Global Communications ogłosiła upadłość. W maju 2000, pozostałości majątku i krążące po orbitach satelity zostały przejęte nowo powstałą firmę New ICO, ściśle współpracującą z Teledesic.



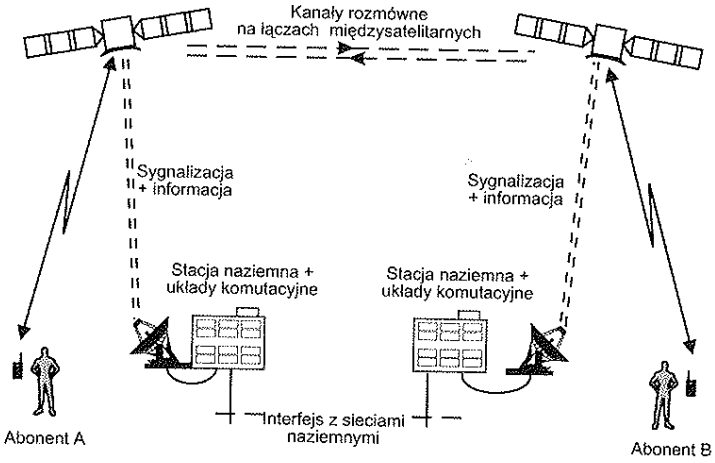
Rys.5.89. *Ogólna konfiguracja systemu ICO; gdzie: SAN (Satellite Access Node) – węzeł dostępu satelitarnego, GW (Gateway) – centrala wejściowa do systemu satelitarnego, PSDN (Public Switched Data Network) – publiczna komutowana sieć danych, PSTN (Public Switched Telephone Network) – publiczna komutowana sieć telefoniczna, PLMN (Public Land Mobile Network) – publiczna sieć radiokomunikacji ruchomej lądowej, SCC (Satellite Control Center), – centrum sterowania systemu satelitarnego, NMC (Network Maintenance Center) – centrum utrzymania sieci.*

5.6.5.2. System IRYDIUM

Iridium to jedyna w pełni globalna sieć telefonii satelitarnej, której **usługi dostępne dosłownie na całym świecie**. Jest to system 66 sztucznych satelitów telekomunikacyjnych rozmieszczonych na orbicie okołoziemskiej 485 mil nad Ziemią (780 km). System ten pierwotnie miał posiadać 77 satelitów, a ponieważ pierwiastek chemiczny iryd ma liczbę atomową 77 stąd nazwa tego systemu. **Iridium** umożliwia komunikację głosową oraz przesyłanie danych na całym świecie za pomocą urządzeń przenośnych. Za funkcjonowanie sieci odpowiedzialne są satelity. Każda z nich może komunikować się z dwoma sąsiadującymi satelitami na swojej orbicie oraz z dwoma najbliższymi z orbit sąsiednich. Wszystkie wyposażone są w 48 anten, obejmujących na Ziemi komórki o średnicy 700 km. Pozwala to na całkowite wyeliminowanie naziemnych przekaźników w przypadku połączeń pomiędzy dwoma telefonami

Iridium. Stacje naziemne są wykorzystywane tylko wówczas, gdy chcemy nawiązać połączenie między telefonami satelitarnym a stacjonarnym lub komórkowym.

Iridium rozpoczęło swoje działanie 1 listopada 1998 roku, a bankructwo przedsięwzięcia ogłoszono 13 sierpnia 1999. Przyczyn niepowodzenia tego systemu upatrywano w wysokich kosztach i niewygodzie użytkowania oraz w silnej konkurencji ze strony usług roamingowych operatorów GSM. Także nie bez wpływu były błędy w zarządzaniu firmą. Satelity systemu **Iridium** pozostały jednak na orbicie i w 2001 roku firma prywatnych inwestorów pod nazwą **Iridium Satellite LLC** wznowiła działanie systemu. Dziś do najważniejszych klientów **Iridium Satelite LLC** należy amerykański Departament Obrony, który płaci za bezprzewodową komunikację 20 tys. pracowników. Nowy operator oferuje usługi telefonii satelitarnej również indywidualnym klientom. Oprócz transmisji głosu, firma świadczy także usługi dostępu do Internetu praktycznie z dowolnego miejsca na ziemi.

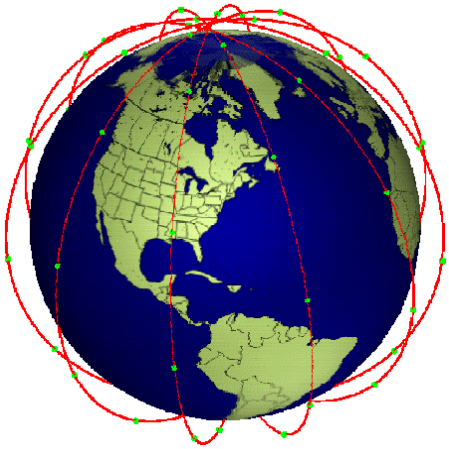


Rys.5.90. *Ogólna koncepcja systemu IRYDIUM*

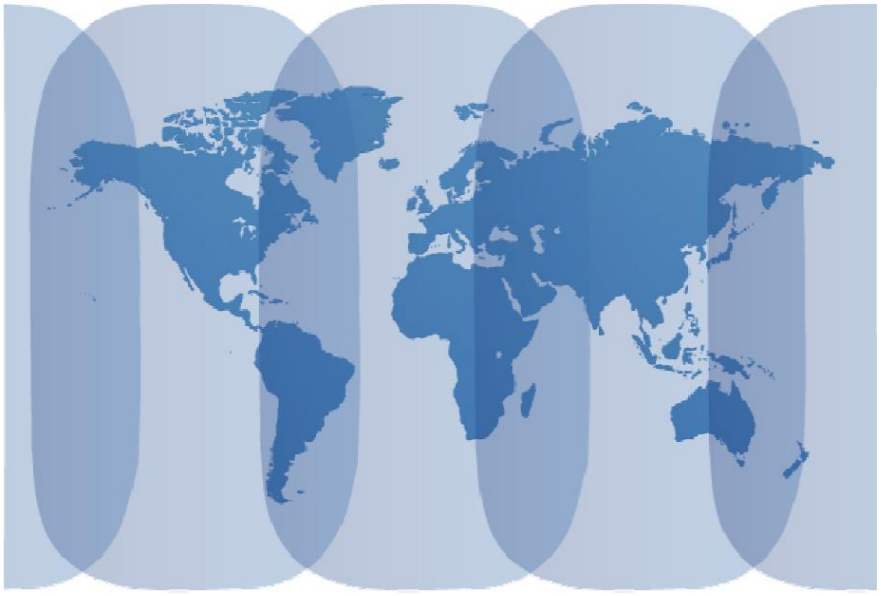
Satelity Irydium dzięki zastosowanym w ich budowie antenom, które prawie bez strat odbijają promienie słoneczne, satelita **Iridium** podczas przelotu może utworzyć na niebie silny błysk (flarę) o jasności nawet do - 9 magnitudo *(jednostka jasności gwiazd, czyli tzw. wielkość gwiazdowa, jest to pozaukładowa jednostka miary natężenia światła)*. Błyski o takiej jasności mogą być widoczne nawet w dzień, czasem identyfikowane jako UFO.

Rys.5.91. *Flary (rozbłyski) od anten satelitów Irydium*

Iridium NEXT - przyszłość sieci. Iridium rozpoczęło intensywny program Badań i Rozwoju (RD) mający za zadanie zdefiniowanie i opracowane konstelacji satelitów najnowszej generacji, która powinna zostać ukończona do roku 2016. Nazwana "Iridium NEXT", nowa sieć będzie dźwignią najnowszych technologii satelitarnych i bezprzewodowych, umożliwiającą wykorzystanie nowych, zaawansowanych urządzeń przez rządy państw i w celach komercyjnych. Iridium ma zamiar wbudować w swoje nowe satelity wtórne komponenty zapewniające przychód, takie jak czujniki pogodowe i oceanograficzne. Niedawno, Iridium ogłosił, że firma ograniczyła poszukiwania głównych partnerów technologicznych dla systemu Iridium NEXT do trzech firm – Lockheed Martin, Space Systems Loral i Thales Alenia Space.



Rys.5.92. *Konstelacja IRYDIUM*



Rys.5.93. *Zasięg IRYDIUM*

Numery telefoniczne **Iridium** składają się z prefixu +**8816** lub +**8817** i 8 cyfrowego numeru abonenta. Nowy telefon satelitarny Iridium 9555 to dużo lżejsza (266 gramów), mniejsza (143 mm x 55 mm x 30 mm) i bardziej wytrzymała na warunki atmosferyczne konstrukcja z chowaną anteną zewnętrzną. Zaletą nowego telefonu jest wbudowany interfejs Mini-USB do pracy z komputerem.

5.6.5.3. System GLOBALSTAR

Projekt Globalstar otworzono w 1991 roku, jako przedsięwzięcie joint-venture firm Loral Corporation i Qualcomm. 24 marca 1994 ogłosili oni powstanie spółki partnerskiej (Globalstar LP) z ograniczona odpowiedzialnością z wkładem finansowym jeszcze ośmiu innych firm, m.in. Alcatel, AirTouch, Deutsche Aerospace, Hyundai i Vodafone. Szacowano wtedy, że system zacznie działać w 1998, kosztem 1,8 mld. USD. W lutym 1995, Globalstar Telecommunications Ltd. zebrało 200 mln USD z emisji akcji w ofercie publicznej podczas wchodzenia na giełdę NASDAQ. Po dwóch podziałach akcji, akcja o początkowej cenie 20 USD, była teraz odpowiednikiem akcji za 5 USD. Po podziałach, w styczniu 2000, notowania sięgnęły 50 USD za udział, ale inwestorzy instytucjonalni zaczęli wróżyć firmie bankructwo do czerwca 2000. Notowania spadły w końcu do kwoty poniżej dolara za aukcje i firma została usunięta z giełdy NASDAQ w czerwcu 2001. Po emisji oferty publicznej, głównym zródłem finansowania Globalstar LP były firmy dostarczające jej

sprzęt, Loral i Qualcomm. Po zainwestowaniu i zadłużeniu się na 4,3 miliarda USD, 15 lutego 2002, Globalstar Telecommunications rozpoczęło proces upadłościowy. Miało wtedy aktywa warte 570 mln USD i zobowiązania na kwotę 3,3 mld USD. Aktywa zostały wykupione za 43 mln USD przez Thermo Capital Partners LLC. Nowo utworzona spółka, na bazie upadłej, w kwietniu 2004, była własnoscia Thermo Capital Partners (81,25%) i pierwotnego wierzyciela, Globalstar L.P. (18,75%). Podobnie jak Iridium, Globalstar otrzymał od amerykańskiej Federalnej Komisji Łączności (FCC) koncesje na użytkowanie pasma częstotliwości w styczniu 1995 i od tego czasu negocjował z innymi krajami możliwość użytkowania tego samego pasma na ich terytorium. Pierwsze satelity zostały wystrzelone 14 lutego 1998. Budowa konstelacji została jednak poważnie opóźniona przez serie kosztownych i szkodliwych dla wizerunku firmy nieudanych startów. Największą stratę spowodował nieudany start rakiety Zenit 2; 9 września 1998, w którym utracono aż 12 satelitów. 08.02.2000 roku ukończono budowę konstelacji satelitów: 48 głównych i 4 zapasowych (zamiast planowanych 8). Pierwsza rozmowa telefoniczna wykorzystująca system Globalstar odbyła się 1 listopada 1998, miedzy Irwinem Jacobsem, prezesem Qualcomm, będącym w San Diego, a Bernardem Schwartzem, prezesem Loral Space and Communications, będącym w Nowym Jorku. W październiku 1999, system zaczął przechodzić pierwsze próby użytkowe z udziałem 44 satelitów. W grudniu 1999, rozpoczęła sie faza ograniczonego funkcjonowania komercyjnego (200 użytkowników; brak satelitów zapasowych). W lutym 2000, Globalstar zaczął normalną pracę komercyjną, z 52 satelitami, na terenie Ameryki Północnej, Europy i Brazylii. Początkowe stawki za rozmowy wynosiły 1,79 USD/minutę, podczas gdy Iridium liczyło sobie 9 USD za minutę rozmowy. W 2005 pierwsze satelity z konstelacji zaczęły osiągać maksymalny czas działania, 7,5 roku. W grudniu tego samego roku, Globalstar zaczął przemieszczać owe satelity na orbity tzw. „cmentarne", powyżej orbity LEO. 18 kwietnia 2007 Globalstar oświadczył, że wyśle dodatkowe 8 satelitów w celu wzmocnienia działania dotychczasowych satelitów pierwszej generacji. 29 maja tego samego roku, konsorcjum Starsem wystrzeliło 4 pierwsze zapasowe satelity. W grudniu 2006, Globalstar ogłosił, że kontrakt na budowę satelitów drugiej generacji, wartości 661 mln USD, wygrała firma Alcatel Alenia Space. Satelity te będą zaprojektowane do pracy przez 15 lat.

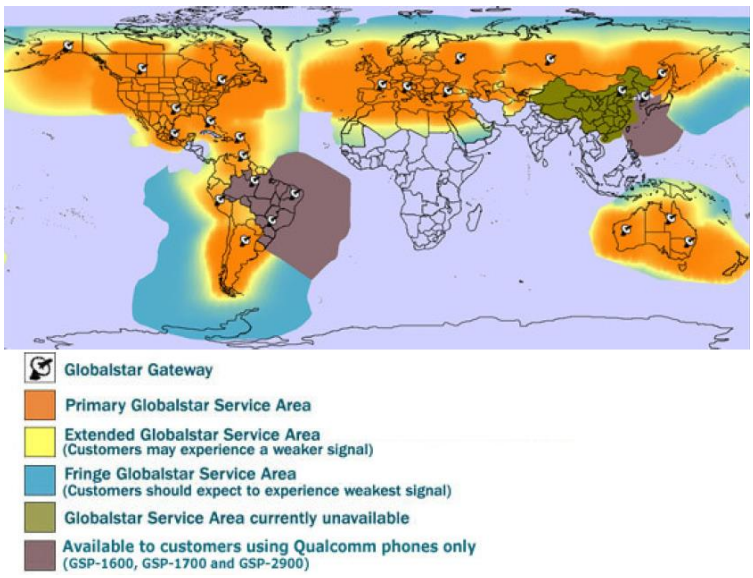
3 kwietnia 2007 Globalstar poinformował także o przyznaniu Alcatel Alenia Space kontraktu, na około 12 mln USD, na usprawnienie działania satelitów Globalstar, w tym wykonanie ulepszeń w sprzęcie i oprogramowaniu w ośrodkach kontroli konstelacji.

System GLOBALSTAR jest prawdopodobnie głównym konkurentem systemu IRIDIUM. Koncepcja systemu zdecydowanie różni się od idei systemu IRIDIUM w wielu aspektach.

Badania nad doborem orbit LEO wykazały, że możliwe są dwie koncepcje ustalenia ich pozycji. Są to:

- orbity w płaszczyźnie biegunów zapewniające pełne pokrycie globu ziemskiego; takie rozwiązanie przyjęto w systemie IRIDIUM,
- system orbit w płaszczyznach pod ustalonym kątem (z określoną inklinacją) względem płaszczyzny równika nie zapewniający pokrycia obszarów okołobiegunowych, ale zaprojektowany tak, aby pokryć zadany pas szerokości geograficznych.

Tę drugą koncepcję ustalenia położenia orbit przyjęto w systemie GLOBALSTAR. W założeniu system ma w pełni pokrywać obszar kuli ziemskiej w zakresie ± 70° szerokości geograficznej. Odpowiada to praktycznie pokryciu obszarów zamieszkałych z wyjątkiem północnej części Grenlandii, Spitsbergenu i wysp północnej Kanady. Mapę pokrycia systemu przedstawiono na rys. 5.94.



Rys.5.94. *Zasięg systemu Globalstar*

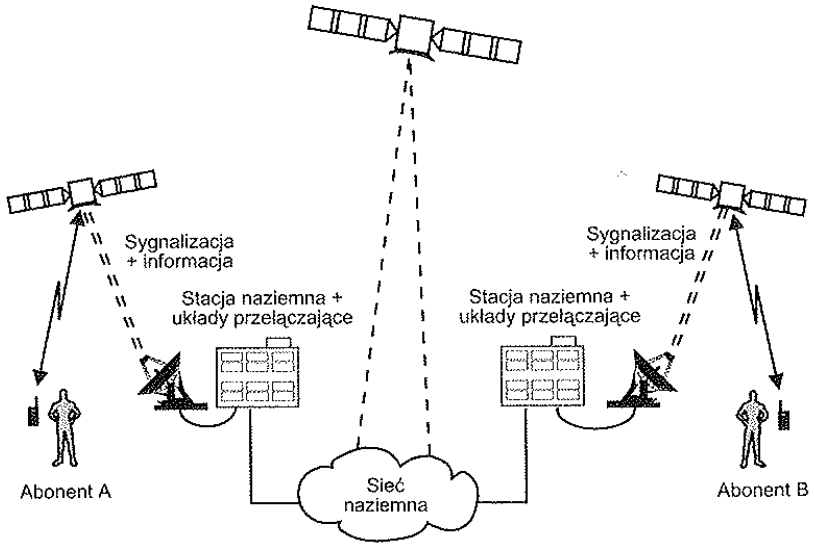
5.6.3.1. Segment satelitarny

System Globalstar w swoim założeniu ma pokryć obszar kuli ziemskiej w zakresie 70° szerokości geograficznej, prócz północnej części Grenlandii, wysp

północnej Kanady i Spitsbergenu. Satelity Globalstar są jedynie przekaźnikami nawiązywanych rozmów i sesji przesyłania danych; nie występują w systemie połączenia miedzy satelitami. Siec naziemnych bramek dostępowych zapewnia połączenie satelitów z ogólnodostępną siecią telefoniczna. Użytkownicy posiadają przypisany numer telefoniczny w systemie numeracji Ameryki Północnej lub kraju, w którym znajduje się przypisana im bramka dostępowa. Ponieważ satelity nie przekazują sygnałów miedzy sobą, aby przekazać połączenie, satelita musi być w zasięgu bramek dostępowych obu stron połączenia. Niektóre niedostępne tereny, takie jak tereny morskie położone daleko od lądu, nie objęte bramkami dostępowymi, nie są objęte działaniem sieci Globalstar, mimo że przelatują nad nimi satelity. Aby uzyskać jak najlepsze własności propagacyjne ustalono kąt inklinacji satelitów równy 52°, przez co nie obejmują regionów polarnych i podbiegunowych. Okres okrążenia kuli ziemskiej wynosi 114 min. Satelity krążą w ośmiu płaszczyznach na wysokości 1414 km (orbita LEO) z przesunięciem faz miedzy płaszczyznami o 7,5°. Istotną cechą konstelacji satelitów systemu GLOBALSTAR jest to, że zapewniona jest równoczesna widzialność dwóch satelitów. Pozwala to na ciągłości działania systemu mimo możliwej awarii pojedynczych satelitów. Zapewnia to zachowanie ciągłości działania systemu mimo możliwej awarii pojedynczych satelitów. Ustalona wysokość orbit satelitów powoduje niewielkie opóźnienia propagacji sygnału oraz pozwala uniknąć niekorzystnego oddziaływania pasów Van Allena (Pasy Van Allena to toroidalne pasy radiacyjne ponad kulą ziemską skoncentrowane nad równikiem około 2200 i 18500 km nad powierzchnią Ziemi, koncentrujące naładowane cząstki. W pasach tych występuje silne promieniowanie elektromagnetyczne i aparatura w nich znajdująca się wymagałaby specjalnej ochrony). Podniesienie wysokości orbit w stosunku do tych, na których krążą satelity systemu IRIDIUM spowodowało, że ich liczba jest mniejsza - na każdej z ośmiu płaszczyzn krąży 6 satelitów czynnych oraz jeden zapasowy. Minimalne i maksymalne opóźnienia propagacji sygnału wynoszą odpowiednio 4,63 i 11,5 ms.

Następnym elementem różniącym system GLOBALSTAR od IRIDIUM jest ogólna koncepcja funkcjonowania systemu. Jego projektanci założyli, że ma on być przedłużeniem systemów radiokomunikacji ruchomej lądowej. Oznacza to, że abonent systemu GLOBALSTAR nawiązuje łączność z satelitą, który łączy go z najbliższą stacją naziemną. Ta zaś poprzez naziemną sieć łączności realizuje połączenie (patrz rys. 5.95). Środkowy satelita pokazany na rys. 5.95 wskazuje, że połączenie pomiędzy

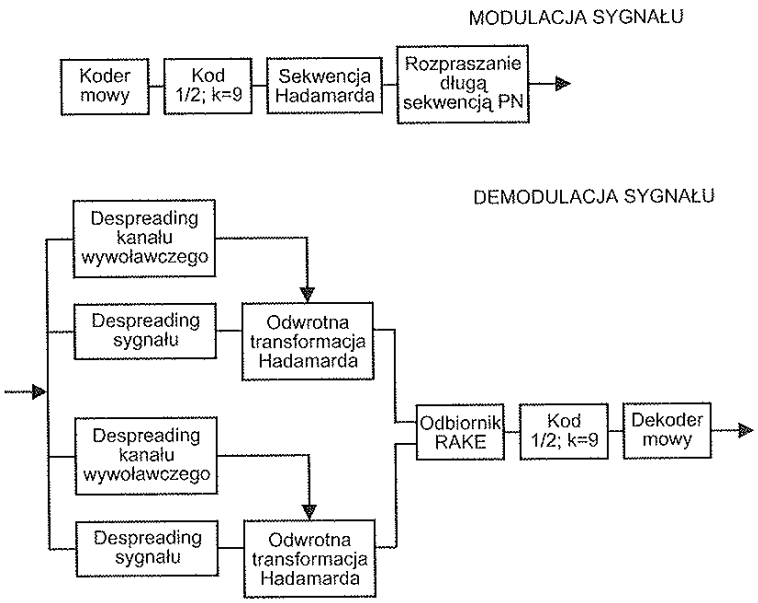
stacją abonenta systemu GLOBALSTAR a stacją drugiego abonenta może być częściowo zrealizowane także z użyciem innych systemów satelitarnych. W konsekwencji część satelitarna ma być „przezroczysta" dla pozostałej części systemu. Powoduje to znaczne uproszczenie części satelitarnej systemu i redukuje jej koszt. „Przezroczystość" części satelitarnej systemu wymaga, aby infrastruktura stacji naziemnych *(gateways)* zapewniała połączenie ich do sieci publicznych, przy czym gęstość stacji naziemnych powinna być rzędu jednej stacji na milion km^2, co odpowiada jednej stacji w średniej wielkości kraju europejskim. Przy takiej gęstości stacji naziemnych nie są wymagane połączenia międzysatelitarne. Przy istnieniu stacji naziemnych w każdym większym kraju lokalni operatorzy nie będą pominięci i dzięki bazom danych zarządzającym ruchem abonentów będą w stanie kontrolować własny ruch i ustalać taryfę zgodnie z własnymi zasadami. Z przezroczystości wynika także zasada działania podobna do działania komórkowych sieci naziemnych. Aby zapewnić ciągłość połączenia, w szczególności, gdy aktualny ruch jest przejmowany od danego satelity przez następnego, abonent ruchomy musi pozostawać w obszarze działania określonej stacji kontroli satelitów, w obrębie której nawiązano połączenie. GLOBALSTAR jest systemem wykorzystującym w technice transmisyjnej metodę CDMA. Z wyjątkiem IRIDIUM oraz ICO, pozostałe systemy mają stosować tę technikę korzystając ze wspólnego, ustalonego w trakcie konferencji WARC'92 pasma (WARC - *World Administrative Radio Conference* - odbywająca się cyklicznie konferencja, na której m. in. Zostają ustalone zasady użytkowania pasm częstotliwości). System musi być więc odporny na interferencje pochodzące od innych użytkowników tego samego pasma stosujących metodę CDMA a także na oddziaływanie innych systemów działających w dolnej jego części.



Rys.5.95. *Ogólna koncepcja systemu GLOBALSTAR*

Na rysunku 5.96 przedstawiono ogólny schemat blokowy części nadajnika wykonującej operacje związane z CDMA. Tak więc sygnał mowy podlega algorytmowi kodowania mowy, w wyniku czego na wyjściu kodera uzyskujemy strumień danych o trzech możliwych szybkościach: 4,8; 2,4 lub 1,2 kbit/s w zależności od aktywności mówiącego. Strumień wyjściowy z kodera mowy podlega następnie kodowaniu korekcyjnemu za pomocą kodu splotowego o sprawności $R = 1/2$ i długości wymuszonej $K = 9$. Ciąg z wyjścia tego kodera jest następnie rozpraszany na osi częstotliwości przez zastosowanie jednego ze 128 ciągów Hadamarda. Rozproszony ciąg jest z kolei mnożony przez ciąg pseudolosowy o długim okresie, który pozwala rozróżnić komórki systemu między sobą. Chociaż ten ogólny schemat jest wielokrotnie cytowany, znając zasadę systemu radiokomunikacji komórkowej IS-95 zaproponowanego przez firmę Qualcomm i wiedząc, że zasada działania systemu GLOBALSTAR pochodzi w zasadzie z tego samego ośrodka, należy przypuszczać, że schemat części nadawczej należy uzupełnić o układ przeplotu oraz układ repetycyjny znajdujące się pomiędzy koderem a układem mnożącym przez ciąg Hadamarda. Pierwszy z nich przy współpracy z układem rozplotu w odbiorniku przyczynia się do tego, że błędy paczkowe powstające w kanale transmisyjnym są rozpraszane przez układ rozplotu, dzięki czemu w odbiorniku jest możliwe efektywne dekodowanie korekcyjnego kodu splotowego. Układ repetycyjny ma za zadanie wyrównać szybkość transmisji zależną od aktywności mówiącego. Równocześnie krotność powtarzania bitów jest wskaźnikiem obniżenia poziomu mocy generowanego sygnału. Dzięki temu zmniejsza się wkład sygnału

z danego połączenia do łącznej interferencji występującej w systemie. Efektywne i precyzyjne sterowanie mocą jest czynnikiem decydującym o pojemności całego systemu stosującego zasadę CDMA.



Rys.5.96. *Uproszczony schemat blokowy nadajnika i odbiornika systemu GLOBALSTAR (despreading oznacza operację odwrotną do rozpraszania)*

W odbiorniku następują operacje odwrotne do zrealizowanych w nadajniku. Dzięki metodzie CDMA w sposób naturalny jest możliwy odbiór zbiorczy, co jest szczególnie korzystne w procesie przejmowania połączenia od jednego satelity do drugiego *(handover).* Odbiór sygnałów z dwóch satelitów widzianych równocześnie zapewnia miękkie przejmowanie połączenia *(soft handover)* i jest realizowane za pomocą pojedyńczego układu radiowo - antenowego stacji ruchomej z zastosowaniem osobnych układów dekorelujących (za pomocą odwrotnej transformacji Hadamarda) i odbiornika RAKE. Sygnał z wyjścia odbiornika RAKE poddawany jest rozplotowi, dekodowaniu splotowemu i dekodowaniu mowy.

Sposób nawiązywania połączenia przez terminal ruchomy, który jest realizowany w systemie GLOBALSTAR wynika z transparentności systemu satelitarnego.

Po włączeniu zasilania terminal ruchomy usiłuje włączyć się do sieci naziemnej. Jeśli działanie to kończy się powodzeniem, zostaje w niej zarejestrowany

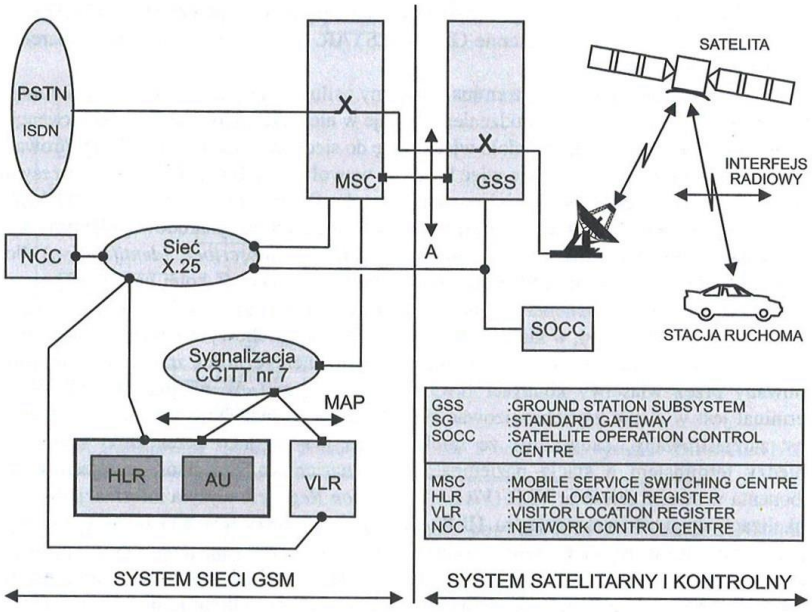
i w konsekwencji może z niej korzystać. Jeśli nie udało włączyć się do sieci naziemnej, usiłuje zarejestrować się w sieci satelitarnej. Poszukuje więc kanałów wywoławczych i za ich pomocą przesyła sygnał satelicie z żądaniem umiejscowienia w określonym kanale (w sensie CDMA) i rejestracji. Terminal ruchomy przesyła także swój sygnał międzynarodowej identyfikacji abonenta ruchomego (IMSI - *International Mobile Subscriber Identification)* do naziemnej stacji sterowania SSC *(Satellite Station Controller).* Z kolei następuje proces obliczenia lokalizacji abonenta ruchomego i sprawdzenie jego danych w rejestrze HLR *(Home Location Register),* w których dane te na stałe są przechowywane. Po wyznaczeniu pozycji terminala ruchomego, potwierdzeniu jego autentyczności zostaje on poinformowany przez właściwy kontroler SSC o jego rejestracji. W wyniku tej informacji terminal jest w stanie zsynchronizować się z kanałem sygnalizacyjnym stacji, w której jest zarejestrowany. Zauważmy, że satelity służą jedynie jako przekaźniki łączności między terminalem a stacją naziemną. Stacja naziemna SSC, która zarejestrowała abonenta w swoim rejestrze VLR *(Visitor's Location Register)* wysyła informację o jego lokalizacji do właściwego rejestru HLR. Od tej chwili wszystkie wywołania abonenta mogą być kierowane za pośrednictwem sieci PSTN, stacji naziemnej SSC i pośredniczącego satelity do abonenta zgodnie z procedurami takimi jak w sieciach naziemnych. Tak więc sieć satelitarna może być zintegrowana z naziemnymi sieciami komórkowymi poprzez tę samą zasadę numeracji, dostęp do usług oferowanych przez sieci itp.

Konfiguracja sieci systemu GLOBALSTAR opiera się na konfiguracji naziemnych sieci komórkowych. Dzięki niewielkiemu opóźnieniu wprowadzanemu przez system satelitarny można zachować bez zmiany protokoły i systemy sygnalizacji stosowane w naziemnych sieciach komórkowych. Podobnie jak to jest w przypadku sieci komórkowych definiuje się analogiczne do występujących w nich styki:

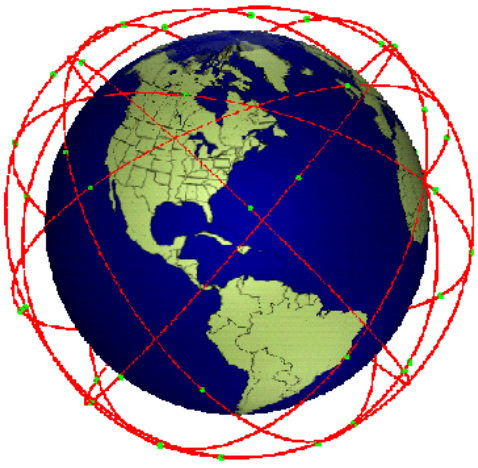
- styk radiowy pomiędzy terminalem ruchomym, satelitą i stacją kontroli naziemnej,
- styk pomiędzy stacją SSC i centralą w publicznej sieci radiokomunikacji ruchomej,
- styk związany z protokołem wymiany informacji pomiędzy centralą radiokomunikacyjną a bazami danych zarządzania systemem terminali ruchomych.

Na rysunku 5.97 przedstawiono uproszczoną architekturę stacji SSC w połączeniu z fragmentem sieci radiokomunikacji naziemnej (np. GSM). Widzimy, że

właściwa naziemna stacja systemu GLOBALSTAR komunikuje się poprzez podsystem układów naziemnych z centralą systemu radiokomunikacji lądowej, w której przez sieć pakietową X.25 oraz sygnalizację SS7 następuje wymiana danych z rejestrami HLR, VLR i AU (potwierdzenie autentyczności). Przez centralę systemu radiokomunikacji ruchomej jest możliwe przejście do sieci PSTN a przez nią ewentualnie do innej SSC i zarejestrowanego w niej abonenta.



Rys.5.97. *Uproszczona architektura stacji SSC systemu GLOBALSTAR*



Rys.5.98. *Konstelacja satelitów Globastar*

Projekt systemu GLOBALSTAR zakłada, że każdy satelita będzie w stanie realizować 2000 do 3000 kanałów głosowych. Zgodnie z opisaną procedurą dwustopniowego włączania się do sieci radiokomunikacyjnej z pierwszym stopniem w postaci próby rejestracji w sieci radiokomunikacyjnej naziemnej, teminale muszą być dwu-modowe. Pierwszy mod (tryb) pracy to praca w sieci naziemnej (np. GSM), natomiast drugi to praca w trybie GLOBALSTAR. Terminale będą miały postać radiotelefonu ręcznego.

5.6.5.3.2. Oferowane usługi

System Globalstar oferuje swoim użytkownikom wysoka jakość oraz niezawodność usług transmisji sygnałów mowy oraz transmisji danych. Nawet klienci korzystający z mobilnych terminali satelitarnych o niskiej mocy mogą oczekiwać cyfrowej jakości głosu, porównywalnej z sieciami komórkowymi. Biorąc pod uwagę prędkość poruszania się oraz liczbę satelitów na orbitach, braki zasięgu są minimalne i zazwyczaj czas ich trwania nie przekracza kilku minut. Wysoka jakość połączeń jest uzyskiwana dzięki temu, że terminale utrzymują bezpośrednie połączenia z maksimum trzema satelitami jednocześnie, a te z kolei komunikują się z najbliższą bramą naziemną. Dodatkowo wykorzystywana jest opatentowana metoda odbioru sygnału Path Diversity™, która dzięki odbiorowi sygnałów z kilku satelitów, pozwala na znaczącą redukcje opóźnień w transmisji i podniesieniu jej jakości. Metoda ta zmniejsza ryzyko zerwania połączenia, nawet w środowisku miejskim. Duża liczba satelitów na orbicie LEO gwarantuje, że w przypadku chwilowej awarii jednego z nich, sąsiednie mogą szybko go zastapić, bez znaczących strat w zasięgu działania systemu.

Obok usługi transmisji sygnałów mowy w systemie funkcjonuje usługa poczty głosowej oraz przekierowywania połączeń. Niektóre modele terminali umożliwiają również określenie swoich pozycji geograficznej, co może być szczególnie przydatne w przypadkach, gdy wymagana jest szybka pomoc.

5.6.5.3.3. Terminale

Terminale noszone obok realizacji usług transmisji sygnałów mowy umożliwiają poprzez opcjonalne przystawki, podłączenie komputerów przenośnych lub PDA do sieci Internet dzięki usłudze transmisji danych. Dostępne są również zestawy morskie i samochodowe, dzięki którym użytkownicy mogą korzystać ze swoich telefonów wewnątrz jachtów, samochodów i budynków.

Globalstar GSP-1700 Handheld Phone

GSP-1700 jest najmniejszym i najlżejszym (200g) terminalem noszonym systemu Globalstar, który dzięki ergonomicznej konstrukcji jest komfortowy i wygodny w użyciu. Przy użyciu opcjonalnego zestawu, można łatwo stworzyć kompletny system telefonii satelitarnej w samochodzie lub na statku. Terminal umożliwia też współprace z opcjonalnymi zestawami słuchawkowymi przewodowymi oraz bezprzewodowymi Bluetooth. Opcjonalny moduł pozwala również na podłączenie terminala z komputerem. Obok usługi cyfrowej transmisji sygnałów mowy o wysokiej jakości oraz transmisji danych z szybkością 9,6 kb/s, terminal umożliwia korzystanie z poczty głosowej oraz obsługę wiadomości SMS, e-mail oraz dostęp do Internetu. Ponadto dzięki usłudze lokalizacyjnej możliwe jest szybkie określenie położenia geograficznego terminala. Bateria wystarcza na użytkowanie telefonu przez czas do 4 godzin rozmów oraz do 36 h w trybie czuwania.

Rys.5.99. *Globalstar GSP-1700 Handheld Phone.*

Globalstar SAT-550 Handheld Phone

SAT-550 jest większy i cięższy (415g) od modelu GSP-1700, ale do jego zalet należy możliwość pracy zarówno w sieci Gloabalstar jak i w sieciach telefonii komórkowej

GSM 900 MHz. Telefon jest przyjazny dla użytkownika, jego obudowa jest solidna i zwarta, dzięki czemu łatwo go nosić i używać na morzu i na ladzie. Terminal umożliwia obsługę wiadomości SMS oraz transmisje danych z szybkością 9,6 kb/s. Dzięki dodatkowemu modułowi można do niego podłączyć komputer lub PDA i korzystać z dostępu do Internetu. Opcjonalny zestaw samochodowy umożliwia korzystanie z terminala w samochodzie lub wewnątrz budynków. Bateria wystarcza na

użytkowanie telefonu w trybie satelitarnym przez czas do 3,5 h rozmów oraz do 10 h w trybie czuwania oraz w trybie GSM przez czas do 9,5 h rozmów oraz do 83 h w trybie czuwania.

Rys.5.100. *Globalstar SAT-550 Handheld Phone.*

Globalstar GSP-1600 Handheld Phone

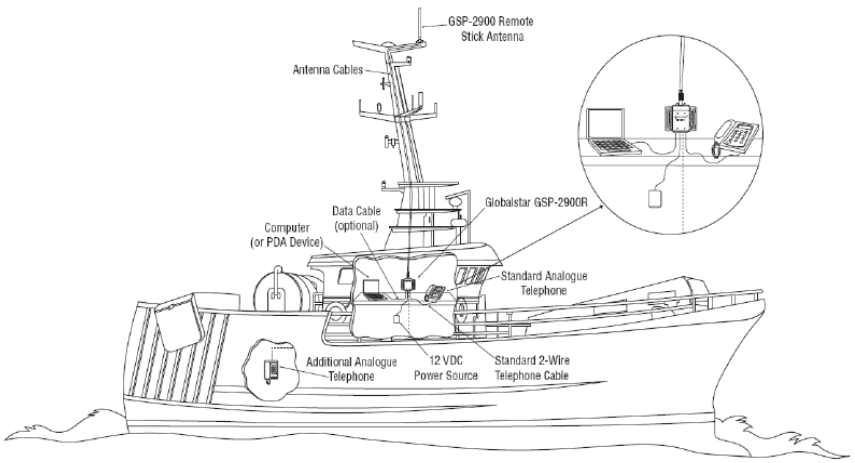
GSP-1600 to drugi dwumodowy terminal systemu Globalstar, który posiada możliwość pracy zarówno w sieci Gloabalstar jak i w sieciach telefonii komórkowej CDMA 800 (IS-95) i AMPS 800 (IS-41). Terminal umożliwia obsługę wiadomości e-mail oraz transmisje danych z szybkością 9,6 kb/s. Ponadto dzięki usłudze lokalizacyjnej możliwe jest szybkie określenie położenia geograficznego terminala. Dzięki dodatkowemu modułowi można do niego podłączyć komputer lub PDA i korzystać z dostępu do Internetu. Opcjonalny zestaw samochodowy umożliwia korzystanie z terminala w samochodzie lub wewnątrz budynków. Bateria wystarcza na użytkowanie telefonu w trybie satelitarnym przez czas do 3,75 h rozmów oraz do 19 h w trybie czuwania, w trybie CDMA 800 przez czas do 4,7 h rozmów oraz do 75 h w trybie czuwania oraz w trybie AMPS 800 przez czas do 2,8 h rozmów oraz do 15 h w trybie czuwania.

Rys.5.101. *Globalstar GSP-1600 Handheld Phone.*

Globalstar GSP-2900 Fixed Phone System

GSP-2900 jest terminalem stacjonarnym systemu Globalstar przeznaczonym dla użytkowników na lądzie i morzu. Terminal może być montowany bezpośrednio na pokładzie statku (na dachu), gdzie zapewniona jest bezpośrednia widoczność z satelitami, lub montowany pod pokładem (wewnątrz budynków) z wykorzystaniem zewnętrznej anteny. Terminal można podłączyć do większości systemów telefonicznych poprzez liniowe wejście analogowe RJ11 ze względu na kompatybilność ze standardowymi telefonami i automatycznymi sekretarkami. Terminal umożliwia obsługę poczty głosowej, przekierowywanie połaczeń, obsługę wielu telefonów oraz za pomocą dodatkowego adaptera i transmisje danych z szybkością 9,6 kb/s. Oprócz tego użytkownicy na morzu mogą wykorzystać ten terminal do komunikacji w relacji statek - ląd oraz do łączności w niebezpieczeństwie.

Rys.5.102. *Globalstar GSP-2900 Fixed Phone.*



Rys.5.103. *Przykład instalacji terminalu Globalstar GSP-2900 na jednostce pływającej.*

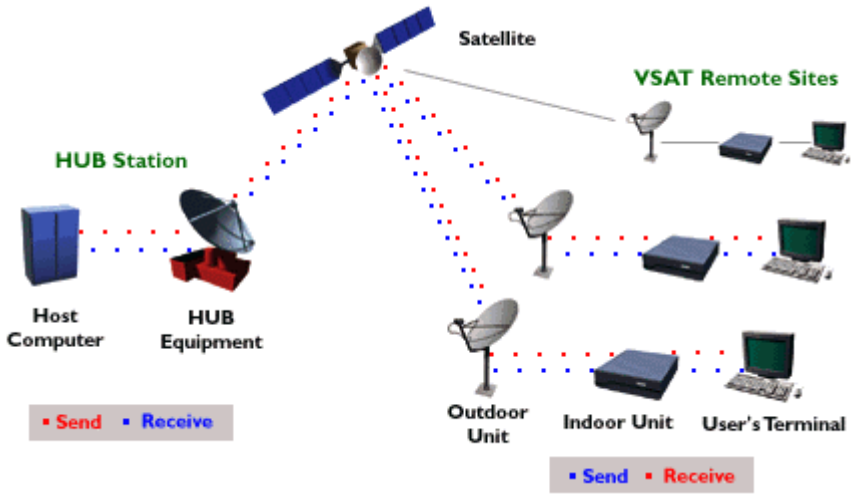
5.7.5.5. System VSAT

Zalecenie RS.725 ITU-R określa VSAT-y jako systemy łączności satelitarnej, gdzie terminale abonenckie mają niewielkie rozmiary - średnice anten nie przekraczają 2.4 metra. Obecnie trudno już mówić, że są to małe rozmiary anten. Nie jest to też żadna ścisła definicja systemów VSAT. Generalnie VSAT - y charakteryzują się tym, że:

- anteny terminali abonenckich mają rozmiary od 0.5 do 3 metrów średnicy,
- przepustowości w systemie zazwyczaj nie przekraczają 2 Mbps, a najczęściej jest to kilkadziesiąt kbit/s,
- często są to systemy zamknięte, ich przeznaczeniem jest przekazywanie specyficznych informacji wewnątrz pewnej firmy, organizacji.

Systemy VSAT zaczęły się intensywnie rozwijać w latach 80-tych. Ich nazwa - Very Small Aperture Terminals - pochodzi właśnie od małych rozmiarów terminali abonenckich. Większość abonentów systemów VSAT to mieszkańcy Ameryki Północnej, głównie USA, choć VSAT - y są coraz chętniej kupowane również w Europie. Obecnie, liczba terminali VSAT na świecie przekracza 500 tys. Coraz intensywniej zagospodarowywane są wysokie częstotliwości przeznaczone dla tych systemów. Większość systemów VSAT funkcjonuje w konfiguracji gwiazdy (*star*). Oznacza to, że wszystkie dane od terminali abonenckich przesyłane są przez satelity do stacji nadzorczych (bazowych) określanych w tych systemach mianem "*hub*". Dopiero w hubie zestawiane jest połączenie i dane są transmitowane dalej do punktu docelowego - na Ziemi lub przez kolejnego satelitę do innego terminala. Hub pełni też role nadzorcze i kontrolne w systemie oraz taryfikuje połączenia. Huby posiadają anteny o dużych rozmiarach, od 5 do 11 metrów średnicy. Inną konfiguracją jest "mesh" (pol. krata, oczko). W takim zestawieniu terminale komunikują się bezpośrednio przez satelitę, połączenia nie przechodzą przez huba. Z tego powodu konfiguracja ta określana jest często mianem "*hubless VSAT network*" - sieć VSAT bez stacji hub. Stacja nadzorcza może uczestniczyć w inicjalizacji połączenia, choć i to nie jest konieczne, a poza tym pełni funkcje kontrolne i ewentualnie taryfikacyjne. Połączenie terminali może przechodzić też przez łącze międzysatelitarne (ISL). Typowy terminal VSAT składa się z trzech części: jednostki wewnętrznej (*indoor unit*), zewnętrznej (*outdoor unit*) i anteny. Jednostka wewnętrzna przyłączona jest do urządzeń użytkownika (np.

komputer PC) i zapewnia mu interfejs sieciowy, dzięki czemu do sieci VSAT można podłączyć terminale pracujące na różnych protokołach. Najczęściej są to protokoły: BiSync, SDLC, X.25, Frame Relay. Poprzez częstotliwości pośrednie (*Intermediate Frequences*) jednostka wewnętrzna komunikuje się z jednostką zewnętrzną. Dalej sygnał przetwarzany jest na częstotliwości radiowe i poprzez antenę transmitowany do satelity.



Rys.5.104. *Budowa systemu VSAT* (rysunek ze strony firmy iSAT)

Segment kosmiczny systemów VSAT to satelity geostacjonarne. Każdy system to co najmniej kilka aktywnych satelitów i jeden zapasowy - na wypadek awarii jednego z działających. Transmisja danych w tych systemach odbywa się w pasmach częstotliwości **C**, **Ku** lub **Ka.** Aby możliwe było transmitowanie wielu sygnałów (informacji od wielu użytkowników) jednocześnie z satelity lub huba stosuje się techniki zwielokrotnienia dostępu (*multiple access*). Jest to zwielokrotnienie w dziedzinie:

- czasu - TDMA,
- częstotliwości - FDMA
- lub techniki z widmem rozproszonym - CDMA.

Wybór danej techniki zależy od ilości użytkowników systemu, świadczonych im usług oraz mocy i pasma dostępnych satelitom. Najczęściej stosuje się techniki TDMA. Jednocześnie gdy zastosuje się już zwielokrotnienie dostępu konieczny jest wybór metody przydzielania kanału pojedynczemu użytkownikowi.

Możliwy jest :

- stały przydział kanału (*Fixed Assignment Multiple Access*),
- losowy przydział kanału (*Random Assignment Multiple Access*),
- użytkownicy jednocześnie korzystają ze wspólnego medium, w przypadku kolizji dostępu konieczne są retransmisje,
- przydział kanału na żądanie (*Demand Assignment Multiple Access*).

Decyzja, którą z powyższych technik wybrać zależy głównie od statystyki ruchu w sieci, wymaganych parametrów (opóźnienia, obciążenie sieci) i kosztów przeznaczonych na wdrożenie i utrzymanie techniki. Ze względu na rodzaj świadczonych usług systemy VSAT można dzielić na :

- systemy rozgłoszeniowe (*broadcasting, data distribution*) - informacja jest transmitowana tylko od stacji bazowej do terminali abonenckich. Nie ma możliwości transmisji w kierunku przeciwnym. W ten sposób mogą działać systemy w obrębie jednej firmy, gdzie istnieje konieczność regularnego przesyłania pewnych informacji (np. cenniki, oferty handlowe, bazy danych o produktach lub klientach) z centrum firmy do jej oddziałów i placówek. Na zasadzie transmisji jednokierunkowej mogą też działać systemy rozprowadzające sygnał telewizyjny, jednak wyłącznie w obrębie danej firmy lub grupy firm. Satelitarnych sieci telewizji publicznej nie zalicza się do systemów VSAT.
- systemy gromadzące informacje (*data gathering systems*) - również transmisja tylko w jednym kierunku - terminale abonenckie wysyłają informacje do stacji nadzorczej np. wysyłanie informacji o dokonanych transakcjach lub przesyłanie zleceń ich wykonania. Taki układ sieci jest jednak rzadko stosowany, jako że w tym przypadku stacja nadzorcza nie możliwości sprawowania kontroli nad podległymi jej terminalami abonenckimi. Dlatego też tego typu sieci realizuje się zazwyczaj jako sieci z komunikacją dwukierunkową.
- systemy dialogowe - interaktywne (*two-way systems*) - informacje wymieniane są w dwóch kierunkach. Jest to rozwiązanie zdecydowanie najczęściej stosowane. Przykładami mogą być rozmowy telefoniczne, przesyłanie faksów, połączenie telekonferencyjne czy też weryfikacja pewnych informacji np. handlowych.

Firma chcąca zostać operatorem systemu VSAT w pewnym regionie musi wydzierżawić satelitarny kanał radiowy (lub jego część) od firmy będącej właścicielem satelity. Po wybudowaniu swojej stacji nadzorczej może zacząć sprzedawać (lub dzierżawić) terminale VSAT i świadczyć w ten sposób usługi klientom. Instytucjami potencjalnie zainteresowanymi tego typu usługami mogą być :

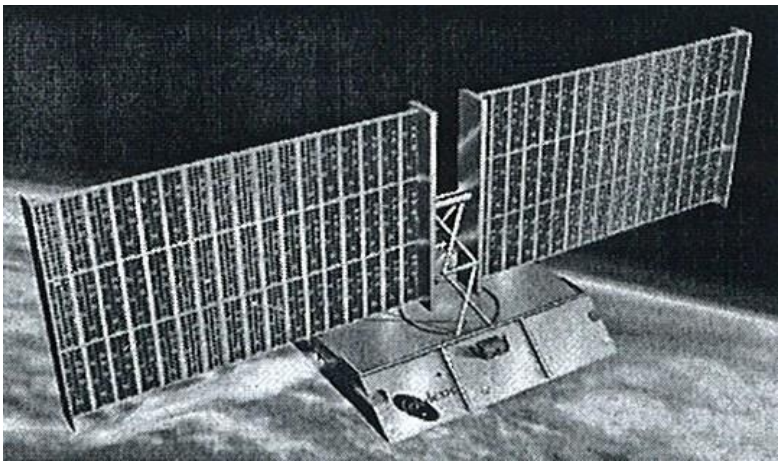
- sieci sklepów,
- banki lub inne instytucje handlowe,
- organizacje dozoru meteorologicznego, ekologicznego bądź sejsmologicznego,
- służby ratownicze,
- urzędy administracji państwowej,
- towarzystwa ubezpieczeniowe,
- agencje informacyjne, reklamowe i turystyczne.

Satelitów, które mogą świadczyć usługi VSAT jest dużo. Dane pochodzące jeszcze z roku 1992 mówią o ponad 150 satelitach. Z bardziej znanych, przynajmniej w Europie, można wymienić serie Eutelsat, Intelsat, Astra czy Telecom. W Polsce dostęp do systemów VSAT oferuje kilku operatorów; Telekomunikacja Polska S.A., Bankowe Przedsiębiorstwo Telekomunikacyjne Telbank S.A. (obecnie część grupy Exatel S.A. (polski operator telekomunikacyjny), Powszechna Agencja Informacyjna PAGI S.A. i inni.

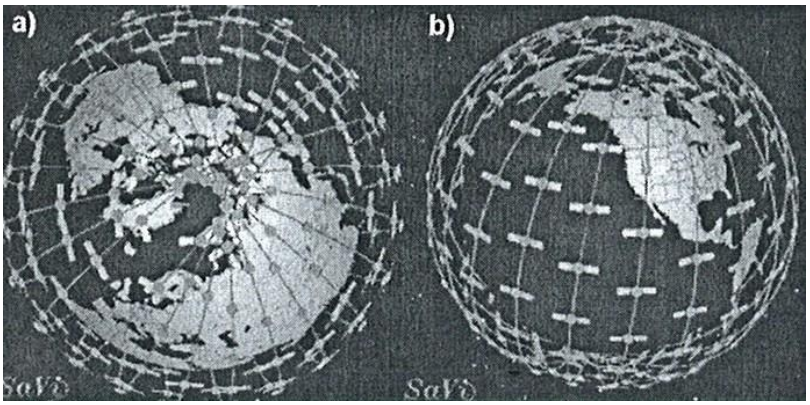
Rys.5.105. *Stacja VSAT w Porębach Leśnych*

5.7.5.6. System TELEDESIC

Teledesic jest jedną z ciekawszych propozycji satelitarnych systemów multimedialnych. Charakterystycznymi cechami systemu są duża pojemność, stacjonarne komórki, adaptacyjne marszrutowanie, zakres częstotliwości 20/30 GHz. Początkowo (rok 1990) zakładano, że człon kosmiczny systemu będzie się składać z 840 satelitów aktywnych i 84 satelitów zapasowych umieszczonych równomiernie na 21 orbitach o wysokości około 700 km i kącie inklinacji 98,16°. W roku 1998 zmieniono konstelację satelitów. Obecnie uważa się, że będzie złożona z 288 satelitów aktywnych (rys.5.106) rozmieszczonych równomiernie na 12 orbitach o wysokości 1350 km (rys.5.107).

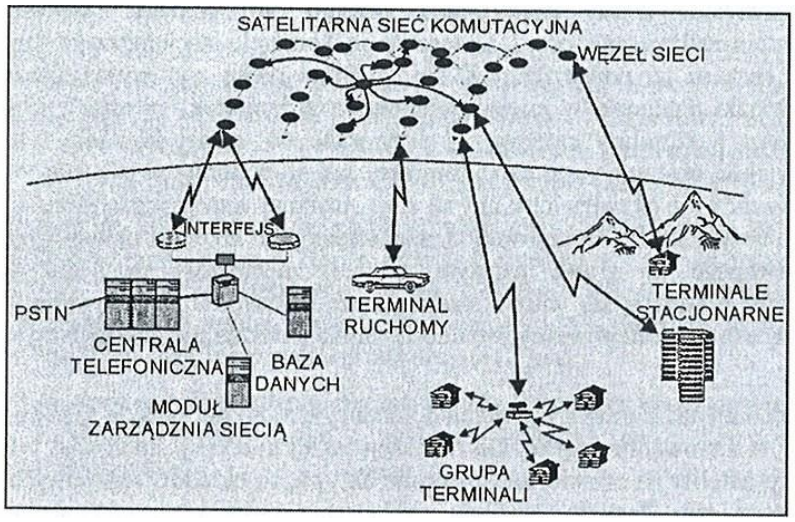


Rys.5.106. *Satelita systemu Teledesic*



Rys.5.107. *Konstelacje satelitów systemu Teledesic:*
a) widok w płaszczyźnie równika
b) widok wzdłuż osi Ziemi

Na rysunku 5.108 przedstawiono poglądowo architekturę systemu Teledesic. Stosuje się tu szybką komutację pakietów, podobną do ATM. Każdy rodzaj komunikacji jest traktowany jako strumień pakietów o ustalonej długości. Pakiet zawiera nagłówek z adresem, bity kontrolne oraz bity informacyjne. Długość pakietu ma wynosić 512 bitów, co nie jest zgodne ze standardem ATM (53 bajty). Pomiędzy siecią Teledesic i naziemnymi użytkownikami końcowymi będzie musiała nastąpić konwersja. Terminale będą konwertować standardowe protokoły naziemne, takie jak: IP, ATM, Frame Relay z/i na specyficzny format pakietów sieci wewnętrznej systemu Teledesic.



Rys.5.108. *Architektura satelitarnego systemu multimedialnego Teledesic*

Każdy satelita jest węzłem komutacyjnym połączonym z ośmioma satelitami: czterema na tej samej orbicie (dwa wcześniejsze i dwa późniejsze) i po jednym na każdej z dwóch sąsiednich orbit (rys.5.126). Układ połączeń ma formę siatki i zapewnia konfigurację sieci odporną na awarie i lokalne przeciążenia. Zmiany natężenia ruchu telefonicznego w sieci powodują ustawianie się kolejek pakietów na satelitach, co wydłuża czas oczekiwania na retransmisję do następnego satelity. Ten, jak i inne czynniki są brane pod uwagę przy zestawianiu połączenia. Decyzje są podejmowane w każdym węźle komutacyjnym (satelicie) stosując adaptacyjny algorytm marszrutowania. Algorytm ten korzysta z informacji rozprzestrzenianej w sieci przez każdego satelitę, na podstawie której określa się obciążenie sieci i dokonuje wyboru trasy o najmniejszym opóźnieniu. Pakiety tego samego połączenia mogą podążać różnymi drogami przez sieć. Każdy węzeł niezależnie marszrutuje pakiet wzdłuż trasy, która aktualnie oferuje najmniejsze opóźnienie do miejsca przeznaczenia. Terminal lub

adapter w miejscu docelowym, jeśli jest taka potrzeba, porządkuje pakiety by wyeliminować efekty opóźnień czasowych. Rozległe i szczegółowe badania sieci i algorytmu marszrutowania wykazują, że dla długiej trasy całkowite opóźnienie między punktami końcowymi jest często mniejsze niż w naziemnym połączeniu światłowodowym tych samych punktów.

System obsługuje przede wszystkim terminale stacjonarne, możliwa jest także obsługa terminali przewoźnych. Terminale stacjonarne nie są ograniczone mocą lub rozmiarem anteny. Terminale stacjonarne wykorzystują kanał o podstawowej przepływności 16 kb/s i dodatkowo 2 kb/s do sygnalizacji i sterowania. Mogą one być multipleksowane do przepływności 2 Mb/s. Podstawowa przepływność zapewnia jakość kodowania mowy taką jak w naziemnych systemach cyfrowych (64 kb/s). Zwielokrotnienie przepływności kanału podstawowego umożliwia tworzenie kanałów *n* x 64 kb/s i realizację usług ISDN.

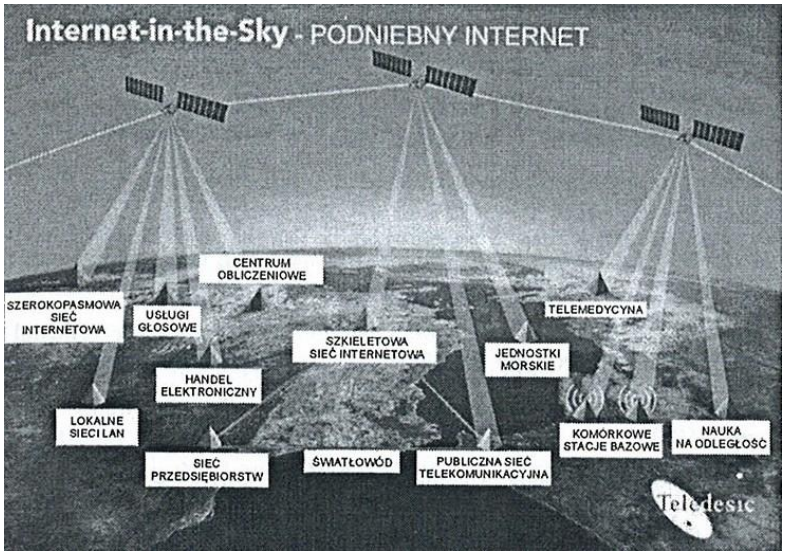
Terminale stacjonarne są wyposażone w anteny o średnicy około 25 cm, ustawione w ustalonej pozycji. Należy się spodziewać, że przeważająca liczba stacjonarnych terminali będzie połączona ze standardową siecią telefoniczną lub siecią ISDN. Możliwe jest stosowanie terminala grupowego który umożliwia uzyskanie dostępu do sieci małym wsiom lub komunikację abonentów używających niedrogich telefonów bezprzewodowych.

Obszar pokrywany przez satelitę jest złożony z przylegających do siebie komórek, analogicznie jak w naziemnych systemach komórkowych. Wiązka antenowa satelitów przemieszcza się nad powierzchnią Ziemi z prędkością około 25 tys. km/h. Gdyby obszar komórki przesuwał się wraz, z wiązką satelitarną, to terminal pozostałby w niej zaledwie przez kilka sekund, a częste , przekazywanie rozmów zwiększyłoby koszty użytkowania systemu. W systemie Teledesic przekazywanie rozmów jest zminimalizowane przez zastosowanie komórek stacjonarnych przypisanych do określonego obszaru na powierzchni Ziemi. Podczas ruchu nad powierzchnią Ziemi satelita kieruje swoje wiązki antenowe w miejsca stacjonarnych komórek, wewnątrz jego obszaru pokrycia. Częstotliwości i szczeliny czasowe są przypisane do każdej komórki przydzielane przez satelitę aktualnie obsługującego daną komórkę. Jak długo terminal pozostaje w obszarze komórki, tak długo zachowuje przydzielony mu na czas rozmowy kanał, niezależnie od tego przez ile satelitów będzie w tym czasie

obsługiwany. Małe, stacjonarne komórki umożliwiają ograniczenie obszaru obsługiwanego do granic państwa, co jest niemożliwe przy dużych komórkach lub komórkach, które poruszają się wraz z satelitą. Baza danych komórki zawarta każdym satelicie, określa rodzaj usług, które powinny być udostępnione na aktualnie obsługiwanym, obszarze. Zastosowanie naziemnych stacjonarnych komórek bazuje na dokładnej znajomości pozycji satelity i jego orientacji oraz precyzyjnym sterowaniu wiązką. Do realizacji takiej koncepcji konieczne jest automatyczne określanie pozycji satelity na orbicie, zastosowanie aktywnych układów antenowych, wykorzystanie metod zwielokrotnienia dostępu, szybkie przełączanie pakietów i adaptacyjne marszrutowanie.

Dla systemu Teledesic zarezerwowano dwa pasma częstotliwości o szerokości 500 MHz w zakresie **Ka**: 18,8 GHz dla łącza od satelity do terminala *(downlink)* i 28,6 - 29,1 GHz dla łącza od terminala do satelity *(uplink)*.

System Teledesic świadczy rozmaite usługi (rys.5.109).



Rys.5.109. *Usługi w systemie Teledesic*

Wykorzystywana, biorąca udział w wymianie informacji, sieć globalna – dostarcza połączeń z dużą szybkością do sieci przedsiębiorstw, sieci korporacyjnych, oddziałów biur i do pracowników dostępnych poza obszarem działania Intranetów.

• Łańcuch sieci dostawców - wzrost planowania zasobów przedsiębiorstw zachęca użytkowników biznesowych do użycia technologii powodującej wzrost wydajności w szerokim układzie wewnętrznych procesów od produkcji do finansów. Biznesmeni

sięgają po połączenia swoich sieci, aby mieć szybszy kontakt zarówno z dostawcami, partnerami jak i klientami. Teledesic otwiera dostawę do „łańcuszka" zachowując wysoki poziom integracji szybszy niż był do tej pory.

• Dostęp do Internetu - o ile szybkość transmisji i zastosowanie światłowodowych kabli pomiędzy głównymi centrami miejskimi gwałtownie wzrasta, o tyle „ostatnia mila" w połączeniach do biur i domów pozostaje dotkliwie wolna. System Teledesic dostarcza szerokopasmowy dostęp bezpośrednio do zainteresowanych biznesmenów i organizacji życzących sobie drogi obejściowe do istniejących sieci lokalnych wprowadzających korki.

• Połączenia morskie - usługi te dostarczają liniowcom oceanicznym, tankowcom i innym statkom zabezpieczeń niezawodnych i szybkich połączeń do naziemnych sieci i systemów danych przedsiębiorstw.

• Telemedycyna, handel elektroniczny, wideokonferencje, nauka na odległość; szerokopasmowe aplikacje wymagające interaktywnego wzajemnego oddziaływania.

System Teledesic ułatwi tym i innym aplikacjom wysoki poziom jakości, ochrony i niezawodności.

W zależności od zapotrzebowania odbiorcy na rozmaitość i - co jest nowością - jakość oferowanych usług, dynamicznie będzie przydzielana odpowiednia liczba kanałów transmisyjnych. Wiąże się to również z bilingowaniem połączeń, klient płaci za rzeczywiste wykorzystanie łącza.

6. Bezpieczeństwo systemów łączności (teleinformatycznych)

6.1. Wprowadzenie

Punkt ten opracowano głównie na podstawie publikacji *„Podstawy bezpieczeństwa systemów informatycznych"* autorstwa Pana Mariana Molskiego [28]. Chronimy swoje mieszkania upewniając się każdorazowo przed ich opuszczeniem, czy pozostawiamy je zamknięte, często sprawdzając także, czy wyłączyliśmy odbiorniki energii elektrycznej, piecyki gazowe i krany. Zanim pozostawimy samochód na ulicy, włączamy system alarmowy. Większej gotówki nie przechowujemy **w** domu, powierzając ją bankowi. Wszystko to traktujemy jako zabiegi naturalne, niebudzące niczyjego zdziwienia.

Pytanie - czy chronisz należycie informacje, w szczególności te przechowywane w systemach komputerowych - niejednego może zdziwić. Niestety, stan świadomości społeczeństwa w tej dziedzinie na początku XXI wieku nie jest najwyższy. Zdobycie dziś ważnej informacji kosztuje, lecz jej utrata może kosztować jeszcze więcej. A ile może przedsiębiorstwo kosztować modyfikacja informacji w rzeczywistości będąca dezinformacją? Jak kosztowne może być niepożądane ujawnienie informacji?

Systemy i sieci komputerowe (teleinformatyczne) wraz z całym „dobrodziejstwem inwentarza" wniosły w dziedzinę przetwarzania informacji niebezpieczeństwo zniszczenia, modyfikacji i ujawnienia informacji przez świadomego intruza atakującego system lub w wyniku katastrofy bądź pomyłek personelu obsługującego system komputerowy. Taka jest niestety, cena nowoczesności. Od kilku lat zagadnienia bezpieczeństwa komputerów (ang. **computer security, CS)** lub inaczej bezpieczeństwa informacji *(*ang. **information security, IS)** nabierają coraz większego znaczenia. *Zdaniem wielu ekspertów wiedza jest najlepszym zabezpieczeniem systemów komputerowych.* Kursy, szkolenia, studia, dobre podręczniki oraz instrukcje na pewno stanowią „warstwę ochronną" przed zagrożeniami i atakami systemów komputerowych. Stąd właśnie w tym opracowaniu, przedstawiony zostanie w sposób elementarny, a jednocześnie w miarę kompleksowy wprowadzi uczestników kursu w zagadnienia bezpieczeństwa systemów i sieci komputerowych wykorzystywanych w przestrzennych systemach przetwarzania danych. Warto w tym miejscu podać kilka faktów i danych liczbowych, by zdać sobie sprawę ze znaczenia tej problematyki:

- CIA i Departament Obrony USA utworzyły przy Narodowej Radzie Bezpieczeństwa ośrodek do spraw ataków komputerowych.
- W Polsce opracowano i wdrożono ustawy o ochronie danych osobowych i ochronie informacji niejawnych.
- System Pentagonu atakowany jest z zewnątrz ponad 500 razy dziennie.
- Zaistniał termin „infoterroryzm"; możliwe jest dzisiaj zdalne atakowanie systemów komputerowych za pomocą „armat" typu HERF (ang. *High Energy Radio Frequence*) oraz „bomb" typu EMPT (ang. *Electromagnetic Pulse Transformation*); zarówno „armaty" HERF i „bomby" EMPT mogą spowodować katastrofalne zakłócenia w pracy systemu komputerowego lub jego unieruchomienie.

- Stan zabezpieczeń oceniany statystycznie jest fatalny (tab.6.1) - 23% użytkowników ma łatwe do odgadnięcia hasła, a 21% nie ma żadnych haseł.
- W Internecie stosuje się tzw. diabelskie pakiety, np. „telefonicznego wojownika", zestawy do łamania haseł, podręczniki pirata i hakera, laboratoria do tworzenia wirusów itp.

Tabela 6.1. Ilustracja fatalnego stanu zabezpieczeń komputerów *(Computerworld)*

Zagrożenie	Stopień zagrożenia
Użytkownik rzadko zmienia hasła	**85%**
Użytkownik ma łatwe do odgadnięcia hasła	**23%**
Brak w systemie jakichkolwiek haseł	**21%**
Nieaktywne konta w systemie	**14%**

- Polscy hakerzy i specjaliści do spraw zabezpieczeń informacji twierdzą, że polskie firmy lekkomyślnie traktują swoje zasoby informacyjne.
- W polskich przedsiębiorstwach dominuje często pogląd, że wydatki na zabezpieczenia są zbędne; zawsze znajdą się „ważniejsze" cele.
- Zdaniem polskich hakerów, w Polsce nie trzeba zatrudniać szpiegów gospodarczych i politycznych; wystarczy wiedza, komputer i modem.
- Umiejętności bezrobotnych informatyków zwolnionych z zakładów zbrojeniowych byłego ZSRR wykorzystuje ponoć rosyjska mafia.
- Hakerzy ostatnio, kilkukrotnie zaatakowali stronę informacyjną lotnictwa wojskowego USA w WWW sieci Internet i udało się im zamieścić tam treści pornograficzne i obraźliwe opinie na temat rządu USA (doniesienia PAP).
- Program SATAN (ang. *Security Analysis Tool for Auditing Networks)* służący do wykrywania włamań w sieci Internet jest wykorzystywany przez hakerów właśnie do penetracji w sieci Internet.

Arbitralne zestawienie istniejących zagrożeń dla informacji powinno nas skłonić do zadania pytania: **Kiedy, co, jak, przed kim i za ile chronić?** Najłatwiej odpowiedzieć na człon pytania „kiedy". Myślenie o bezpieczeństwie systemu

komputerowej powinno zaczynać się już w momencie podjęcia decyzji o komputeryzacji przedsiębiorstwa lub instytucji. Odpowiedzi, na pozostałe człony pytania (co, jak, przed kim i za ile) zostaną wyjaśnione w dalszej części opracowania.

6.2. Pojęcia podstawowe

Zagadnienia dotyczące bezpieczeństwa systemów informatycznych, jak już wspomniano, są coraz bardziej dostrzegane i zyskują na znaczeniu, aczkolwiek w węższym sensie znane były wcześniej, niemalże od początku rozwoju informatyki. Jak zwykle, terminologia ciągle się rodzi, ulega modyfikacjom, postuluje się jej normalizację. Niewątpliwie trzy bardzo bliskoznaczne pojęciowo terminy w języku angielskim dominują. Chodzi tu o *security, safety* oraz *protection.* Według „Wielkiego słownika angielsko-polskiego" (J. Stanisławski), dwa pierwsze słowa bliższe są znaczeniu bezpieczeństwo, a trzecie słowo oznacza ochronę. W literaturze krajowej często zamiennie używa się terminów bezpieczeństwo informacji oraz ochrona informacji (danych). Nie będziemy w tym miejscu zastanawiali się nad zakresem pojęciowym obu terminów mając nadzieję, że opracowywane normy państwowe (branżowe) ujednolicą precyzyjnie terminologię.

Zwróćmy w tym miejscu jedynie uwagę na sygnalizowaną wcześniej kolizję terminologiczną między pojęciami bezpieczeństwo a ochrona. Według Hoffmana **bezpieczeństwo informacji** polega na jej **ochronie** przed przypadkowym lub umyślnym zniszczeniem, ujawnieniem lub modyfikacją zaś według Dorothy Denning - **ochrona informacji** zajmuje się metodami **zabezpieczania** informacji przed nie upoważnionym dostępem i zmianami informacji w systemach komputerowych. Wyraźnie widoczne jest definiowanie jednego pojęcia za pomocą drugiego i odwrotnie. Być może, jest to efekt tłumaczenia literatury obcojęzycznej przy braku obowiązujących standardów terminologicznych. Do dziś, zresztą autorzy różnych publikacji, szkoleń i instrukcji pisząc (mówiąc) o tym samym stosują różne terminy, gdyż w jakiś sposób zostaliśmy ukształtowani przez podstawowe źródła bibliograficzne.

Często za podstawę ustaleń standaryzacyjnych w dziedzinie terminologii z zakresu CS (ang. *Computer Security)* oraz IS (ang. *Information Security)* przyjmuje się definicje Narodowego Biura Standardów i Stowarzyszenia do Spraw Urządzeń Obliczeniowych ACM (ang. *Association for Computing Machinery).*

Oprócz cytowanej już definicji bezpieczeństwa można znaleźć tam definicje środków bezpieczeństwa, poufności, tajności oraz nienaruszalności.

- **Środki bezpieczeństwa** to zabezpieczenia technologiczne i administracyjne które można zastosować do komputerów, programów i danych w celu zapewnienia ochrony interesów przedsiębiorstw oraz poufności indywidualnej.
- **Poufność** to prawo jednostki do decydowania o tym, jakimi informacjami chce się podzielić z innymi ludźmi i jakie jest skłonna od nich przyjąć.
- **Tajność** to atrybut danych opisujących stopień ochrony, której mogą one podlegać, uzgodniony przez osoby lub organizacje otrzymujące te dane.
- **Nienaruszalność danych** to cecha określająca, że dane nie różnią się od danych źródłowych i nie zostały przypadkowo lub umyślnie zmienione, ujawnione lub zniszczone.

Przy omawianiu zagadnień związanych z kryptografią klasę podstawowych pojęć poszerzymy o kolejne - **uwierzytelnienie** (ang. *authentication),* **integralność** *(*ang. *integrity),* **niezaprzeczalność** *(*ang. *non-repudiation).*

Według D. E. Robling Denning, zagadnienia związane z ochroną danych obejmują:

- sterowanie szyfrowaniem,
- sterowanie dostępem,
- sterowanie przepływem informacji,
- sterowanie wnioskowaniem,
- procedury składowania (archiwizowania) i odzyskiwania danych.

Ten podział często narzuca (sugeruje) autorom opracowań strukturę metodyczną tematyki związanej z bezpieczeństwem systemów informatycznych. W pewnym sensie ma to swoje odbicie w niniejszym opracowaniu.

Zagadnienia będące przedmiotem naszych rozważań mają punkty styczności takimi dziedzinami, jak np. *niezawodność (*ang. *reliability), analiza ryzyka (*ang. *risk analysis), przestępczość komputerowa (*ang. *computer crime), kryptologia* (*cryptology), kompatybilność elektromagnetyczna* (ang. *electromagnetic compatibility)* itd. Należy o tym zawsze pamiętać, choćby wtedy gdy np. przyjdzie nami wybierać interdyscyplinarny zespół do spraw bezpieczeństwa komputerowego

w przedsiębiorstwie lub tzw. sztab kryzysowy w przypadku wykrycia przestępstwa (ataku) komputerowego.

Podstawą bezpiecznego działania systemu informatycznego w przedsiębiorstwie winien być formalny dokument akceptowany przez dyrekcję, zwany **programem bezpieczeństwa lub polityką bezpieczeństwa** *(*ang. *security policy)* i opisujący reguły tworzenia i użytkowania bezpiecznego systemu.

6.3. Przestępczość komputerowa

6.3.1. Określenie przestępczości komputerowej

Komputeryzacja zrodziła zupełnie nie pożądane przez twórców komputerów zjawisko - przestępstwo komputerowe w rozmaitych odmianach. Przestępstwa komputerowe pojawiły się wraz z powstaniem komputerów drugiej generacji, choć – ze względu na trudności w ich programowaniu - nie mogły się wówczas upowszechnić. Wzrost przestępczości komputerowej należy raczej kojarzyć z komputerami trzeciej generacji, to jest z drugą połową lat sześćdziesiątych. Jeszcze w latach siedemdziesiątych wielu ekspertów, autorów i naukowców bagatelizowało znaczenie tych przestępstw.

Według Siebera (ekspert w dziedzinie ochrony informacji, autor podręczników o przestępczości komputerowej), **przestępczość komputerowa to wszelkie bezprawne, nieetyczne i nie upoważnione zachowania odnoszące się do procesu przetwarzania i (lub) przekazywania danych.**

Cornwall (również ekspert d/s bezpieczeństwa informacyjnego), dzieli przestępstwa komputerowe na cztery zasadnicze grupy:

1. niemożliwe do dokonania poza środowiskiem komputerowym (np. zamachy na ośrodki obliczeniowe, kradzież materiałów eksploatacyjnych),
2. ułatwione przez komputery (np. fałszerstwa, kradzież informacji, podsłuch),
3. popełniane przy biernym udziale komputerów (np. oszustwa, szkody w interesach gospodarczych oraz prywatnych),

4. dokonywane przez zawodowych przestępców z wykorzystaniem komputerów (np. nadzór interesów, zacieranie śladów).

6.3.3. Haker, cracker, phreaker

W żargonie informatycznym słowa haker i cracker stały się międzynarodowymi określeniami osób włamujących się do systemu komputerowego. Nazywa czasami cyberpunkami (USA), piratami (Francja) lub technopatami. Określenia ***cracker*** i ***hacker*** są w języku angielskim bliskoznaczne - *to crack* znaczy trzaskać powodować pęknięcia, rozłupywać, natomiast *to hack* znaczy ciąć, rąbać, pokiereszować.

W literaturze usiłuje się czasami w sposób dość płynny i umowny rozróżnić terminy. Przyjmuje się, że **haker** to osoba próbująca poznać techniczne aspekty systemu, natomiast **cracker** to ktoś usiłujący złamać zabezpieczenia systemu. Opinie o tych grupach intruzów komputerowych ewoluują od zachwytów (pasjonat, entuzjasta, człowiek zafascynowany techniką) do zabarwień pejoratywnych. Dla psychologów i socjologów haker jest człowiekiem socjalnie nieprzystosowanym, ponieważ wręcz obsesyjnie stawia towarzystwo komputerów przed ludzkim, a wspólną cechą hakerów jest osamotnienie i brak akceptacji społecznej.

Działalność hakerów to nie tylko złe strony. Ich udane ataki na systemy terowe zmuszają projektantów do szukania nowych i lepszych zabezpieczeń, się dosyć często, że bardzo młodych hakerów zatrudnia się jako ekspertów im testowanie skuteczności zabezpieczeń wszelkich systemów, w których bezpieczeństwo informacji ma znaczenie szczególne (wojsko, policja, banki). Haker ukrywa się pod fantazyjnymi pseudonimami, gdyż anonimowość utrudnia jego śledzenie i ułatwia unikanie ryzyka odpowiedzialności karnej.

Jednym z etapów włamania do systemu jest procedura poszukiwania tajnego hasła użytkownika. Programy poszukujące hasła nazywa się skanerami (ang. *to scan* - przeglądać) lub sprinterami. Trzeba przyznać, że bardzo często te programy mają ułatwione zadanie, gdyż niefrasobliwość użytkowników komputera w dziedzinie tworzenia haseł jest ogromna, dlatego duże znaczenie ma właściwy wybór haseł.

Włamywacze stosują często dwie metody: tzw. sniffing i spoofing (ang. *to sniff*- wąchać, węszyć, wyczuwać; (ang. ***to spoof*** - naciągać, kantować, szachrować, oszukiwać).

Sniffing polega na podsłuchaniu haseł przesyłanych z terminalu do serwera.

Spoofing polega na oszukaniu serwera, do którego haker chce się włamać w taki sposób, aby serwer „myślał", że pakiety pochodzą od akceptowanych przez niego komputerów (terminali), a nie z pirackiego komputera. Przykładowo za spoofing można uznać piracki skrypt, który po uruchomieniu:

1. przerywa aktualną aplikację użytkownika,
2. wyświetla winietę systemu,
3. nakazuje użytkownikowi ponowne logowanie (logowanie – zameldowanie, meldowanie (ang. *log* – dziennik pokładowy, okrętowy),
4. prosi o podanie hasła (i przechwytuje je!),
5. informuje o awarii terminalu sugerując użytkownikowi, aby zmienił terminal.

Mało podejrzliwy użytkownik sądzi, że to tylko dziwne losowe zachowanie systemu, nie zgłasza tego faktu nikomu i nie zdaje sobie sprawy, że jego hasło bardzo łatwo zostało przechwycone.

Prekursorami dzisiejszych włamywaczy komputerowych byli frikerzy (ang. *phreaker),* którzy starali się wszędzie telefonować za darmo wykorzystując różne słabości central telefonicznych.

Nie dziwi już dziś to, że hakerzy mają swoje specjalistyczne pisma, np. 2600 - amerykański kwartalnik założony w 1984, wydawany w New Jeresy (osiągalny pod adresem PO BOX 752, Middle Island, New York, USA). Bez kłopotów i ograniczeń informacje specjalistyczne dla hakerów można znaleźć w Internecie.

Związek pomiędzy obiektami i sprawcami przestępstw zawierają tabele 6.2 i 6.3.

Tabela 6.2. Zależność między sprawcami a obiektami przestępstw

	Sprawcy przestępstw			
Obiekty przestępstw	**Pracownicy firmy**	**Wspólnicy i konkurencja**	**Przestępcy profesjonalni**	**Terroryści polityczni**
	Listy płac Listy premii Inwentarz Stan magazynów Sprzęt komputerowy Materiały eksploatacyjne Informacje do sprzedania osobom trzecim	Inwentarz Stan magazynów Plany rozwojowe Projekt zakupów Analizy i oceny Kosztorysy Lista klientów lista dostawców Plany finansowe Zamówienia Badania marketingowe	Inwentarz Gotówka Informacje do korupcji Informacje do szantażu Informacje kadrowe	Wszystkie elementy systemu, które pozwalają na unieruchomienie działalności firmy celem wymuszenia korzyści politycznych

Tabela 6.5. Sprawcy przestępstw

Urzędnicy	49,5%
Kadra kierownicza, nadzór	21,8%
Zatrudnieni przy przetwarzaniu danych	10,9%
Kasjerzy	7,6%
Inni	10,9%

6.3.3. Sabotaż, wywiad gospodarczy, szpiegostwo

Sabotaż komputerowy dokonywany jest często z pobudek ideologicznych i politycznych. Przedmiotem sabotażu mogą być zarówno obiekty materialne (budynki mieszczące ośrodki obliczeniowe, pomieszczenia będące archiwami zbiorów, sprzęt, wyposażenie itp.), jak i programy oraz zbiory danych. **Fizyczne metody sabotażu to** między innymi podpalenia, zamachy bombowe lub inne sposoby unieruchamiające, zakłócające bądź powodujące awarie, np. HERF, EMPT. Za proste metody sabotażu uznaje się także wrzucanie opiłków metali, spinaczy, skrawków foli aluminiowej do urządzeń w celu spowodowania zwarć; wylewanie kawy i środków chemicznych na klawiatury i inne urządzenia; wdmuchiwanie dymu, wtryskiwanie lakieru do urządzeń; zakłócanie systemów klimatyzacyjnych i zasilania elektrycznego, przecinanie kabli, wpuszczenie gryzoni na drogach przebiegu kabli.

Logiczne metody sabotażu to stosowanie programów powodujących zniszczenie dużej liczby plików w krótkim czasie, spowalniające pracę programów aplikacyjnych itp. Wśród tych programów wyróżniamy: wirusy, konie trojańskie, robaki, bomby logiczne. Metody logiczne sabotażu są często wspomagane środkami technicznymi poprzez wykorzystywanie obcych pól magnetycznych, wyłączanie zasilania, zmianę oznakowań (etykiet) dyskietek, taśm, kabli, wtyczek itp. Niestety, często mniej świadomi użytkownicy komputerów - nie znający opisanych tutaj metod - całą winę przypisują komputerowi, a tym samym ułatwiają sabotażyście dalszą nie zakłóconą działalność. Sabotażystą może być nie tylko ktoś działający z pobudek ideologicznych i politycznych, lecz także niezadowolony pracownik firmy lub nieuczciwa konkurencja.

Wywiad gospodarczy to metoda zbierania określonych informacji i badania opinii publicznej polegająca na przeprowadzaniu odpowiednio ukierunkowanych rozmów. Ocenianie wywiadu gospodarczego w kategoriach dobra czy zła jest gdyż ocena tego zjawiska jest skomplikowana i złożona. Wywiad gospodarczy, w przeciwieństwie do szpiegostwa, nie ma pejoratywnego zabarwienia i może dotyczyć także działań legalnych.

Formy i metody zbierania informacji służące wywiadowi gospodarczemu mogą być różne:

1. działania agenturalne,

2. tzw. wywiad biały (zdobywanie informacji przez czytanie dostępnych wydawnictw, prasy itp.),
3. wykorzystanie techniki, szczególnie elektroniki (np. podsłuch),
4. wykorzystanie satelitów.

We wszystkich tych metodach można wykorzystać komputer selekcjonujący, przetwarzający i wnioskujący. **Szpiegostwo** w prawie polskim traktowane jest przestępstwo, które obejmuje działalność wywiadowczą dotyczącą wojskowości, polityki, dyplomacji, wynalazczości i polega na braniu udziału w działalności obcego wywiadu, a także na podjęciu się działania na rzecz obcego wywiadu oraz zbierania i przekazywaniu wiadomości na rzecz tego wywiadu. Działanie na rzecz obcego wywiadu przez obywatela polskiego stanowi zbrodnię zdrady ojczyzny.

6.3.6. Piractwo komputerowe

Wymagającą oddzielnego zwrócenia uwagi grupą przestępstw jest także **piractwo komputerowe,** czyli nielegalne kopiowanie, a następnie posługiwanie się programami i zbiorami danych będących cudzą własnością. Od klasycznej kradzieży piractwo odróżnia to, że właściciel najczęściej nie wie, że został okradziony, a ponadto nie traci on fizycznie swojej własności. Straty wskutek piractwa osiągają znaczne sumy. Piratem jest nie tylko pojedynczy użytkownik lub mała grupa, lecz także wielki korporacje. Stopień „dzikiego" kopiowania programów komputerowych określa się bardzo często jako iloraz liczby legalnie sprzedanych programów do liczby sprzedanych komputerów. Tak zdefiniowany przyjmuje wartości z przedziału <0.3 ; 2>, co należy czytać - trzy komputery na jeden zakupiony program bądź dwa programy na jeden komputer. Zakładając, że komputer nie działa bez systemu operacyjnej (licencjonowanego?), to wskaźniki graniczne należałoby obniżyć. Komentarze na temat skali piractwa są chyba w tym miejscu zbyteczne. Do zagadnień tych powrócimy przy omawianiu aspektów prawnych ochrony informacji.

6.3.5. Przestępstwa bankowe

Do listy opisanych przestępstw (sabotaż, wywiad gospodarczy, szpiegostwo, kradzież usług i elementów komputerowych, piractwo) - ze względu na swój spektakularny charakter - trzeba dołączyć przestępstwa bankowe. Tu w grę wchodzą czasami olbrzymie pieniądze, a wielu przestępców do dziś jest ściganych

międzynarodowymi listami gończymi, co działa na naszą wyobraźnię. Ostrożny defraudant preferuje metodę „salami" polegającą na kradzieży małych porcji (plasterków - stąd określeni; „salami"), np. centów, groszy stanowiących końcówki (często w wyniku proces; arytmetycznych zaokrągleń do dwóch miejsc po przecinku) z setek lub tysięcy kont. Zbierane przez dłuższy czas na własne konto i przelewane do innego banku mogą złożyć się na dużą sumę. Manipulacje w bankach bywają ułatwione przez to, ż banki mają przerwę weekendową w pracy i nie zawsze czujne komórki kontroli wewnętrznej. Z kolei sławny akcelerator (oscylator) Bagsika i Gąsiorowskiego był możliwy w polskim systemie bankowym z powodu kilkudniowej czasami „wędrówki' przelewów między odległymi w Polsce miejscowościami. Odpowiedzią polskiego systemu bankowego jest koncepcja elektronicznej izby rozrachunkowej (ang. *clearing house),* czyli system rozliczeń międzybankowych ELIXIR. W systemie tym transakcje (przelewy, zwroty przelewów) są opatrywane podpisem cyfrowym z wykorzystaniem kart inteligentnych (ang. *smart card).* Idea podpisu cyfrowego zostanie później omówiona dokładniej.

Wśród oszustw bankowych można wymienić następujące:

- operowanie czekami bez pokrycia lub zastrzeżonymi (manipulacja na plikach czeków zastrzeżonych),
- fałszowanie zastawów i gwarancji na pobierane kredyty,
- manipulacje na bankomatach (fikcyjne bankomaty wychwytujące PIN-kod i symulujące awarie),
- podrabianie i fałszowanie kart kredytowych,
- operacje dotyczące depozytów i skarbców,
- „pranie" pieniędzy.

Warto tutaj zaznaczyć, że manipulacje bankomatowe stały się plagą Japonii, która na początku lat osiemdziesiątych była krajem przodującym w dziedzinie komputeryzacji operacji bankowych.

Przestępcy często wykorzystują ogólnodostępną wiedzę dotyczącą normalizacji międzynarodowej ISO regulującej np. sposoby kodowania i formaty danych na kartach bankomatowych.

6.4. Rodzaje, charakterystyka i rodzaje zagrożeń

Zastosowanie systemów informatycznych (komputerów) w dziedzinie systemów potencjalnie niebezpiecznych (elektrownie atomowe, badania w kosmosie itp.) jest nowym wyzwaniem dla informatyków specjalistów w dziedzinie bezpieczeństwa systemów informatycznych. Mówi się nawet o systemach uwarunkowanego bezpieczeństwa, tj. takich, w który niepoprawne funkcjonowanie może doprowadzić do skutków katastrofalnych - śmierci lub zranienia ludzi, wielkich strat materialnych, destrukcji lub zatrucia środowiska ... Rozwoju zastosowań komputerów nie da się jednak powstrzymać, a więc wzrasta znaczenie zagadnień bezpieczeństwa systemów informatycznych w zastosowaniach potencjalnie niebezpiecznych.

Skutki stosowania mało bezpiecznych systemów informatycznych mogą być też katastrofalne skutki finansowo w takich dziedzinach zastosowań (nie należących przecież systemów potencjalnie niebezpiecznych!), jak bankowość, ubezpieczenia społeczne telekomunikacja itd.

Systemy informatyczne (teleinformatyczne) zatem, trzeba chronić przed zagrożeniami (narażeniami), którym mogą podlegać. Aby wiedzieć, jak chronić systemy - trzeba, co oczywiste najpierw uzmysłowić sobie rodzaje zagrożeń (narażeń).

6.4.1. Próba klasyfikacji zagrożeń w systemie informatycznym

Przy dokonywaniu jakichkolwiek klasyfikacji istotne jest kryterium, które przyjmujemy. Z tego powodu istnieje kilka podziałów dychotomicznych.

Zagrożenia można podzielić na:

- **bierne** - nie uprawnione ujawnienie informacji bez oddziaływania na system informatyczny, czyli np. podsłuch, analiza ruchu w sieci, emisja ujawniająca,
- **czynne** - aktywne oddziaływanie na system informatyczny, czyli np. modyfikacje, niszczenie informacji, dezinformacja, nie uprawnione zwiększanie możliwości terminalu itd.

Należy sobie zdawać sprawę, że działania bierne intruza najczęściej są etapem przygotowawczym stanowiącym swoisty rekonesans przed działaniami aktywnymi. Istotne jest także to, że efekty działań biernych mogą przynieść ogromne straty, gdy dostaną się w niepowołane ręce (szantaż, korupcja).

Z drugiej strony, zagrożenia mogą być*:*

- **wewnętrzne** - *dokonywane ze strony legalnych użytkowników systemu; oczywiście, należą do najbardziej niebezpiecznych,*
- **zewnętrzne** - dokonywane ze strony zewnętrznych użytkowników to być ataki bierne (podsłuch, emisja ujawniająca, analiza ruchu) lub czynne (udawanie legalnych użytkowników, modyfikacje informacji itd.).

Naturalny wydaje się też inny podział:

- **przypadkowe** - powodowane działaniem nieumyślnym osób korzystających z systemu (brak wiedzy, roztargnienie) bądź błędami oprogramowania lub awariami sprzętu,
- **celowe (umyślne)** - świadome działanie mające na celu niszczenie modyfikację informacji lub unieruchomienie (poprzez doprowadzenie do awarii) systemu.

Oczywisty jest także podział zagrożeń na:

- **sprzętowe** - powodowane przez sprzęt,
- **programowe** - powodowane poprzez oprogramowanie.

W obu powyższych przypadkach chodzi o błędy, awarie sprzętu komputerowego i oprogramowania lub świadomą ingerencję w sprzęt i oprogramowanie. Widać więc, że te ogólnie przedstawione klasyfikacje zagrożeń mogą się wzajemnie przenikać czyli konkretne zagrożenie może być np. jednocześnie czynne (aktywne), wewnętrznie celowe i programowe lub jednocześnie przypadkowe i sprzętowe.

Pozornie wydawałoby się, że taka ogólna klasyfikacja jest klasycznym przykładem „sztuki dla sztuki" opisującym fakty oczywiste, lecz nie wolno nam pominąć aspektu porządkującego. Można zapytać, czy ktoś rozsądny neguje np. potrzebę klasyfikacji informacji w komputerze na system plików, korzeń, katalog, podkatalog, plik i różne jego typy. Gdyby takiego podziału nie było, w pamięci komputera byłby śmietnik, a wyszukiwanie informacji byłoby syzyfową pracą. Podobnie tutaj - trzeba metodycznie „poszufladkować" zagrożenia po to, aby dobrać adekwatne (też sklasyfikowane) środki zabezpieczeń przed zagrożeniami.

Z bardzo ogólnego punktu widzenia, wszystko w technice cyfrowej, informatyce, teleinformatyce da się sprowadzić do formuły **3xC**, to znaczy – *Calculation, Control* i *Communication,* czyli przetwarzania, sterowania (program pamiętany), przesyłania. Każdy komputer przetwarza, przechowuje (pamięta) i przesyła informacje. Istniejące zagrożenia są - jak łatwo dostrzec - pochodną tego prostego i ogólnego spostrzeżenia, gdyż ataki mogą dotyczyć przetwarzania (np. modyfikacja informacji), przechowywania (np. zniszczenie informacji) lub przesyłania (np. podsłuch). Biorąc to wszystko pod uwagę, można wymienić następujące najważniejsze zagrożeni systemie teleinformatycznym:

1. przechwycenie informacji,

2. modyfikacja informacji,

3. zniszczenie informacji,

4. czasowe blokowanie dostępu do informacji,

5. celowe lub przypadkowe przerwv w pracy svstemu (sabotaż, awarie itp.).

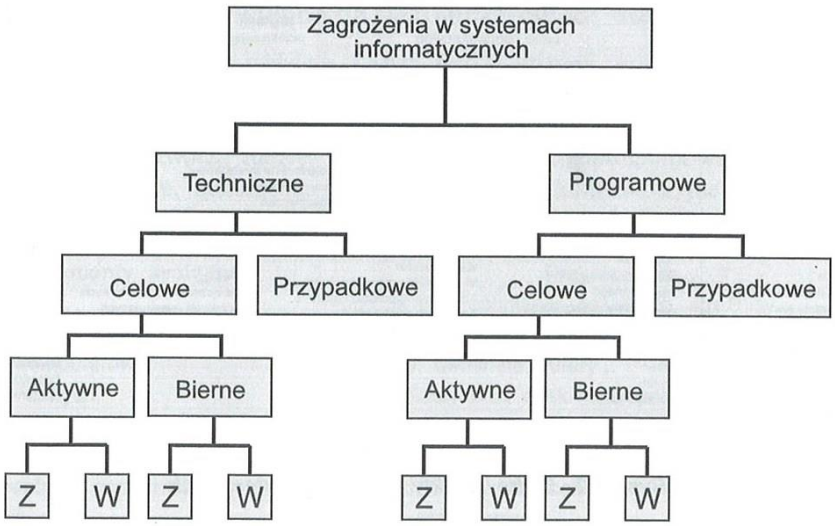
W celu wywołania wymienionych efektów stosuje się między innymi następują ataki:

- maskarada - terminal (komputer) nie uprawniony udaje (podszywa się), że jest uprawniony,
- podsłuch, np. wykorzystujący emisję ujawniającą,
- HERF i EMF - nadajniki zakłócające,
- wirusy, robaki, konie trojańskie, bomby logiczne,
- inne - omówione w kolejnych rozdziałach.

Wymienione zagrożenia mogą występować pojedynczo lub kilka jednocześnie Skuteczny atak na system informatyczny wymaga przełamania bariery, którą stanowią reguły dostępu do systemu. Właściwy dobór haseł przez administratora i użytkowników systemu będzie pierwszą barierą utrudniającą dostęp do systemu informacyjnego. Podkreślić należy; że najbardziej niebezpieczne zagrożenia istnieją ze strony legalnych (wewnętrznych) użytkowników systemu. Zagrożenie wzrasta wraz z liczbą

użytkowników i zróżnicowaniem ich uprawnień. Wynika stąd ważna rola administratora systemu nadającego prawa dostępu do plików danych i programów oraz kontrolującego działanie programów użytkowych i respektowanie nadanych uprawnień. Pełna kontrola systemów powinna wykrywać nie upoważnione próby dostępu i identyfikację użytkownik wykonującego takie próby. Jest to możliwe dzięki tzw. śladom kontrolnym (ang. *audit trail),* dziennikom systemowym, raportom personelu itd.

Nie zawsze użytkownicy systemu zdają sobie sprawę z zagrożenia, jakim może być korzystanie z tzw. wersji testowych (wersji beta) oprogramowania, które na etapie tworzenia może mieć ukryte wady.



Rys.6.1. *Diagram kwalifikacyjny zagrożeń w systemach teleinformatycznych*

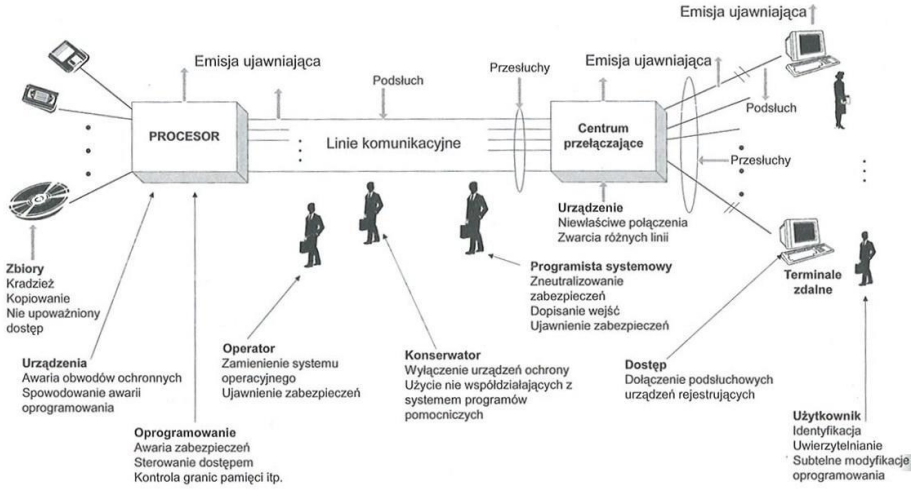
Pierwszym „pierścieniem osłaniającym" system informatyczny powinien być bezpieczny system operacyjny.

Sąd, iż na przykład DOS nie należy do bezpiecznych systemów operacyjnych, nie jest - niestety - powszechnie uświadamiany. Unix zaś ma mechanizmy bezpieczeństwa już wbudowane. Szerzej o tych kwestiach można dyskutować w kontekście dotyczących standardów normalizacyjnych klas bezpieczeństwa *(Orange Book* – "Pomarańczowa księga".

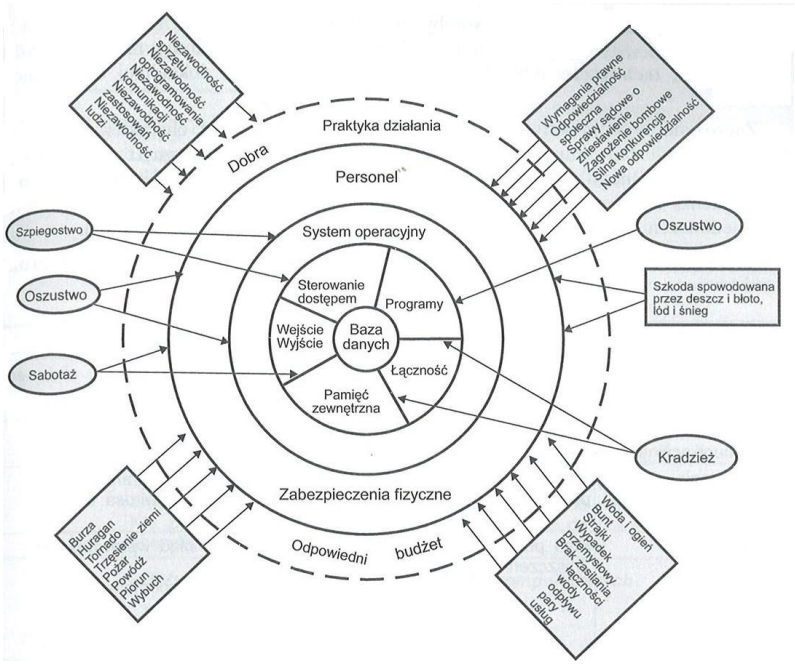
Przeprowadzone tutaj rozważania klasyfikacyjne można podsumować w sposób pokazany na rys. 6.1.

6.4.2. Słabe punkty systemu a typowe środki ochrony

W przypadku zarówno zagrożeń zewnętrznych, jak i wewnętrznych konieczne jest uświadomienie sobie dróg, którymi docierają one do systemu, czy też inaczej mówiąc tzw. słabych punktów systemu informatycznego (ang.*vulnerabilities*) punkty systemu informatycznego przedstawiono na rys. 6.2 według klasycznej już i często cytowanej ilustracji, natomiast typowe środki ochrony na tle zagrożeń prezentuje rysunek 6.3.



Rys.6.2. *Słabe punkty sieci komputerowych*



Rys.6.3. *Zagrożenia i typowe środki ochrony*

6.4.3. Elementy wpływające na bezpieczeństwo; rodzaje ryzyka i strat

Z systemowego punktu widzenia system jest zagrożony, gdy jakikolwiek jego element jest zagrożony. Atak na jeden element systemu może stanowić zagrożenie dla innego elementu itd. Elementy tworzące szeroko pojęty system informatyczny wraz z jego otoczeniem tworzą ludzie, infrastruktura, sprzęt, oprogramowanie, nośniki danych, dane użytkowe, dokumentacja papierowa, łącza komunikacyjne (tab. 6.6).

Tabela 6.6. Elementy wpływające na bezpieczeństwo systemów i sieci komputerowych

Elementy systemu	**Przykładowo…**
Ludzie	pracownicy techniczni, sekretarki, strażnicy….
Infrastruktura	budynki, zasilanie, kontrola wejścia….
Sprzęt komputerowy	serwery, terminale, rutery…..
Nośniki danych	dyski elastyczne, dyski optyczne, taśmy…..
Oprogramowanie	system operacyjny, edytory, kompilatory…..
Dane użytkowe	wyniki obliczeń, adresy, zestawienia ….
Dokumentacja papierowa	wydruki, instrukcje obsługi
Komunikacja	poczta elektroniczna ….

Każdy z tych elementów może być obiektem ataku czy też zainteresowania intruza, a więc każdy z nich musi być chroniony. Metody ochrony mogą być różne np. fizyczne, techniczne, organizacyjne, prawne.

Zagrożenia wspomnianych elementów systemu mogą mieć charakter ryzyka pasywnego (czyli zagrożenia przypadkowego) lub ryzyka aktywnego (czyli zagrożenia celowego, umyślnego). Dla prowadzących śledztwo jest przecież istotne, do czynienia z pożarem, czy też podpaleniem, czy pliki zniszczono przez roztargnienie, niedouczenie, czy też jest to celowe działanie o znamionach sabotażu.

Zależność między rodzajami ryzyka a poszczególnymi elementami przedstawiono w tabeli 6.7.

Tabela 6.7. Zagrożenia w systemach komputerowych

Klasa zagrożenia	Ryzyko pasywne	Ryzyko aktywne
Centrum komputerowe	Pożar, powódź, inne kataklizmy Awaria instalacji: gaśniczej, zasilania, klimatyzacyjnej	Podpalenie Sabotaż Strajk okupacyjny
Infrastruktura telekomunikacyjna	Błędy przesyłania, adresowania danych	Podsłuch linii
Wykonywanie programów	Korzystanie z nieaktualnej wersji pliku lub programu	Kopiowanie oprogramowania Wprowadzanie wirusa do programów
Korzystanie z systemu	Błąd przy wprowadzaniu danych Zniszczenie pliku przez nieuwagę	Świadomy błąd wprowadzania danych Kopiowanie, podmiana lub niszczenie plików Wykonywanie prac niedozwolonych lub własnych
Nośniki danych	Błąd przy manipulacji nośnika powodujący utratę danych elektrycznością statyczną lub polem magnetycznym	Kradzież nośników Podmiana nośnika Kopie nośników w celu analizy danych

Użytkownik systemu informatycznego w wyniku ataku dokonanego na system ponosi straty materialne lub niematerialne. W obrębie bezpośrednich strat materialnych i niematerialnych możemy mieć do czynienia ze stratami:

- obliczalnymi lub trudno obliczalnymi,
- dającymi się udowodnić lub trudnymi do udowodnienia,
- dającymi się naprawić i niemożliwymi do naprawy,
- dającymi się ubezpieczyć i warunkowo ubezpieczyć.

Istnieją jeszcze **pośrednie** straty materialne i niematerialne:

- utrata kontaktów,
- utrata marki, prestiżu,
- utrata klientów,
- utrata technologii.

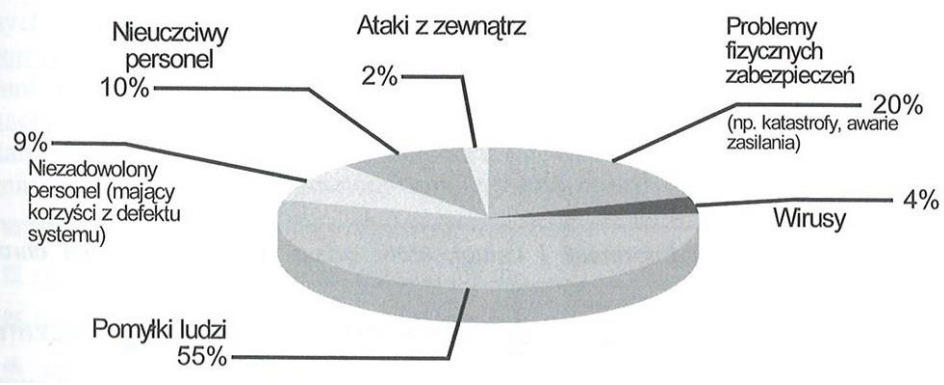
Te właśnie straty (jak to widać w tab. 6.8) są bardzo trudne do obliczenia, udowodnienia, naprawy i ubezpieczenia. To spostrzeżenie nie wymaga chyba komentarza.

Tabela 6.8. Podział strat w systemach komputerowych

Straty	Materialne	Niematerialne
Bezpośrednie	Sprzęt komputerowy Łącza Instalacje (gaśnicza, zasilanie, klimatyzacja) Budynki	Zawartość plików Oprogramowanie
	Charakterystyka: Obliczalne Dające się udowodnić Dające się naprawić Dające się ubezpieczyć	**Charakterystyka:** Trudno obliczalne Trudne do udowodnienia Nie zawsze dające się naprawić Możliwe do ubezpieczenia pod pewnymi warunkami
Pośrednie	Utrata kontraktów Straty eksploatacyjne	Utrata marki Utrata klientów Utrata technologii
	Charakterystyka: Trudne do obliczenia Trudne do udowodnienia Trudne do naprawy Nie zawsze możliwe do ubezpieczenia	**Charakterystyka:** Bardzo trudno obliczalne Bardzo trudne do udowodnienia Bardzo trudne do naprawy Bardzo trudne do ubezpieczenia

6.4.4. Statystyka typowych zagrożeń

W tabeli 6.4 przedstawiono statystykę typów przestępstw oraz sprawców (tab.6.**5**). Przestępstwo, oczywiście, należy do celowych zagrożeń, a więc w tych statystykach nie uwzględniono zagrożeń przypadkowych. Diagram statystyki zagrożeń przedstawiono na rys. 6.4.



Rys.6.4. *Typy zagrożeń. Przybliżony diagram częstości występowania*

Zwróćmy uwagę na czynnik ludzki i to dotyczący personelu firmy (zagrożeni wewnętrzne). Sumując procentowy udział zagrożeń ze strony personelu **(pomyłki, nieuczciwość, niezadowolenie)** otrzymujemy 74%! Zagrożenia spowodowane atakami z zewnątrz, wirusami i katastrofami są trzykrotnie mniejsze. To naprawdę zmusza do zastanowienia. Niektórych z czytelników zdziwi chyba nikły procent (4% dotyczący roli wirusów w zagrożeniach systemu.

6.4.5. Zagrożenia a podstawowe usługi przed nimi chroniące

W punkcie 6.4.1 wspomniano już o przechwytywaniu, modyfikacji i niszczeniu informacji. Tutaj wstępnie zasygnalizujemy fakt istnienia usług, które gwarantują integralność zawartości, integralność sekwencji, uwierzytelnienie nadawcy, niezaprzeczalność nadania oraz poufność zawartości. W tabeli 6.9 przedstawiono usługi które chronią przed wspomnianymi zagrożeniami. Niektóre usługi ze swojej istoty zawierają już w sobie inne usługi. Taką wzajemną zależność przedstawiono w tab. 6.10.

Tabela 6.9. Zagrożenia dla informacji i usługi, które przed tymi zagrożeniami chronią

Usługa / Zagrożenie	Integralność zawartości message content integrity	Integralność sekwencji message sequence integrity	Uwierzytelnienie nadawcy message origin authentication	Niezaprzeczalność nadania non-repudiation of message origin	Poufność zawartości confidentiality of content
Nie uprawniony odczyt wiadomości					
Wprowadzenie fałszywych wiadomości					
Modyfikacja wiadomości					
Zduplikowanie wiadomości lub jej przejęcie i opóźniona transmisja					
Skasowanie wiadomości					
Zaprzeczenie wysłania wiadomości					

. **Tabela 6.10.** Związki pomiędzy usługami ochrony informacji

Zawiera / Usługa	Integralność zawartości message content integrity	Uwierzytelnienie nadawcy message origin authentication	Niezaprzeczalność nadania non-repudiation of message origin	Poufność zawartości confidentiality of content
Integralność zawartości				
Uwierzytelnienie nadawcy				
Niezaprzeczalność nadania				
Poufność zawartości				

6.4.6. Emisja ujawniająca - zastosowania i metody ograniczania

Jak już wcześniej wspomniano (punkt 6.4.1), zagrożeniem biernym, sprzętowym i celowym jest podsłuch. Jako tradycyjne telekomunikacyjne środki podsłuchowe stosuje się najczęściej:

- ♦ mikronadajniki stacjonarne („pluskwy") lub przenośne,
- ♦ nadajniki umieszczone w aparacie telefonicznym,
- ♦ miniaturowe mikrofony uruchamiane przez dotyk,
- ♦ przenośne laserowe skanery okienne; podsłuch jest możliwy z odległości kilkuset metrów po nastawieniu urządzenia na okno podsłuchiwanego pomieszczenia
- ♦ ukryty dyktafon umieszczony w przenośnych przedmiotach (np. teczce) i uruchamiany głosem rozmówców.

Urządzenia te jednak służą podsłuchiwaniu dźwięku (mowy) i nie mają zastosowania w „podsłuchiwaniu" komputera. W przypadku systemów informatycznych mamy do czynienia z **emisją ujawniającą**. Każde urządzenie elektroniczne biorące udział w przetwarzaniu, przechowywaniu i przesyłaniu informacji jest źródłem niepożądanej (mówimy także - ubocznej) emisji elektromagnetycznej. **Mówimy o emisji ujawniającej wtedy, gdy sygnał emisji ubocznej jest skorelowany z informacją.** Emisja ujawniająca może być promieniowana lub przewodzona. Emisja ujawniająca (czasami mówi się - emanacja ujawniająca) stosowana jest do infiltracji lub penetracji elektromagnetycznej. Przez stosowanie retransmitujących „pluskiew" (ang.*bugs*) można osiągnąć zasięg około 1 km. Wykorzystanie emisji ujawniającej do przewodów powoduje istotne zwiększenie tego zasięgu. Jak wynika z wielu badań laboratoryjnych, **emituje każdy element systemu komputerowego** (płyta główna, monitor, drukarka, klawiatura) w mniejszym lub większym stopniu. Najbardziej niebezpieczne z punktu widzenia ochrony informacji są monitory i drukarki. Poziom emisji ujawniającej zależy od wielu czynników, np. konfiguracji przewodów w przestrzeni, kształtu sygnałów, częstotliwości, sprzężeń galwanicznych, sposobu zasilania i uziemienia. Istnieją następujące metody zmniejszania emisji ujawniającej:

- ▪ obniżenie poziomu mocy emisji z urządzeń,
- ▪ stosowanie osłon i kabin ekranujących,
- ▪ instalowanie sprzętu w pomieszczeniach ekranowanych,

- filtrowanie układów zasilania,
- właściwe okablowanie (np. odległość kabli sygnałowych od zasilaniowych),
- prowadzenie łączy światłowodowych w osłonach PCV,
- uziemienie obudów sprzętu komputerowego,
- wykonanie uziemienia niezależnego.

Problematyką dotyczącą zwalczania emisji ujawniającej zajmuje się dziedzina zwana kompatybilnością elektromagnetyczną EMC (ang. *electromagnetic compatibiliy*). Intensywne prace badawcze prowadzone są w Politechnice Wrocławskiej pod kierunkiem prof. Bema. Wyniki tych prac są relacjonowane na KST (Krajowe Sympozjum Telekomunikacji) w Bydgoszczy (w ostatnich latach KSTiT stała się konferencją „wędrującą" po różnych Ośrodkach akademickich).

Emisji ujawniającej przypisuje się coraz większe znaczenie, gdyż jej wykorzystanie jest związane nie tylko z przechwytywaniem informacji, lecz jakby z „odwrotnym" działaniem. Oczywistym jest, że po rozpoznaniu parametrów sygnału nożna skonstruować generator sygnału o identycznych parametrach i odpowiedniej mocy. Taki generator, o którym wspomniano już w punkcie 6.1, może powodować zdalnie istotne zakłócenia a nawet destrukcję systemu komputerowego (pamięci, kart graficznych, dysku), co jest ewidentnym sabotażem. Należy jednak zdawać sobie sprawę z ogromnych kosztów zarówno odbiorników emisji ujawniającej, jak i wspomnianych generatorów. Nie od rzeczy jest więc pytanie, czy przeciwnika, intruza atakującego nasz system stać na taki koszt. W ważnych zastosowaniach ze sfery militarnej, dyplomatycznej, szpiegowskiej należy jednak brać pod uwagę taką możliwość.

Jako ciekawostkę dodajmy tutaj, że w Polsce zostały opracowane obudowy komputerów, terminali, telefonów oraz kabiny zapewniające bezpieczną pracę.

6.5. Sposoby zabezpieczeń

6.5.1. Klasyfikacja, charakterystyka ogólna

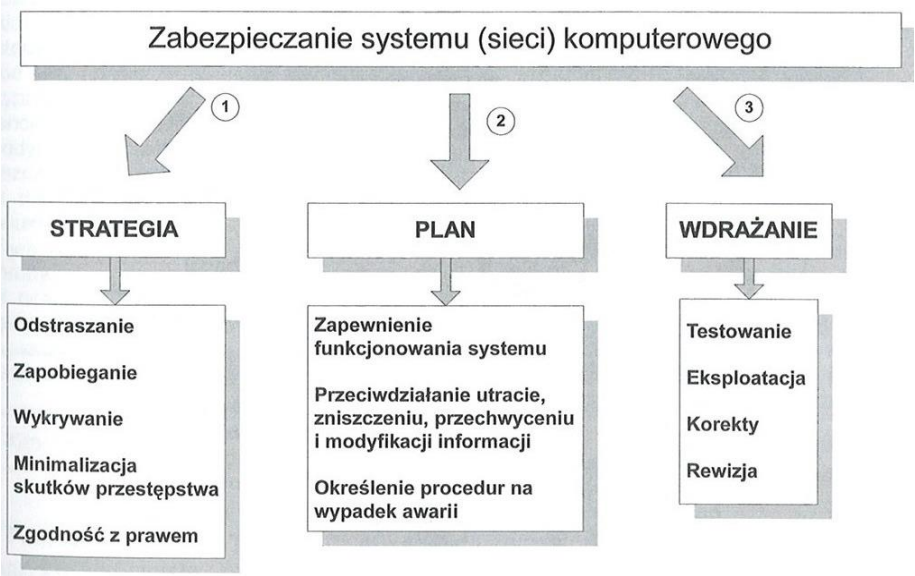
Problematyka dotycząca zabezpieczeń systemu informatycznego w gruncie rzecz sprowadza się do pytania: CO, PRZED KIM (CZYM), JAK i ZA JAKĄ CENĘ

trzeba chronić? Innymi słowy, chodzi tutaj kolejno o obiekty zagrożeń, rodzaje zagrożeń, metody skutecznego przeciwdziałania zagrożeniom oraz koszty. Mówiąc kosztach mamy na uwadze te wymierne, jak i niewymierne (np. zabezpieczenia mogą pogorszyć komfort pracy personelu, spowodować istotne spowolnienie pracy komputera itd.). W punkcie 6.4 zostały już wyspecyfikowane ogólne rodzaje zagrożeń, natomiast w punkcie 6.5 omówimy głównie metody przeciwdziałania zagrożeniom.

6.5.1.1. Etapy zabezpieczenia systemu informatycznego

Zabezpieczenie systemu informatycznego jest zbiorem działań, w którym można wyróżnić trzy etapy:

Co, przed kim (czym?), jak, za ile chronić



Rys.6.5. *Strategia, plan oraz istota zabezpieczeń*

1. określenie **strategii,**

2. opracowanie koncepcji szczegółowej **(planu),**

3. wdrażanie.

Szczegółowy opis poszczególnych etapów przedstawiono na rys.6.5.

Zwróćmy uwagę, że jednym ze składników strategii jest odstraszanie. Słuchacz chyba zna z praktyki takie odstraszanie na przykładzie m.in. przestróg autorów programów przed nielegalnym kopiowaniem tychże programów.

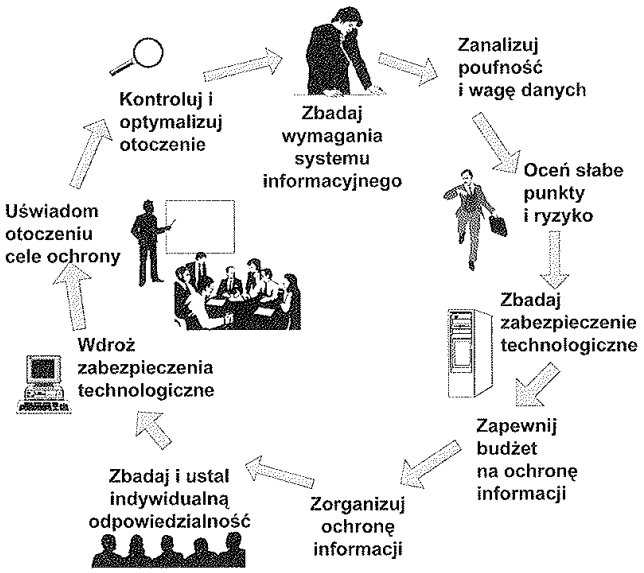
Ostrzeżenie typu: „W przypadku próby skopiowania sformatuję Twój dysk twardy" jest często skuteczne. Z punktu widzenia zgodności z prawem, taka ochrona jest zabroniona, tak więc możemy być pewni, że ostrzeżenie jest gołosłowne. Większość elementów wyszczególnionych na rys.6.5 nie wymaga komentarza. Zauważmy jedynie, że istotną cechą planu zabezpieczeń jest określenie procedury postępowania na wypadek awarii. Procedura ta powinna być niezwykle drobiazgowo rozpisanym na role scenariuszem.

Procedura postępowania na wypadek awarii powinna między innymi:

uwzględniać możliwość tradycyjnego („ręcznego") przetwarzania danych przynajmniej przez jakiś czas, określać osoby odpowiedzialne, kierujące procedurą awaryjną, przewidywać konieczność udziału konsultantów (różnych specjalności) spoza firmy, określać zadania, które muszą być wykonywane bezwzględnie niezależnie od awarii itd.

W tym miejscu należy zaproponować refleksję - czy w macierzystej firmie coś takiego istnieje?

Innym środkiem wyrazu charakteryzującym działania zabezpieczające jest rysunek 6.6.



Rys.6.6. *Przegląd zabezpieczeń i działania zabezpieczające*

Dwa elementy na tym rysunku są warte uświadomienia - w dobrym planie zabezpieczeń musi być ustalona indywidualna odpowiedzialność osób za określone

fragmenty systemu ochrony, ponadto ogromną rolę odgrywa uświadamianie personelowi celów ochrony. Żaden najlepszy plan zabezpieczeń nie będzie funkcjonował i pozostanie „martwym planem" jeśli nie będzie w przedsiębiorstwie (lub poza nim!) służb rewizyjnych *(audit).* Z kontrolą nie należy jednak przesadzać, w tym sensie np. aby kontrolować kontrolującego. Wyobraźnia dotycząca zagrożeń jest potrzebna lecz nie może się przecież przerodzić w manię prześladowczą. Rozmiar służb kontrolnych (etaty, pieniądze) powinien być adekwatny do wartości chronionej informacji, sprzętu i oceny potencjalnych zagrożeń.

Ważną rolę strategiczną pełni w zakresie zabezpieczeń systemu informatycznego kierownictwo firmy. IBM opublikowało bardzo obszerną tabelę pomocną kierownictwu firm w tym zakresie, której fragment przedstawiono poniżej (tab. 6.11).

Tabela 6.11. Fragment „Tabeli działań kierownictwa w zakresie ochrony informacji zaproponowanej przez IBM

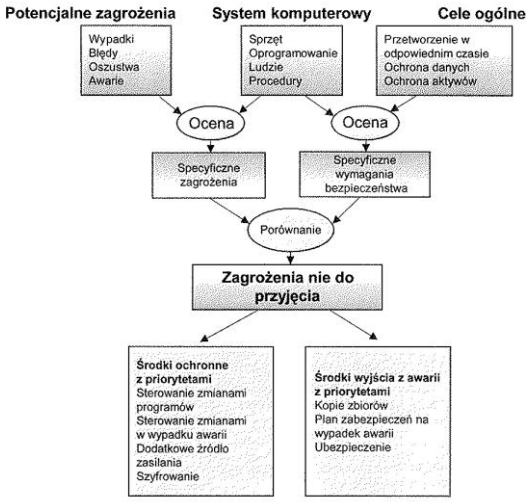
Krok działania sprawa kierownictwa	**Zbadaj wymagania systemu informacji**	**Analizuj poufność i wagę danych**
Na jakie pytania trzeba sobie odpowiedzieć?	Jakie dane są zbierane? Kto ich potrzebuje? Dlaczego ono są potrzebne? Kiedy są potrzebne? Czy dowiadujesz się o nowych danych i nowych sposobach wykorzystania danych?	Jak skomplikowana powinna być struktura kwalifikacji? W jaki sposób będziesz oceniał wartość informacji? Jaka jest twoja odpowiedzialność prawna i społeczna? Jak dalece trzeba chronić każdy z rodzajów informacji?

Oceń słabe punkty i ryzyko	**Zbadaj zabezpieczenia technologiczne**	**Zapewnij budżet na ochronę informacji**
Jakie są słabe punkty systemów informacyjnych? Jakie jest ryzyko	Jakich technologicznych zabezpieczeń użyto? W jaki sposób organizacja	Jakie są koszty wdrożenia i działania programu zabezpieczającego?

przypadkowego bądź intencjonalnego odkrycia, zmodyfikowania bądź zniszczenia informacji? Jak dalece można zredukować ryzyko przy danym wzroście ochrony? Jak oceniasz kompromis między zwiększeniem bezpieczeństwa a wzrostem kosztów?	używa najnowszych dostępnych technologii? Jakie są koszty związane z dostępnymi zabezpieczeniami technologicznymi? Jak skuteczne są dostępne zabezpieczenia technologiczne?	Którymi z nich można obciążyć użytkowników, a które stanowią narzut? Jaka jest wartość poufności? W jaki sposób maksymalizować bezpieczeństwo przy danych budżetowych lub w jaki sposób zminimalizować koszty przy danych wymaganiach bezpieczeństwa? Ile bezpieczeństwa zapewni dodatkowo wydana złotówka? Kto zapłaci za zwiększony koszt przetwarzania podczas wdrażania?

Pomocna forma w postaci pytań ułatwia niewątpliwie uświadamianie sobie problematyki, być może, przedtem rzadko (wcale) uświadamianej. Dużo pytań dotyczy wydatków na ochronę, a wszystkie sprowadzają się do pytania ogólnego: **Jak oceniasz kompromis między zwiększeniem bezpieczeństwa a wzrostem kosztów?** Jest to jedno z fundamentalnych pytań tzw. **analizy ryzyka** (ang. *risk analysis*).

Diagram, za pomocą którego można sformułować specyficzne zagrożenia w systemie informatycznym z jednej strony oraz specyficzne wymagania bezpieczeństwa z drugiej strony, przedstawiono na rys. 6.7. Przez porównanie zagrożeń i wymagań następuje selekcja zagrożeń, które są nie do przyjęcia, a co za tym idzie - określenie środków ochrony i środków (procedur) wyjścia z sytuacji awaryjnej.



Rys.6.7. *Analiza ryzyka dla zabezpieczeń systemu komputerowego*

6.5.1.2. Model postępowania w obecności zagrożeń

W literaturze dotyczącej przestępczości komputerowej, jest zalecany przez FBI model postępowania w obecności zagrożeń przedstawiony na rys.6.8.

Wyróżnia się w nim trzy składniki:

1. prewencja (ang. *prevention),*

2. wykrywanie (ang. *detection),*

3. postępowanie (proces) sądowe (ang. *prosecution*).

Rys.6.8. *Model postępowania w obecności zagrożeń zalecany przez FBI*

Wymienione na rys.6.8 składniki prewencji, tzn. różne rodzaje ochrony, są przedmiotem rozważań w kolejnym punkcie 6.5.1.3.

6.5.1.3. Klasyfikacja metod utrzymania bezpieczeństwa, poziomy ochrony

Charakterystycznym zjawiskiem w każdej nowej, rodzącej się dyscyplinie są próby porządkowania wiedzy wynikającej z doświadczeń praktycznych. Spotyka się więc różne terminy, definicje, klasyfikacje. Nie dziwmy się zatem, że w stosunków młodej, jeszcze dojrzewającej przecież dziedzinie mamy do czynienia z różnymi klasyfikacjami, mniej lub bardziej zbliżonymi do siebie i częściowo pokrywającymi się.

Metody utrzymania bezpieczeństwa w systemie informatycznym dzielimy na cztery grupy:

1. ochrona fizyczna (ang. physical security),

2. ochrona kadrowa (ang**.** personnel security),

3. ochrona komunikacji (ang. communication security),

4. ochrona operacyjna (ang. operation security).

We wszystkich czterech przypadkach możemy, oczywiście, zamiennie używać terminu bezpieczeństwo (zabezpieczenia) zamiast terminu ochrona.

Zabezpieczenia fizyczne dotyczą katastrof i awarii (pożar, dym, woda, trzęsienie, wibracje, ogrzewanie, oświetlenie, klimatyzacja, zasilanie energetyczne) oraz zabezpieczeń przed fizycznym wtargnięciem intruza (konstrukcja budynku, okna, drzwi podłogi, systemy alarmowe, telewizja przemysłowa itp.).

Zabezpieczenia kadrowe (personelu) dotyczą wszystkiego, co wiąże się z personelem: sprawdzanie niekaralności, dublowanie dostępu do systemu, szkolenia, sprawdzanie powiązań personelu z konkurencją, asekuracyjna procedura zwalnianie personelu, polityka urlopowa i czasu pracy, polityka rotacji między stanowiskami i doboru współpracowników.

Zabezpieczenia komunikacyjne dotyczą oprogramowania i plików danych, w szczególności przy przesyłaniu informacji komunikacji w sieci komputerowej(ochrona poczty elektronicznej, szyfrowanie, programowe reguły dostępu do systemu, ochrona i dobór haseł itp.).

Zabezpieczenia operacyjne dotyczą wszystkich działań powodujących strony wzrost świadomości użytkowników dotyczącej zagadnień bezpieczeństwa oraz zniechęcających przestępców do popełnienia przestępstwa z drugiej strony. Wszystkie te przedsięwzięcia w tej grupie mają jak można się domyślić, charakter organizacyjny.

W stosunku do innych znanych klasyfikacji może dziwić nieobecność grupy zabezpieczeń technicznych i programowych. Aspekty techniczne i programowe są zapewne ukryte w grupie zabezpieczeń komunikacyjnych.

Dla odmiany przytoczymy inną klasyfikację. Według Cronina metody utrzymywania bezpieczeństwa w systemie informatycznym dzielimy również na cztery grupy:

1. ochrona techniczna,

2. ochrona programowa,

3. ochrona organizacyjna,

4. ochrona kadrowa.

Jak łatwo zwrócić uwagę, w cytowanym podziale brak grupy „ochrona fizyczna", która istniała w pierwszej klasyfikacji. Należy sądzić, że w tej klasyfikacji środki fizyczne z poprzedniej klasyfikacji (np. metody uniemożliwiające **fizyczne** wtargnięcie intruza) w tej klasyfikacji zaliczane będą do grupy środków technicznych. Przy okazji rozważań o klasyfikacji nasuwa się refleksja bardziej ogólna. **Wszelkie podziały klasyfikacyjne - zarówno zagrożeń, jak i sposobów zabezpieczeń - są w sposób nieunikniony nieostre.** Z jednej więc strony porządkowanie klasyfikacyjne jest potrzebne, z drugiej strony - klasyfikacja jest rozmyta. Bardzo często możemy mieć wątpliwości, do jakiej grupy zaliczyć konkretną metodę zabezpieczeń, np. szyfrowanie (przecież istnieje „czysto" sprzętowe, bo istnieje wyodrębnione urządzenie; a może być także programowe). Inną wątpliwość mamy przy próbie klasyfikowania ograniczenia wstępu do pomieszczeń z użyciem kart elektronicznych (środek techniczny?, organizacyjny?, fizyczny?).

W celu uniknięcia opisanych wątpliwości, niespójności i braku ostrości można zaproponować następującą klasyfikację metod utrzymywania bezpieczeństwa systemów informatycznych:

1. ochrona **fizyczna,**

2. ochrona **techniczna,**

3. ochrona **programowa,**

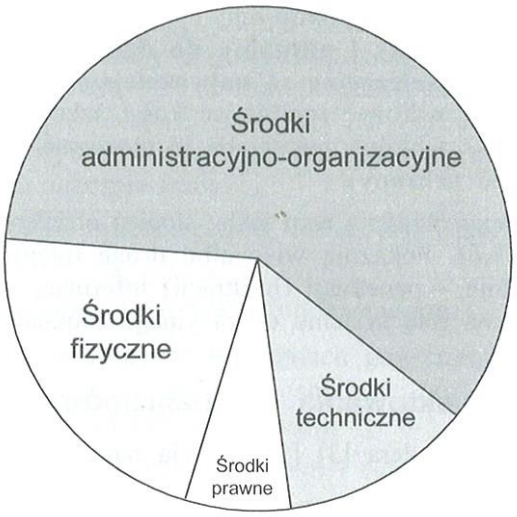
4. ochrona **organizacyjno-administracyjna,**

5. ochrona **prawna,**

6. ochrona **kryptograficzna** (opcjonalnie! - z powodu swojej specyfiki, odrębności w wybranych dziedzinach).

Przynależność poszczególnych specyficznych metod ochrony do odpowiednich grup zostanie przeanalizowana w punkcie 6.2.

Dla zobrazowania udziału poszczególnych środków w utrzymywaniu bezpieczeństwa przedstawiono w sposób przybliżony klasyczny – diagram na rys. 5.5.



Rys.6.9. *Środki do utrzymania bezpieczeństwa*

Rys.6.10. *Poziomy ochrony informacji*

Zastanawia brak środków programowych; być może, zostały ukryte w środkach technicznych (?). **Najważniejszy i aktualny do dziś wniosek to spostrzeżenie - środki administracyjno-organizacyjne są najważniejsze;** można je szybko, skutecznie i prawie bez kosztów wdrożyć (pomijając koszt szkoleń i wydawanych instrukcji). Rozpatrując metody zabezpieczeń trzeba je ulokować na właściwym **poziomie ochrony** (lub **pierścieniu ochrony**).

Zauważmy, że poziomy określają nam jakby stopień oddalenia od komputera w kierunku otoczenia (rys. 6.10). Pokazują więc albo drogę (etapy) „ucieczki" informacji z systemu bądź odwrotnie - penetracji (infiltracji) informacji z zewnątrz.

6.5.2. Przegląd metod utrzymania bezpieczeństwa

W punkcie 6.5.1.3 dokonano klasyfikacji metod utrzymywania bezpieczeństwa zwracając uwagę na istnienie kilku rodzajów klasyfikacji. W tym punkcie omówimy zabezpieczenia fizyczne, techniczne i organizacyjno – administracyjne. Ze względu na ich odrębność, oddzielnie omówimy zabezpieczenia kryptograficzne oraz zabezpieczenia programowe.

6.5.2.1. Zabezpieczenia fizyczne

Na zabezpieczenia fizyczne składają się następujące elementy:

♦ ochrona przeciwwłamaniowa,

♦ ochrona przeciwpożarowa,

♦ ochrona przeciw innym katastrofom (np. zalanie wodą),

♦ kontrola dostępu do obiektów i ruchu po obiekcie,

♦ wybór pomieszczeń dla systemu komputerowego - ogólnie, architektura pomieszczeń,

♦ dobór materiałów budowlanych,

♦ dobór rozmieszczenia drzwi i okien w pomieszczeniach komputerowych.

Listę tę, oczywiście, mógłby każdy z Czytelników wydłużać, lecz wymienione tu elementy pozwalają na zrozumienie tego, co się kryje pod określeniem „zabezpieczenie fizyczne".

Przytoczymy obecnie listę praktycznych zaleceń - wskazówek dla użytkowników systemów informatycznych:

- używaj barier ogniowych w otoczeniu pomieszczeń, w których mieści się sprzęt komputerowy,
- instaluj detektory przeciwpożarowe,
- instaluj systemy przeciwpożarowe powodujące automatyczne zamknięcie systemu (ang. *shut down)* w przypadku alarmu,
- przechowuj sprzęt przeciwpożarowy w bliskim sąsiedztwie pomieszczeń, w których znajduje się sprzęt komputerowy,
- wprowadź zakaz palenia tytoniu, spożywania napojów i posiłków w bliskim sąsiedztwie komputerów (terminali),
- ograniczaj stosowanie tworzyw sztucznych w pomieszczeniach komputerowych (np. stosuj atestowane wykładziny antyelektrostatyczne),
- stosuj ogniotrwałe sejfy do przechowywania archiwizowanych nośników informacji,
- kontroluj dostęp do obiektów i ruch po obiekcie instruując służby wartownicze, stosując odpowiednie zamki, czujniki, sygnalizatory, systemy alarmowe, telewizję przemysłową itp.,
- lokalizuj sprzęt komputerowy w oddaleniu od okien, tak aby podglądanie ekranu monitora było utrudnione,
- nie instaluj sprzętu komputerowego na parterze, lecz na wyższych kondygnacjach (dlaczego?),
- stosuj dodatkową podłogę ukrywającą okablowanie,
- instaluj czujniki wykrywające obecność wody w pomieszczeniach komputerowych,
- chroń magnetyczne nośniki informacji przed zewnętrznymi polami magnetycznymi,
- stosuj zamki szyfrowe do pomieszczeń komputerowych,

- upewnij się, że nie jest możliwe włamanie do pomieszczeń komputerowych – przez okno z zewnątrz budynku lub z pomieszczeń sąsiadujących (od góry, z dołu i z boku).

Jeśli w tym miejscu można odnieść wrażenie, że są to oczywistości, to nic nie szkodzi. Praktyka, niestety, wykazuje, że mimo tych oczywistości obserwuje się dużą beztroskę personelu w tym względzie i warto zaakcentować znaczenie form ochrony, a w szkoleniach ciągle je uświadamiać! Wystarczy samemu poobserwować jak często przy komputerze (terminalu) pije się napoje i pali papierosy.

6.5.2.2. Zabezpieczenia techniczne

Na zabezpieczenia techniczne składają się między innymi następujące elementy:

- dobór właściwej konfiguracji sprzętowej komputera,
- dublowanie dysków twardych (ang. *mirroring, duplexing)* związane z bezpieczną archiwizacją,
- blokowanie sprzętowe dostępu do klawiatury, napędów dyskietek i dysków,
- klucze na kartach inteligentnych,
- urządzenia klimatyzacyjne,
- techniczna ochrona przed emisją ujawniającą,
- urządzenia do podtrzymywania zasilania (UPS).

Lista praktycznych zaleceń dla użytkowników systemów informatycznych jest następująca:

- utrzymuj właściwą temperaturę i wilgotność (10°C-26°C, 35%—50%) oddzielną klimatyzację dla pomieszczeń komputerowych,
- stosuj bezprzerwowe systemy zasilania (UPS) pozwalające po zaniku zewnętrznego na poprawne zamknięcie systemu (ang. *shut down),*
- stosuj osłony ekranujące (kabiny) chroniące przed emisją ujawniającą,

- instaluj urządzenia (karty sprzętowe) wykrywające nielegalny dostęp do komputera,
- prowadź w sposób regularny właściwą konserwację urządzeń (czyszczenie głowic napędów dyskietek, drukarek, czytników kart magnetycznych, streamerów; czyszczenie klawiatur; usuwanie zanieczyszczeń - „odkurzanie" jednostki centralnej, drukarek itd.),
- obserwuj i okresowo monitoruj wydajność (moc obliczeniową) komputera,
- dbaj właściwie o bieżące zaopatrzenie w części zamienne, akcesoria oraz materiały eksploatacyjne.

6.5.2.3. Zabezpieczenia organizacyjno-administracyjne

Zwróciliśmy wcześniej uwagę, że ten rodzaj zabezpieczeń jest bardzo skuteczny i prawie nie wymagający kosztów. W przyjętej przez nas klasyfikacji, w tej grupie znajdują się bardzo istotne czynniki kadrowe. Szczególną uwagę zwrócimy na dwie kwestie: rolę administratora systemu oraz służb rewizyjnych (ang. *audit).*

Zabezpieczenia organizacyjno-administracyjne tworzą następujące składniki:

- instrukcje pisemne określające szczegółowo tryb postępowania w warunkach normalnej pracy i w sytuacjach wyjątkowych (awaryjnych),
- intensywne i systematyczne szkolenia personelu,
- codzienne uświadamianie zagrożeń na konkretnych przykładach i faktach,
- istnienie kompleksowego programu zabezpieczeń w firmie wydanego w postać oficjalnego dokumentu,
- ustalenie jednoosobowej odpowiedzialności osób z precyzyjnym określeniem zakresu czynności, za które się odpowiada,
- właściwa polityka kadrowa przy zatrudnianiu (zwalnianiu) pracowników oraz w sezonie urlopowym (zastępstwa!, przekazywanie uprawnień),
- selekcja kadrowa (konkurs?) przy zatrudnianiu administratora systemu; precyzyjne ustalenie zakresu jego obowiązków i możliwości zastępowania,

- określenie poziomu uprawnień programowego dostępu użytkowników do eksploatowanej aplikacji,
- nadzór nad pracami serwisowymi pracowników zewnętrznych (dotyczy usuwania awarii sprzętu i oprogramowania) oraz wszelkimi pracami adaptacyjnymi w pomieszczeniach komputerowych,
- ochrona administracyjno-organizacyjna w zakresie wszelkiej dokumentacji dotyczącej sprzętu, oprogramowania, tras przebiegu kabli, szafek rozdzielczych (energetycznych i telekomunikacyjnych),
- prowadzenie „książki wejść do pomieszczeń komputerowych" dla osób postronnych, dokumentowanie w „dzienniku pracy systemu komputerowego" wszelkich awarii, napraw i dziwnych zachowań systemu,
- przestrzeganie zasad (wynikających z instrukcji firmy) przekazywania i przechowywania wewnątrz firmy magnetycznych nośników informacji oraz tabulogramów (wskazane kwitowanie odbioru!),
- systematyczne i skrupulatne prowadzenie ewidencji kart magnetycznych i elektronicznych (inteligentnych) oraz określanie zasad ich wydawania i zdawania (np. dłuższa nieobecność w pracy),
- opracowanie procedury komisyjnego niszczenia zbędnych tabulogramów, zużytych kart magnetycznych i elektronicznych.

Przytoczona tutaj dość obszerna lista (z powodu jej ważności) składników zabezpieczeń organizacyjno - administracyjnych implikuje jednoznacznie zbiór zaleceń praktycznych. Każdy z wymienionych punktów może być obszernie komentowany. Pozostawiamy to Słuchaczom jako swoiste ćwiczenie.

6.5.3. Podstawy zabezpieczeń kryptograficznych

Zagadnienia związane z zabezpieczeniami kryptograficznymi doczekały się bardzo bogatej i dobrej bibliografii, także w języku polskim. Są to na ogół opracowania na bardzo wysokim poziomie akademickim i wymagające od Czytelnika niezbędnego przygotowania matematycznego. Zdarzają się też książki opisujące praktyczne aspekty kryptografii (np. Schneier B., *Applied Cryptography, Protocils, Algoritmthms and*

Source Code In C. J. Wiiley and Sons 1994). Przez długi okres sprawy ochrony informacji były kojarzone prawie wyłącznie z kryptografią. Stosunkowo niedawno zagadnienia dotyczące kryptografii stanowią istotny fragment większego kompleksu, jakim jest dziedzina zwana *computer security.* Z przedstawionej w punkcie 6.5.1.3 klasyfikacji wynika, że zabezpieczenia kryptograficzne są jednym z sześciu sposobów zabezpieczeń systemów informatycznych. Przytoczona argumentacja jest chyba wystarczającym usprawiedliwieniem, że zakładamy w tym opracowaniu bardzo elementarny poziom opisu kryptografii sugerując Słuchaczom zainteresowanym szczegółami studiowanie bogatej literatury problemu.

6.5.3.1. Pojęcia podstawowe

Kryptografia zajmuje się utajnionym zapisem informacji.

Szyfr jest metodą utajnionego zapisywania w taki sposób, że tekst jawny (otwarty) jest przekształcany w tekst zaszyfrowany (kryptogram).

Szyfrowaniem nazywa się proces przekształcania tekstu jawnego w tekst zaszyfrowany.

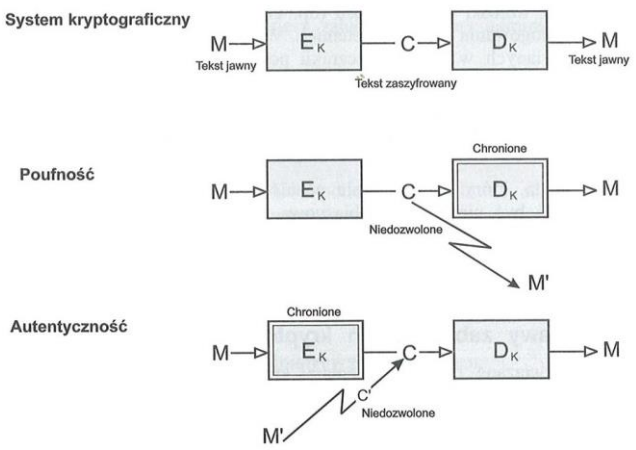
Deszyfrowaniem nazywamy proces odwrotny, czyli umożliwiający przekształcenie tekstu zaszyfrowanego w tekst jawny.

Szyfrowanie i deszyfrowanie są sterowane przez klucz lub klucze kryptograficzne. Czasami deszyfrowanie nie jest potrzebne, gdyż istnieje tzw. szyfrowanie **jedno kierunkowe** (np. haseł dostępu do systemu informatycznego).

Kryptoanaliza zajmuje się metodami łamania szyfrów.

Kryptologia to dziedzina obejmująca kryptografię i kryptoanalizę.

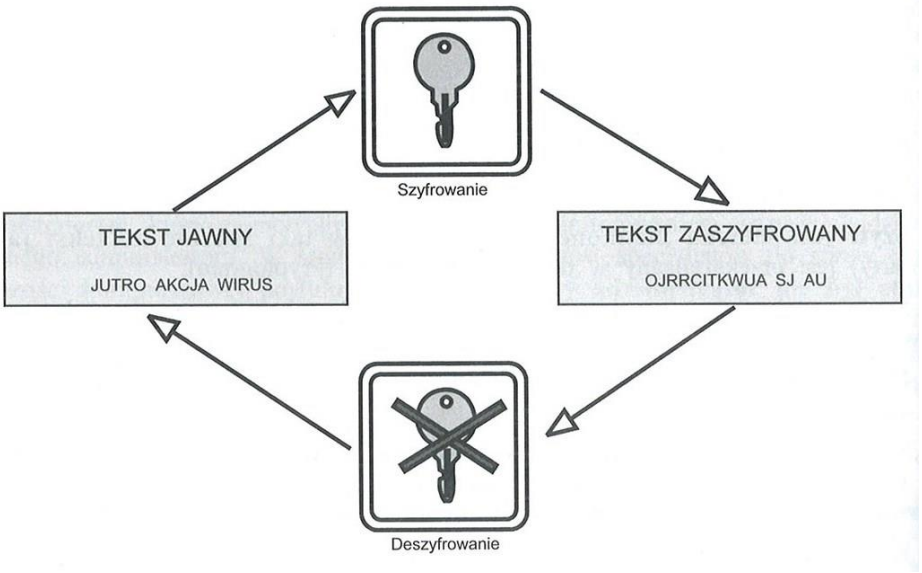
Na rys.6.11 i rys.6.12 symbolicznie przedstawiono ideę szyfrowania i deszyfrowania.



E_k – algorytm szyfrujący z kluczem **k**

D_k – algorytm deszyfrujący z kluczem **k**

Rys.6.11. *System kryptograficzny, poufność i autentyczność*



Rys.6.12. *Szyfrowanie i deszyfrowanie*

Mówi się, że szyfr jest przełamywalny, gdy istnieje możliwość odtworzenia tekstu jawnego na podstawie tekstu zaszyfrowanego albo określenie klucza na podstawie znajomości tekstu jawnego i zaszyfrowanego.

Literatura przedmiotu określa kilka rodzajów ataku na system kryptograficzny.

Poufność informacji (ang. *confidentiality)* to takie przekształcenie informacji, aby była ona niemożliwa do odczytania przez inną osobę poza właściwym odbiorcą.

W celu zachowania poufności wymaga się jedynie ochrony przekształcenia deszyfrującego, tzn. klucza deszyfrującego.

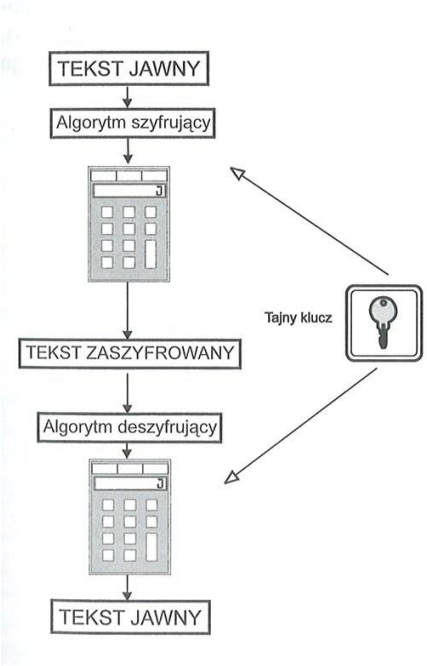
Autentyfikacja (ang. *autentication)* zapewnia możliwość sprawdzania, czy nadawca jest tym użytkownikiem, za którego się podaje. Autentyfikacja wymaga ochrony tylko przekształcenia szyfrującego, tzn. klucza szyfrowania. W Polsce używane są określenia **autentyzacja** i **autoryzacja.**

Idea poufności i autentyfikacji została przedstawiona na rys. 6.11.

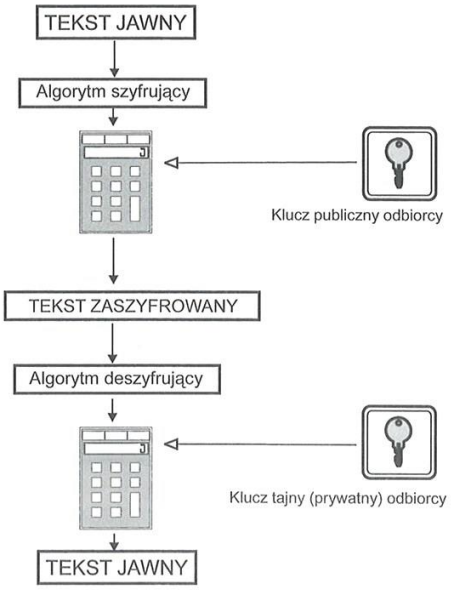
Niezaprzeczalność nadania (ang. *non-repudiation)* chroni przed możliwością wyparcia się przez nadawcę faktu wysłania określonej informacji.

Usługa niezaprzeczalności dostarcza dowodu co do integralności informacji i co do autentyczności nadawcy. Usługa zabezpiecza także przed próbą zmiany informacji i przedstawienia w sądzie jako autentycznej. Usługa niezaprzeczalności jest realizowana przez podpis cyfrowy.

Kryptosystemem z kluczem tajnym (system symetryczny, jednokluczowy) jest system, w którym klucze szyfrowania i deszyfrowania są jednakowe (rys.6.13).



Rys.6.13. *Kryptosystem z kluczem tajnym*



Rys.6.14. *Kryptosystem z kluczem publicznym*

Kryptosystemem z kluczem publicznym (system asymetryczny, dwukluczowy,z kluczem jawnym) jest system, w którym są stosowane dwa klucze: publiczny i tajny (prywatny) (rys.6.14).

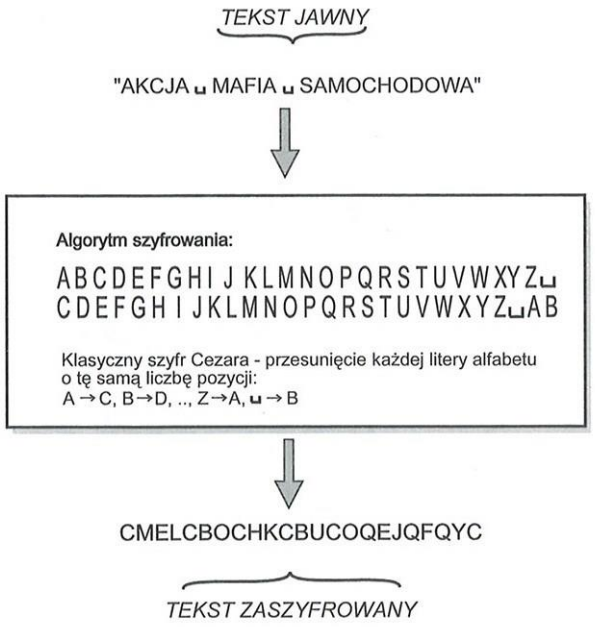
W kryptosystemach z kluczem tajnym istotnym problemem jest przesłanie klucza (który został wygenerowany u jednego z użytkowników) w bezpieczny sposób. Na ogół jest to transport klucza w sejfie pod ścisłą eskortą.

Kryptosystem z kluczem publicznym nie wymaga takich zabiegów. Każdy użytkownik generuje parę kluczy: tajny (deszyfrujący) i publiczny (szyfrujący), publiczny można udostępnić wszystkim, a klucz tajny jest pilnie strzeżoną tajemnicą użytkownika i nie wymaga bezpiecznego transportu. Nadawca szyfruje wiadomość kluczem publicznym odbiorcy. Odbiorca deszyfruje wiadomość własnym kluczem tajnym i tylko on może to uczynić. System ten zapewnia poufność oraz uwierzytelnia odbiorcę.

6.5.3.2. Przykłady szyfrowania

Historia utajniania informacji jest tak stara jak cywilizacja. Literatura przedmiotu dokonuje bardzo obszernej klasyfikacji rodzajów szyfrów. Z uwagi na wspomniane wcześniej ograniczenie tematyki w tym opracowaniu, przedstawimy elementarną ilustrację szyfrowania podstawieniowego i przestawieniowego.

Szyfr podstawieniowy polega na zastępowaniu znaków (bloków) ich ustalonymi zamiennikami. W prostym szyfrze podstawieniowym (monoalfabetycznym) każdą literę tekstu zastępuje się literą otrzymaną w wyniku przesunięcia litery źródłowej o k pozycji alfabetu, a alfabet tworzy cykl zamknięty (tzn. po literze z jest litera a). Kluczem jest tu wielkość k. Szyfr ten nazywa się szyfrem Cezara (Cezar używał go dla k = 3). Ilustracją tego rodzaju szyfrowania jest rys.6.15.



Rys.6.15. *Przykład szyfrowania podstawieniowego*

Szyfr przestawieniowy polega na przestawieniu (permutacji) znaków tekstu jawnego według ustalonego klucza. Ilustracją szyfrowania przestawieniowego jest rysunek 6.16. Algorytm szyfrowania jest tam komentowany w ostatniej kolumnie tabeli.

TEKST JAWNY	TEKST ZASZYFROWANY	ALGORYTM SZYFROWANIA
ALARM␣DLA␣DYWIZJI ←	IJZIWYD␣ALD␣MRALA	Tekst czytany wspak
ALARM␣DLA␣DYWIZJI␣	LARA␣MLD␣AYDIWJZ␣I	Przestawienie dwóch sąsiednich znaków
R A M ␣ A D Z J / A L ␣ L Y I / A D W	R␣JAMADZIL␣LYIADW	Tekst jawny pisany według figury (płot, piła), a tekst zaszyfrowany jest czytany wierszami
A L A R / M ␣ D L / A ␣ D Y / W I Z J / I	AMAWIL␣␣JADDZRLYJ	Tekst jawny wpisany wierszami w prostokąt, a tekst zaszyfrowany jest czytany kolumnami

Rys.6.16. *Przykład szyfrowania przestawieniowego*

Szyfry podstawieniowe monoalfabetyczne są łatwe do złamania przy zastosowaniu analizy częstości występowania liter w szyfrogramie i prostym kojarzeniu

kryptogramu z literami tekstu jawnego. Statystyki występowania liter w poszczególnych językach są znane i na przykład w języku polskim najczęściej występuje litera **a** – 8,5% tekstu pisanego.

6.5.3.3. DES i RSA

Szyfr DES (ang. *Data Encryption Standard*) powstał jako kontynuacja prac nad programem LUCIFER prowadzonych przez firmę IBM. DES został zatwierdzony i wprowadzony przez Narodowe Biuro Normalizacji *(National Bureau of Standard)* do ochrony informacji przez agendy rządowe USA. DES jest szyfrem przestawieniowo - podstawieniowym o długości bloków danych 64 bity. Do szyfrowania używa się klucza mającego 56 użytecznych bitów. Algorytm szyfrowania jest symetryczny, co oznacza, że klucze szyfrujący i deszyfrujący są identyczne.

Algorytm DES został powszechnie udostępniony zainteresowanym, co jest zasadą stosowaną w kryptografii, gdyż powoduje powstawanie nowych idei poprzez wykazywanie słabych punktów publikowanych rozwiązań. Istnieją implentacje sprzętowe umożliwiające szyfrowanie z szybkością kilkudziesięciu Mb/s. Wadą szyfru jest brak jego odporności na tzw. zmasowany atak, czyli poszukiwanie jego 2^{56} wszystkich możliwych kluczy. Częściowe wyobrażenie o tym daje nam tabela 6.12.

Tabela 6.12. Jak szybko można sprawdzić klucze

Szybkość procesora	**Liczba procesorów potrzebna do przestrzeni kluczy w czasie:**		
Liczba testów na sekundę	1 rok	1 tydzień	1 dzień
4 miliony (1990)	600	29800	208500
32 miliony (1995)	75	3700	26100
256 milionów (2000)	9	500	3300

Szyfr RSA (od nazwisk trzech jego twórców: Rivesta, Shamira i Adelmana 1978) należy do grupy szyfrów asymetrycznych. W systemach z kluczem publicznym (asymetrycznym) każdy użytkownik generuje parę kluczy - klucz publiczny. Klucz publiczny zostaje udostępniony wszystkim użytkownikom. Klucz (prywatny) jest dostępny jedynie dla użytkownika, który generował parę kluczy.

Jeśli nadawca chce przesłać informację do odbiorcy, wówczas pobiera klucz publiczny odbiorcy, szyfruje nim informację i zaszyfrowaną przesyła. Tylko odbiorca ma klucz tajny (od pary), a więc tylko on może odczytać informację. W ten sposób realizowana jest usługa poufności (nadawać może wielu, lecz tylko właściwy odbiorca może odczytać informację). Szyfr RSA umożliwia generowanie podpisu cyfrowego (punkt 6.5.3.4). Pozwala na realizację usług autentyfikacji i niezaprzeczalności. Wówczas nadawca szyfruje informację kluczem tajnym, a odbiorca deszyfruje kluczem publicznym. Nadawca jest jeden i nie może się wyprzeć nadania informacji, a o poufność w tym przypadku nie chodzi i każdy może informację odebrać.

Liczba kluczy w algorytmie RSA jest znacznie większa niż w DES, a ponadto istnieje możliwość zwiększenia długości klucza, co w przypadku szyfru DES nie jest możliwe.

Uproszczone porównanie cech kryptosystemów DES i RSA przedstawiono w tab. 6.13.

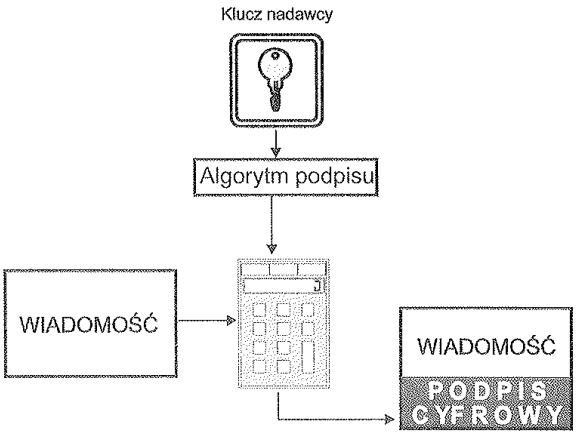
Tabela 6.13. Porównanie systemów DES i RSA

Usługa	**DES**	**RSA**
Poufność	**duże szybkości szyfrowania i deszyfrowania**	małe szybkości szyfrowania i deszyfrowania
Integralność i wierzytelność	**osiągane przy użyciu tego samego przekształcania co poufność**	osiągane przy użyciu innego przekształcenia co poufność
Niezaprzeczalność	trudność generacji podpisu cyfrowego	**łatwość generacji podpisu cyfrowego**
Dystrybucja kluczy	trudna w realizacji	**łatwa w realizacji**

6.5.3.4. Idea podpisu cyfrowego

Podpis cyfrowy jest ciągiem bitów (krótszym od przesyłanej informacji) będącym **funkcją podpisywanej informacji oraz klucza tajnego nadawcy**. **Podpis cyfrowy** w odróżnieniu od podpisu ręcznego zależy od zawartości dokumentu. Mówiąc dokładniej - zależy od skompensowanej próbki dokumentu, gdyż odwzorowania

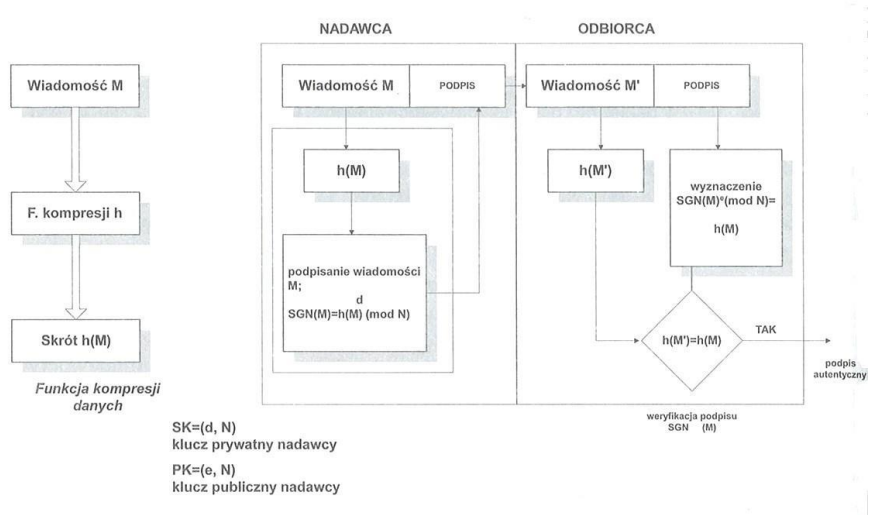
informacji z dokumentu na jej skompensowaną próbkę dokonuje się za pornocą tzw. funkcji skrótu (haszującej - ang. *hash).*



Rys.6.17. *Idea tworzenia podpisu cyfrowego – schemat uproszczony*

Kompensacja (skrót) dokonywana jest - oczywiście - tak, aby dwie różne informacje miały w miarę możliwości różne skróty. Podpis cyfrowy, analogicznie jak podpis ręczny, identyfikuje osobę podpisującą oraz stanowi dowód akceptacji podpisywanego dokumentu.

Podpis cyfrowy umożliwia autentyfikację (autentyzacja i autoryzacja), niezaprzeczalność oraz integralność (nienaruszalność) informacji przesyłanych. W sposób uproszczony ideę podpisu cyfrowego pokazano na rys. 6.17, a dokładniej - na rys. 6.18.



Rys 6.18. *Generacja i weryfikacja podpisu cyfrowego wg schematu RSA*

Jak już zaznaczyliśmy, próbka informacji jest szyfrowana kluczem tajnym nadawcy i dołączona do informacji stanowiąc jej podpis cyfrowy. Całość (informacja + podpis) szyfrowana jest kluczem publicznym odbiorcy (gdy wymagana jest poufność). Odbiorca deszyfruje swoim tajnym kluczem odebraną całość (informacja + podpis), po czym deszyfruje kluczem publicznym nadawcy jego podpis wylicza funkcję skrótu dla przesłanej informacjii porównuje z uzyskaną po zdeszyfrowaniu funkcją skrótu. Zgodność jest gwarancją że podpis cyfrowy dotyczy przesyłanego dokumentu oraz daje gwarancję nienaruszalności informacji. W rozwiązaniu tym możliwe jest sfałszowanie podpisu cyfrowego przez odbiorcę. Ponieważ podpis cyfrowy nie musi być przesyłany łącznie z dokumentem, dlatego może być przesłany do uzgodnionego między nadawcą a odbiorcą arbitra. Taka koncepcja stosowania podpisu cyfrowego jest bezpieczna.

Porównanie cech podpisu ręcznego i cyfrowego przedstawiono w tab. 6.14.

Tabela 6.14. Porównanie podpisu ręcznego i podpisu cyfrowego

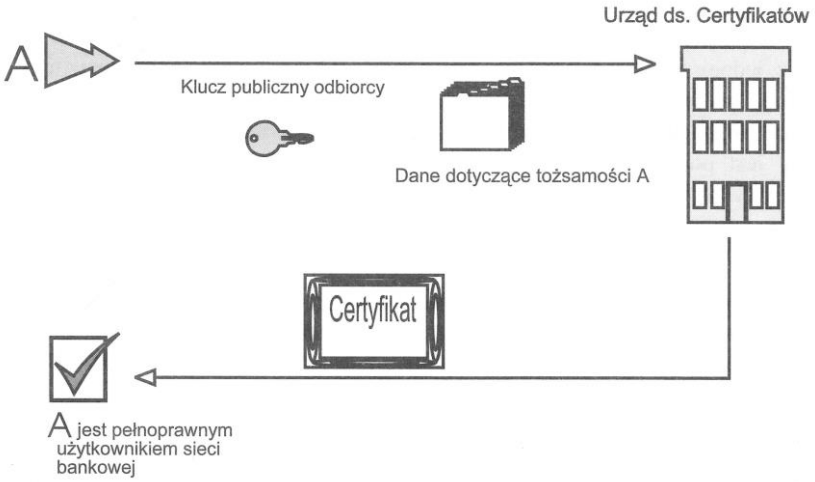
Podpis ręczny	Podpis elektroniczny
Cechy wspólne	
■ Przypisany jednej osobie ■ Niemożliwy do podrobienia ■ Uniemożliwiający wyparcie się go przez autora ■ Łatwy do weryfikacji przez osobę niezależną ■ Łatwy do wygenerowania	
Różnice	
■ Związany nierozłącznie z dokumentem ■ Taki sam dla wszystkich dokumentów ■ Trudny do komputerowej identyfikacji	■ Może być składowany i transmitowany niezależnie od dokumentu ■ Jest funkcją dokumentu ■ Prosta identyfikacja komputerowa

Oprócz zastosowania szyfru RSA w idei podpisu cyfrowego są stosowane są schematy EL-Gamala oraz NIST DSS (1991, *National Institute of Standards and Technology).*

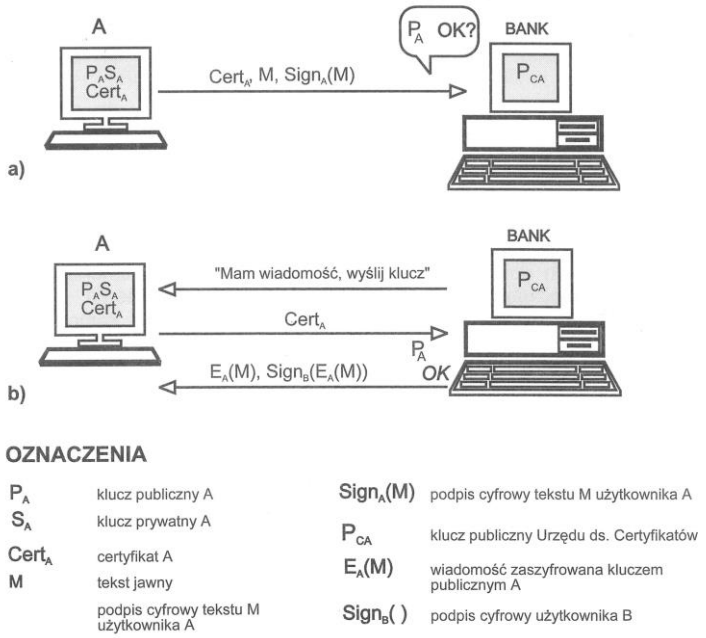
6.5.3.5. Dystrybucja kluczy

W dużych sieciach komputerowych jest praktyczną niemożliwością, aby każdy użytkownik sieci przechowywał klucze publiczne wszystkich swoich korespondentów Właśnie dlatego wprowadza się instytucję pośredniczącą (nadzorującą) zwaną Urzędem do Spraw Certyfikatów CA (ang. *Certification Authority).* Urząd ten ma własną parę kluczy: klucz publiczny PCA (ang. *public)* oraz klucz tajny SCA (ang. *secret)* Klucz publiczny tego urzędu znają wszyscy użytkownicy sieci, klucz tajny zaś jest

wykorzystywany do generacji niemożliwego do podrobienia podpisu łączącego informacje, które stwierdzają tożsamość użytkownika z jego kluczem publicznym. Urząd tworzy informację uwierzytelniającą użytkownika, generuje podpis cyfrowy związany z kluczem publicznym użytkownika i informację uwierzytelniającą go tworząc tzw certyfikat użytkownika i przekazuje tenże certyfikat użytkownikowi. Zasady rejestracji nowego użytkownika w Urzędzie do Spraw Certyfikatów przedstawia rys. 6.19, natomiast sposoby przesyłania podpisanych wiadomości - rys. 6.20.



Rys.6.19. *Rejestracja nowego użytkownika w Urzędzie ds. Certyfikatów*



Rys.6.20. *Wykorzystanie certyfikatów: a) wysłanie podpisanej wiadomości do banku; b) przekaz tajnej informacji z banku*

6.6. Kontrola dostępu do systemu i jego obiektów

W punkcie 6.5.2 omówiono klasyfikację metod utrzymania bezpieczeństwa, w której wydzielono grupę zabezpieczeń programowych. Właśnie do tej klasy zabezpieczeń należą kontrola dostępu oraz diagnostyka antywirusowa. Jak już wcześniej zwróciliśmy uwagę, klasyfikacje nie są ostre, gdyż metody kontroli dostęp są metodologicznie programowe - zawierają elementy sprzętowe (techniczne) czytniki kart magnetycznych lub inteligentnych.

Użytkownik powinien korzystać z systemu komputerowego zgodnie z nadanymi mu przez administratora uprawnieniami. Sprawdzanie tego wymogu jest nazywane kontrolą dostępu, przy czym wyróżnia się kontrolę dostępu do systemu oraz kontrlę dostępu do obiektów systemu. Najlepsze zabezpieczenia fizyczne, techniczne, organizacyjno-administracyjne będą bezużyteczne, jeśli proces przypisywania uprawnień użytkownikom i ich kontrolowania będzie wadliwy. W tym sensie można mówić o komplementarności systemu zabezpieczeń, w którym kontrola dostępu jest problemem fundamentalnym.

6.6.1. Kontrola dostępu do systemu

6.6.1.1 Uwierzytelnianie użytkowników

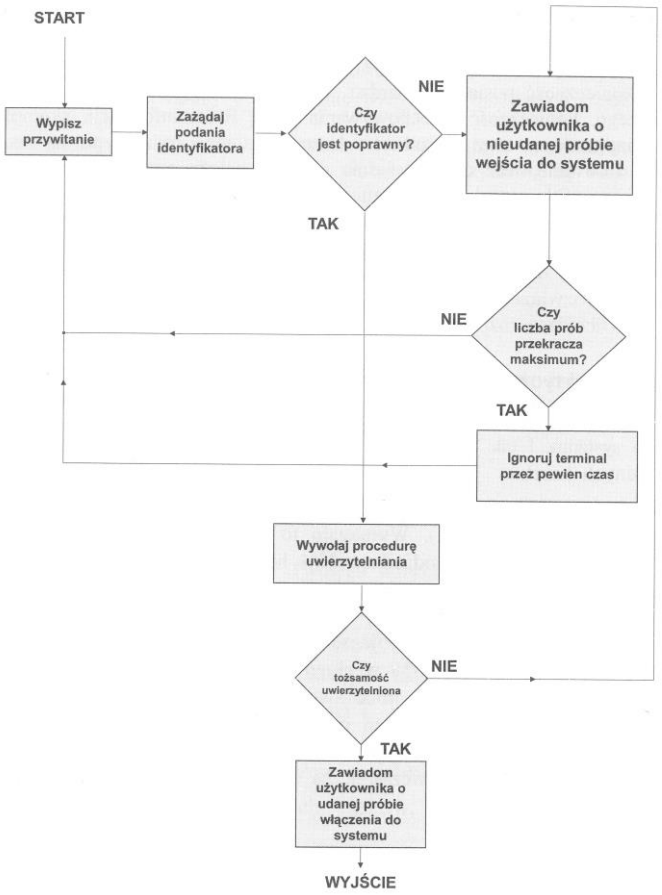
Kontrola dostępu do systemu polega na uwierzytelnieniu „użytkownik” (człowiek), komputer, terminal, karta sprzętowa) przez innego „użytkownika" poprzez analizę charakterystycznych cech. Rozróżnia się trzy metody uwierzytelniania:

- SYK (ang. by something you know – „coś co wiem”) - na podstawie tego co „użytkownik” zna,
- SYH (ang. by something you have – „coś co mam”) - na podstawie tego co „użytkownik” ma (karty, tokeny),
- SYA (ang. by something you are – „coś czym jestem”) - na podstawie tego kim (czym) użytkownik" jest.

Uwierzytelnianie SYK polega na sprawdzaniu przez system informacji, którą posiada użytkownik, np. hasło lub PIN-kod (ang. Personal Identity Number - osobisty numer identyfikacyjny). Wadą tego rozwiązania jest to, że nie da się udowodnić prawa

własności użytkownika do posiadanej informacji (hasła). Nie ma gwarancji, że. hasło nie zostało wykradzione. Zaletą tej metody jest łatwość w stosowaniu (implementacja programów kontrolujących hasła) oraz wygoda dla użytkownika. Oczywiście, przy stosowaniu haseł użytkownicy powinni konsekwentnie przestrzegać wielu reguł. W sposób ogólny procedurę identyfikacji i uwierzytelnienia przedstawiono rys.6.21.

Uwierzytelnianie SYH polega na sprawdzeniu tego co użytkownik ma (np. karta magnetyczna, karta inteligentna, klucz elektroniczny, token). Zaletą jest fakt, że próba podrobienia kart wymaga zaangażowania środków finansowych i technologicznych (sfałszowanie kart magnetycznych jest łatwiejsze niż kart inteligentnych). Wadą tej metody jest wrażliwość kart magnetycznych na zewnętrzne pola magnetyczne, a kart półprzewodnikowych pola elektrostatyczne (wykładziny, odzież z tworzyw sztucznych) powodujące „iskrzenie".



Rys.6.21. *Typowa procedura identyfikacji i uwierzytelniania*

Nasuwa się bardzo prosty wniosek, gdy przeanalizujemy wady i zalety metod SYK i SYH. Otóż jednoczesne stosowanie obu metod w sposób znaczny zwiększa

bezpieczeństwo kontroli dostępu. W zdecydowanej większości publicznych sieci bankomatowych zabezpieczeniami są karta bankomatowa oraz hasło do niej (PIN-kod).

Uwierzytelnianie SYA polega na rozpoznaniu charakterystyk człowieka na podstawie metod biometrycznych lub antropometrycznych. Można weryfikować podpis ręczny, odciski palców, głos, wzór na siatkówce oka, linie papilarne, uzębienie, układ żył. Zaletą tego rodzaju uwierzytelniania jest niepowtarzalność i wystarczająca stałość w czasie tych cech charakterystycznych oraz wygoda użytkownika. Niestety, wadą jest konieczność posiadania bardzo skomplikowanego i kosztownego urządzenia rozpoznającego, konieczność przechowywania dużej ilości informacji, skomplikowany program rozpoznający oraz zawodność. Urządzenia tego rodzaju nie są jeszcze powszechnie stosowane, lecz chyba właśnie do nich należy przyszłość. Istotnym problemem jest w nich margines tolerancji urządzenia, gdyż dane rozpoznawanego użytkownika nie mogą być nigdy identyczne jak wzorcowe (np. podpis użytkownika). Margines tolerancji urządzenia rozpoznającego nie powinien odrzucać uprawnionego użytkownika, natomiast powinien odrzucać użytkownika nie uprawnionego. Ten nie do końca rozwiązany praktycznie problem powoduje największą liczbę tego rodzaju urządzeń rozpoznających.

6.6.1.2. Praktyczne wskazówki wyboru haseł

Należy zasygnalizować fatalny stan zabezpieczeń oceniany na podstaw dostępu do systemu. I tak 23% użytkowników ma łatwe do odgadnięcia hasła, a 21% nie ma żadnych haseł.

Daniel Klein zbadał w USA i Wielkiej Brytanii 13797 plików z hasłami (/etc/passwd w systemie Unix). Wymagało to użycia dwunastu procesorów przez miesiąc (1990 rok). Udało się odgadnąć 25% haseł, z czego 21% już w pierwszym tygodniu, a około 3% już po 5 minutach. Zastosowano w tym badaniu bardzo proste sposoby zgadywania - wyczerpują one listę przeciwwskazań przy tworzeniu haseł, którą przytoczymy. Nadmieńmy jeszcze, że **57% użytkowników nie zmieniało swoich haseł przez pół roku, 13% w ciągu roku, a 1% użytkowników nie zmieniało hasła przez 2 lata.** Warto mieć świadomość tego, jak wiele istnieje możliwości tworzenia haseł. Jeśli przez m oznaczyć liczbę dostępnych na klawiaturze znaków (duża litera i mała litera to znaki różne), a przez n długość hasła liczbę znaków je tworzących, wówczas liczba możliwych do utworzenia hast się wzorem:

$$L_{HASEL} = m^n$$

gdyż z matematycznego punktu widzenia są to wariacje z powtórzeniami, Przyjmując w przybliżeniu m = 100 (na klawiaturze PC wyłączając znaki sterujące można używać 103 znaki) i n = 8 otrzymujemy;

$$L_{HASEŁ} = 100^8 = 10^{16}$$

W niektórych systemach dopuszcza się stosowanie haseł długości n = 32 Proponujemy Czytelnikowi tego opracowania, pouczające ćwiczenie rachunkowe. Należy najpierw teoretyczną szybkość obliczeniową odgadywania haseł, np. 1000/s. Przy ocenie szybkości uwzględniamy czas wygenerowania hasła (w metodzie brutalnego ataku), jego zaszyfrowania (hasła są przechowywane jako zaszyfrowane) i porównania ze wzorcem przechowywanym w pliku haseł. Po założeniu szybkości proponujemy:

– obliczyć, ile haseł można sprawdzić w ciągu miesiąca i jaka to część wszystkich teoretycznie możliwych (czyli prawdopodobieństwo odgadnięcia hasła przez miesiąc),

– obliczyć, ile lat trwałoby odgadywanie wszystkich możliwych haseł.

Jeśli te teoretyczne wyliczenia wyraźnie się rozmijają z cytowanymi wcześniej wynikami badań praktycznych, to właśnie dlatego, że użytkownicy ułatwiają życie intruzom tworząc łatwe hasła.

Powyższa argumentacja skłania nas do przytoczenia tu listy wskazówek, które użytkownik powinien uwzględnić przy wyborze hasła. Przedstawimy ją w dwóch częściach: złe hasła i dobre hasła.

Nie wybieraj jako hasła:

- nazwiska (imienia, pseudonimu, przezwiska) Twojego lub Twojej żony, rodziców, dzieci, przyjaciół, współpracowników, ulubionych postaci (aktorów, sportowców itp.) - w ogóle żadnych nazwisk i imion,
- nazwy używanego systemu operacyjnego,
- nazwy Twojego komputera,

- numeru Twojego telefonu,
- numeru rejestracyjnego i marki Twojego samochodu,
- numeru Twojego ubezpieczenia, prawa jazdy, dowodu osobistego, paszportu, żadnej informacji, którą łatwo o Tobie uzyskać (np. nazwy ulicy),
- czyjejkolwiek daty urodzenia lub w ogóle daty,
- nazwy kontynentu, kraju, miejscowości i w ogóle nazw geograficznych (rzek mórz, gór),
- słów ze słowników, szczególnie słów angielskich,
- ciągu złożonego z identycznych znaków, liter lub cyfr (np. aaaaaaaa, 99999999, ########),
- ciągów kolejnych znaków na klawiaturze (np. qwerty, asdfgh),
- ciągów krótszych niż sześć znaków,
- niczego co wymieniono wyżej - w jakiejkolwiek formie (wspak, dublowanie wyłącznie duże litery), przekleństw i wulgaryzmów.

Wybieraj hasła, które:

- zawierają małe i duże litery,
- zawierają cyfry i znaki specjalne - znaki interpunkcyjne, nawiasy, symbol # @ % $ * itp.,
- mają minimum 8 znaków,
- są łatwe do zapamiętania (aby nie było potrzeby ich zapisywania), lecz trudne do odgadnięcia, np. pierwsze litery wybranego wersu wiersza, piosenki, aforyzmu (np. Bdtt2zccs - Bo do tanga trzeba dwojga zgodnych ciał, chętnych serc),
- można łatwo i szybko wprowadzić z klawiatury (wskazane nie jednym palcem ani jedną ręką aby utrudnić podglądanie osobom trzecim),
- są utworzone przez dwa wyrazy łączone znakiem specjalnym (okocim&lech)

- są tworzone na podstawie ważnej dla Ciebie daty, np. 12.02.1997 (poniedziałek) w ten sposób, że bierzemy dwuliterowe skróty od pierwszych liter nazw cyfr końcowych: dnia, miesiąca, roku oraz nazwy dnia tygodnia (s i d w s i p o),
- są tworzone losowo i podpowiadane przez system.

6.6.1.3. Zasady użytkowania haseł

Wybór właściwego hasła zgodnie z podanymi wskazówkami nie wystarczy. Trzeba bezwzględnie dbać o przestrzeganie następujących praktycznych zaleceń:

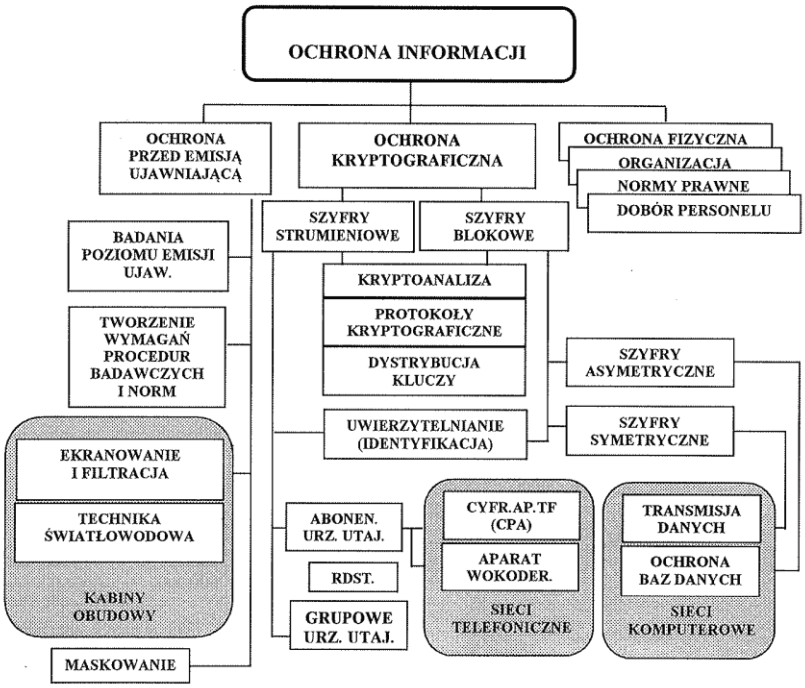
- hasła należy często zmieniać,
- nigdzie nie należy haseł zapisywać,
- podczas wpisywania haseł z klawiatury na ekranie monitora nie powinno być ich echa (dopuszcza się znaki maskujące np. ********)
- po zwolnieniu pracownika z firmy hasła winny być natychmiast zmienione,
- bezskuteczne zgadywanie powinno być limitowane (np. trzykrotne) i po przekroczeniu limitu powinno powodować blokadę systemu,
- zmiana hasła po jego deklarowanym okresie obowiązywania powinna wymuszana przez system,
- wzorce haseł użytkowników powinny być przechowywane w szyfrowanym pliku systemowym,
- hasła mogą być losowo generowane (podpowiadane) przez system,
- administrator systemu może zmienić hasło użytkownikowi, lecz nie może znać haseł wybranych przez użytkownika,
- system powinien wyświetlać czas ostatniego logowania (udanego i nieudanego), po to aby użytkownik mógł reagować na nielegalne próby logowania,
- hasła w szczególnych zabezpieczeniach mogą być dwuczęściowe i wymagać jednoczesnej obecności dwóch osób,
- hasła mogą wymagać uprzednio karty inteligentnej z PIN-kodem,

- mogą być stosowane specyficzne formy kontroli dostępu do systemu:
- jednorazowe hasła według listy,
- hasła uwarunkowane zegarem procesora,
  - typu *challenge - response,*
  - typu dialogowego

Pamiętać trzeba o bardzo ważnej zasadzie, by nawet przy chwilowej przerwie w pracy wylogować się i zakończyć pracę z systemem. Takie bowiem poprawne za kończenie pracy powoduje, że każda następna operacja w systemie musi być ponownie potwierdzona hasłem, czyli użytkownik jest traktowany tak, jakby pracę zaczynał od nowa. Jedną z metod działania intruzów jest „pilne" (!) odwołanie użytkownika od terminalu do rzekomo bardzo ważnych spraw. Użytkownik w pośpiechu opuszcza stanowisko pracy i zapomina zakończyć sesję, a na to tylko czeka intruz, aby pod nieobecność użytkownika wykonać jakąś niecną procedurę, za którą odpowiadać będzie legalny użytkownik terminalu.

6.7. Podsumowanie problematyki ochrony informacji

Podsumowując, całość problemów związanych z ochroną informacji można zoobrazować tak jak to przedstawia rysunek 6.24. Rysunek przedstawia zarówno problemy transmisyjne (światłowody – brak ujawniającego promieniowania elektromagnetycznego, ekranowanie i filtracja, maskowanie), tworzenie koniecznych standardów, ochronę kryptograficzną (szyfry stumieniowe i blokowe) jak i omówione wcześniej problemy ochrony (fizyczna, organizacyjno – prawna i kadrowa), stosowanie urządzeń utajniających indywidualnych (utajnianie u źródła informacji) i grupowych (utajnianie całych traktów – patrz punkt 2.4) aż do ochrony zawartości baz danych.



Rys.6.24. *Całokształt przedsięwzięć związanych z ochroną informacji w systemach teleinformatycznych*