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

AKADEMIA
OBRONY
NARODOWEJ

Płk mgr inż. Zbigniew CIEKANOWSKI

INFRASTRUKTURA TELEKOMUNIKACYJNA JAKO ELEMENT KSZTAŁTOWANIA BEZPIECZEŃSTWA EKONOMICZNEGO POLSKI NA PRZEŁOMIE XX – XXI WIEKU

Rozprawa doktorska

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 58639
II
Akademia Obrony Narodowej

WARSZAWA 2005

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

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ STRATEGICZNO - OBRONNY

INSTYTUT EKONOMII I LOGISTYKI

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 58639
II
Akademii Obrony Narodowej

płk mgr inż. Zbigniew CIEKANOWSKI

INFRASTRUKTURA TELEKOMUNIKACYJNA JAKO ELEMENT KSZTAŁTOWANIA BEZPIECZEŃSTWA EKONOMICZNEGO POLSKI NA PRZEŁOMIE XX÷XXI WIEKU

Rozprawa doktorska

Opracowana pod kierunkiem naukowym

płk. dr. hab. Zenona STACHOWIAKA

WARSZAWA **2005**

SPIS TREŚCI

WSTĘP.....7

1. IDENTYFIKACJA PROBLEMU BEZPIECZEŃSTWA EKONOMICZNEGO I INFRASTRUKTURY TELEKOMUNIKACYJNEJ.....23

1.1. Istota i uwarunkowania kształtowania bezpieczeństwa ekonomicznego państwa.....23

1.1.1. Pojęcie bezpieczeństwa państwa.....23

1.1.2. Uwarunkowania kształtowania bezpieczeństwa państwa.....41

1.1.3. Wyznaczniki i mierniki opisu bezpieczeństwa ekonomicznego państwa.....54

1.2. Istota i uwarunkowania funkcjonowania infrastruktury telekomunikacyjnej.....62

1.2.1. Pojęcia i charakter infrastruktury telekomunikacyjnej państwa.....62

1.2.2. Uwarunkowania kształtowania infrastruktury telekomunikacyjnej.....86

1.2.3. Wyznaczniki i mierniki charakteryzujące infrastrukturę telekomunikacyjną państwa.....93

1.3. Infrastruktura telekomunikacyjna, a bezpieczeństwo ekonomiczne państwa 100

1.3.1. Niedoskonałości infrastruktury telekomunikacyjnej, a zagrożenie bezpieczeństwa ekonomicznego państwa.....100

1.3.2. Wpływ rozwoju infrastruktury telekomunikacyjnej na stan bezpieczeństwa państwa.....102

1.3.3. Wpływ stanu bezpieczeństwa ekonomicznego na kształtowanie i rozwój infrastruktury telekomunikacyjnej.....105

3. MODEL KSZTAŁTOWANIA BEZPIECZEŃSTWA EKONOMICZNEGO W OPARCIU O INFRASTRUKTURĘ TELEKOMUNIKACYJNĄ.....365

3.1. Ogólne założenia uwarunkowań budowy postulatywnego modelu kształtowania bezpieczeństwa ekonomicznego państwa.....365

3.2. Postulowany model kształtowania bezpieczeństwa ekonomicznego państwa i wymagania w zakresie rozwoju infrastruktury telekomunikacyjnej kraju.....389

3.2.1. Formuła sfery realnej modelu kształtowania bezpieczeństwa państwa.....431

3.2.2. Formuła sfery funkcjonalnej modelu kształtowania bezpieczeństwa państwa.....444

3.2.3. Systemy osobowego i kryptograficznego zabezpieczenia infrastruktury telekomunikacyjnej w modelu kształtowania bezpieczeństwa ekonomicznego państwa.....458

3.3. Programy kształtowania infrastruktury telekomunikacyjnej na początku XXI wieku, a założenia postulowanego modelu rozwoju infrastruktury telekomunikacyjnej.....478

3.3.1. Koncepcja kształtowania infrastruktury telekomunikacyjnej na początku XXI wieku.....478

3.3.2. Bariery i zagrożenia realizacji rozwoju infrastruktury telekomunikacyjnej ze strony zasad regulacji rynku telekomunikacyjnego.....487

3.3.3. Bariery i zagrożenia realizacji rozwoju infrastruktury telekomunikacyjnej ze względu na kryteria kształtowania bezpieczeństwa ekonomicznego Polski.....492

ZAKOŃCZENIE.....501

BIBLIOGRAFIA.....517

WYKAZ MAP, SCHEMATÓW, TABEL, WYKRESÓW I ZAŁĄCZNIKÓW.....533

ZAŁĄCZNIKI.....539

2. ANALIZA STANU INFRASTRUKTURY TELEKOMUNIKACYJNEJ I JEJ WPŁYW NA KSZTAŁTOWANIE BEZPIECZEŃSTWA EKONOMICZNEGO W POLSCE NA PRZEŁOMIE XX I XXI WIEKU.....109

2.1. Analiza i ocena stanu infrastruktury telekomunikacyjnej i uwarunkowania jej kształtowania.....109

2.1.1 .Analiza rodzajowa infrastruktury telekomunikacyjnej.....109

2.1.2. Analiza rzeczowo - wartościowa i ocena stanu infrastruktury telekomunikacyjnej w Polsce w latach 1989 ÷ 2003.....245

2.1.3. Analiza rozmieszczenia infrastruktury telekomunikacyjnej.....268

2.2. Analiza i ocena bezpieczeństwa ekonomicznego Polski na przełomie wieku.....281

2.2.1. Analiza uwarunkowań bezpieczeństwa ekonomicznego Polski.....281

2.2.2. Analiza stanu bezpieczeństwa ekonomicznego Polski w latach 1989-2003.....293

2.2.3. Bariery i zagrożenia w procesie kształtowania bezpieczeństwa ekonomicznego Polski.....306

2.3. Analiza i ocena wpływu infrastruktury telekomunikacyjnej na kształtowanie bezpieczeństwa ekonomicznego na przełomie wieku.....321

2.3.1. Analiza wpływu infrastruktury telekomunikacyjnej na kształtowanie bezpieczeństwa ekonomicznego Polski.....321

2.3.2. Ocena wpływu infrastruktury telekomunikacyjnej na kształtowanie bezpieczeństwa ekonomicznego.....326

2.3.2.1. Bariery i zagrożenia dla bezpieczeństwa ekonomicznego Polski ze strony infrastruktury telekomunikacyjnej.....337

2.3.2.2. Szanse i możliwości wzmocnienia bezpieczeństwa ekonomicznego w oparciu o rozwój infrastruktury telekomunikacyjnej.....348

WSTĘP

„Każdy dolar wydany na telekomunikację przynosi kilka dolarów zysku w innych dziedzinach gospodarki."

Pekka Trajanne

Przewodniczący Międzynarodowej Unii Telekomunikacyjnej

Podstawowym celem polityki naszego państwa jest zapewnienie szeroko rozumianego bezpieczeństwa, co stanowi warunek wstępny harmonijnego rozwoju w wymiarze społecznym i gospodarczym. W praktyce polityka ta wyrażana jest w dążeniu do utrzymania suwerenności i nienaruszalności granic RP oraz w rozwijaniu jego potencjału obronnego zdolnego do przeciwdziałania niebezpieczeństwu ewentualnej agresji.

Stosunki międzynarodowe mogą cechować się wzajemnym zrozumieniem, partnerską współpracą i wolą poszukiwania consensusu. Stwarza to możliwość pokojowego i bezpiecznego rozwoju narodu. Brak dobrej woli do negocjacji i określenia warunków porozumienia może doprowadzić do zaostrzenia różnych form wzajemnych oskarżeń, których skutkiem może być stan zagrożenia bezpieczeństwa państwa, a w krańcowych przypadkach - agresja zbrojna. Polska w coraz większym stopniu narażona będzie na skutki wynikające z rozprzestrzeniania technologii podwójnego zastosowania, broni masowego rażenia i środków jej przenoszenia. Problemy te będą występować, zarówno w okresie pokoju, ze względu na położenie geograficzne kraju, który stanowi obszar tranzytowy przy nielegalnym obrocie technologiami i materiałami służącymi do produkcji broni masowego rażenia, jak też w okresie kryzysu i wojny. Wtedy broń masowego rażenia może być użyta przez potencjalnego agresora na wybrane obiekty rozmieszczone w dowolnym miejscu na obszarze państwa.

W świetle zagrożeń występujących aktualnie i mogących mieć miejsce w bliższej i dalszej przyszłości, ogromnego znaczenia nabiera sprawa kierowania systemem obronności państwa. Kierowanie to uznano powszechnie za szczególną formę zarządzania, stanowiącą zespół czynności związanych z racjonalnym wykorzystaniem potencjału ludzkiego, gospodarczego i środków walki na potrzeby obrony kraju przed agresją zbrojną. Kierowanie systemem obronności, a także przygotowaniami do obrony państwa odbywa się w układzie organizacyjno -

bankowości. Nie ma powodu, aby w Polsce było inaczej. Trzeba tylko wiedzieć jakie korzyści dają nowoczesne systemy telekomunikacyjne. Szybkość przemian przede wszystkim ekonomicznych, zachodzących w naszym kraju, nie pozostawia cienia wątpliwości, że możliwość korzystania z telefonu, zwana w telekomunikacyjnym języku usługą powszechną, powinna w możliwie najkrótszym czasie stać się rzeczywiście powszechną. Telefon i usługi telekomunikacyjne powinny być dostępne i osiągalne równie łatwo, jak wiele innych urządzeń w pracy i w domu. Unowocześnienie sieci w domu, wymiana przestarzałych central, instalacja nowoczesnych urządzeń teleinformatycznych, wymaga ogromnych kosztów i czasu. W ciągu kilku lat rozwój telekomunikacji uległ przyspieszeniu, dzięki rozwojowi nowoczesnej technologii, opartej na technice komputerowej. Pojawia się wiele nowych form telekomunikacji i dostępu do nich, szerokie użytkowanie telefonów przenośnych i samochodowych, a w najbliższych latach - transmisja obrazów ruchomych w powiązaniu z telefonami oraz ogromna liczba kombinacji komputerów z urządzeniami telekomunikacyjnymi w różnych miejscach np.: w pracy, miejscu zamieszkania. Uzyskano szybkie wdrożenie postępu technicznego, dużą różnorodność usług, dynamiczny rynek, krótszy okres amortyzacji itp. Zmiany te są wyzwaniem i zarazem stwarzają nowe możliwości. Nowe usługi informacyjne pojawiają się z dnia na dzień. Zadanie udostępnienia telefonu dla każdego mieszkania i zakładu pracy, niezależnie od pozycji społecznej, położenia geograficznego i częstości korzystania, uczyniło usługi publiczne celem nadrzędnym w telekomunikacji. Następuje przyspieszona integracja telekomunikacji, technik przetwarzania danych i środków audiowizualnych.

Obserwując światowe tendencje widzi się, że zmianom ulega samo pojęcie telekomunikacji. Dziś rzadziej kojarzy się ją z zarządzaniem siecią, a przede wszystkim z dynamicznym rozwojem różnorodnych usług telekomunikacyjnych i informatycznych. Uczestnictwo Polski w Unii Europejskiej oraz potrzeba utrzymania ścisłej współpracy z NATO wymuszają konieczność posiadania systemu telekomunikacyjnego, kompatybilnego z ich systemami. Wynika stąd konieczność prowadzenia konsultacji i dokonywania wymiany doświadczeń w dziedzinie organizacji i zabezpieczenia funkcjonowania oraz świadczenia

funkcjonalnym obejmującym: organa władzy, administrację rządową i samorządową z ich ustawowymi kompetencjami, jak również infrastrukturę gospodarczą. Najbardziej newralgicznym okresem w kierowaniu państwem jest przechodzenie z pokojowego systemu kierowania na system wojenny. Dlatego też przyjmuje się zasadę dokonywania jak najmniejszych zmian w kierowaniu państwem w stosunku do zasad i rozwiązań obowiązujących w czasie pokoju.

W celu zapewnienia sprawnego funkcjonowania najwyższych organów władzy, administracji państwa i sił zbrojnych w czasie przechodzenia ze stanu pokojowego na wojenny, już w czasie pokoju tworzy się odpowiednie struktury organizacyjne. Ich zadaniem jest zapewnienie utrzymania ciągłości kierowania oraz sprawnego przejścia gospodarki i sił zbrojnych ze struktury pokojowej na wojenną. W wielu krajach o rozwiniętych demokracjach struktury te są takie same lub zbliżone. System kierowania obronnością państwa, obok podsystemu militarnego i pozamilitarnego jest jednym z zasadniczych elementów systemu obronności. Jego rola polega na informacyjnym sprzężeniu poszczególnych elementów systemu obronności w jednolitą i sprawnie funkcjonującą całość. O jego efektywności decyduje nie tylko właściwy dobór kadr na kierownicze stanowiska i funkcje, ale i jego struktura gospodarcza, a przede wszystkim infrastruktura telekomunikacyjna i informatyczna.

Wzrost ilości informacji we wszystkich obszarach i płaszczyznach ludzkiej działalności spowodował, że informacja obok materii i energii, traktowana jest współcześnie jako trzeci podstawowy element otaczającej nas rzeczywistości. Istota kierowania państwem, zarządzania gospodarką narodową i organizacja bytu społecznego polega na sprawnym przesłaniu informacji na odległość. Dostęp do informacji stał się kluczem do dobrobytu i rozwoju. Informacja jest elementem pojawiającej się gospodarki usługowej i podstawą postępu, wiąże przemysł, usługi i rynki w jedną całość. Staje się to możliwe, dzięki powszechnemu stosowaniu coraz nowocześniejszych środków łączności. Sektor telekomunikacyjny ulega fundamentalnym przemianom. Technika cyfrowa wprowadzana do sieci telefonicznej, zmieniła podłoże telekomunikacji. Dynamiczny postęp techniczny, daje podstawy na przyszłość: sieć cyfrową, światłowody i satelity. Wśród tzw. „złotych branż" - telekomunikacja jest wymieniana na drugim miejscu, zaraz po

Przyglądając się powstającemu na naszych oczach nowemu obszarowi komunikacji, odkrywamy, że jego rozwój zależy w dniu dzisiejszym przede wszystkim od rozwoju sektora telekomunikacyjnego. W procesie rewolucyjnych przemian obrazu dzisiejszego świata słowami kluczowymi stają się więc: komputer, telekomunikacja i multimedia. Społeczne aspekty procesów gromadzenia, przetwarzania, przesyłania i wykorzystania informacji osiągnęły taki stopień natężenia, iż dziedzina ta staje się jednym z immanentnych wskaźników rozwoju bądź zacofania cywilizacyjnego, jak też wyznacznikiem współczesnej społeczności ludzkiej. Z tego też powodu dziedzina teleinformatyki staje się współcześnie jednym z silnie rozwijanych obszarów badawczych.

Świat telekomunikacji, komputerów i mediów przenikają się i zachodzą wzajemnie na siebie integrując się w jeden wielki świat teleinformacji. Znajduje to swoje odbicie w opracowaniach statystycznych, gdzie zaczyna się te dziedziny traktować łącznie. Zamiast mówić o łączach głównych, zaczyna się używać pojęć dostępu do świata informacji, obejmującego zarówno stacjonarny i komórkowy dostęp telefoniczny, komputery, transmisję danych, dostęp do sieci telewizji kablowej i dostęp do internetu. Nawet ujęcie statystyczne telekomunikacji, informatyki i multimediów, przy tak dużej różnorodności usług i urządzeń, nie jest łatwe i proste pomimo, że dane statystyczne i wskaźniki rozwojowe są bardzo dogodnym instrumentem, do analizy i oceny a przede wszystkim planowania rozwoju technicznej infrastruktury telekomunikacyjnej. Dlatego obecnie bardziej adekwatnym sformułowaniem i wierniej odzwierciedlającym otaczającą rzeczywistość jest określenie (pojęcie) infrastruktura teleinformatyczna aniżeli infrastruktura telekomunikacyjna. Z przedstawionych przyczyn w dalszej części opracowania te określenia wystąpią niejednokrotnie zamiennie.

Niezbędnym elementem sprawnego kierowania państwem, zarządzania gospodarką narodową, dowodzenia siłami zbrojnymi oraz kierowania pracą organów bezpieczeństwa państwa jest operatywnie i niezawodnie funkcjonująca łączność. Jej zdolność do wykonywania nałożonych na nią zadań zależy od stanu infrastruktury telekomunikacyjnej (teleinformatycznej) na obszarze kraju, sprawności organizacyjno-technicznej funkcjonujących systemów łączności, ich jakości, przepustowości i niezawodności.

szerokiej gamy usług przez system telekomunikacyjny i informatyczny z przedstawicielami państw Europy Zachodniej.

Potrzeba świadczenia usług telekomunikacyjnych i informatycznych na całym obszarze kraju nie wpłynęła jednak na opracowanie ścisłych ustaw i przepisów prawnych, które stanowią podstawę efektywnej działalności sektora telekomunikacji w innych resortach w zakresie wymiany informacji a obowiązują już od dawna we wszystkich krajach wysoko rozwiniętych. Dlatego też, istnieje pilna konieczność poprawienia tego stanu rzeczy, ponieważ szybki rozwój usług telekomunikacyjnych i przekształcenie ich w system wielousługowy, nadaje telekomunikacji nową rolę w gospodarce i społeczeństwie.

Stan łączności określa stopień doskonałości organizacyjnej społeczeństwa. Procesy informacyjne są generowane przez społeczeństwo, ale jednocześnie współkształtują jego ewolucję[1]. Ta ewolucja u progu XXI wieku jest dość oczywista i prowadzi do społeczeństwa informacyjnego. Rozwijająca się telekomunikacja staje się jednym z podstawowych przedsięwzięć stanowiących wkład w przyszłe społeczeństwo informacyjne[2].

Fundamentem społeczeństwa informacyjnego jest powszechny dostęp do technik informacyjnych. W istniejącej dzisiaj infrastrukturze informacyjnej można wyróżnić trzy „sektory": telekomunikacyjny, informatyczny i mediów elektronicznych. To właśnie te infrastruktury są głównymi stymulatorami współczesnych przemian gospodarczych, społecznych i kulturowych. Poziom rozwoju społeczeństwa informacyjnego jest uzależniony od tempa rozwoju tych sektorów. W związku z rozwojem infrastruktury technicznej społeczeństwo informacyjne ma zapewnioną dostępność do gromadzenia, przetwarzania i przesyłania informacji. Sektor telekomunikacji rozwija się w szybkim tempie i coraz bardziej się ujednolica. Przeprowadzenie jasno zdefiniowanej granicy pomiędzy siecią telekomunikacyjną a informatyczną (komputerową) jest z góry skazane na porażkę. Prowadzi to do przekształcenia telekomunikacji w dominującą siłę, stanowiącą bazę do szerszej działalności gospodarczej, społecznej i kulturalnej.

---

[1]Por. L. Zacher, *Społeczne wymiary efektywności informacyjnej*, Sigma NOT, Warszawa 1990, s. 6.
[2]Por. T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: szanse, wyzwania, zagrożenia*, Wyd. Fundacji Postępu Telekomunikacji, Kraków 1999, s. 31.

rozwiązaniach technicznych. Nie sprzyja to osiąganiu zakładanych celów, lecz powoduje niewspółmierny wzrost nakładów finansowych z budżetu państwa. Taki stan infrastruktury telekomunikacyjnej kraju negatywnie rzutuje nie tylko na realizację zadań obronnych stawianych przez naczelne organy władzy i administracji państwa, jak również na funkcjonalność całego systemu telekomunikacyjnego kraju, a szczególnie uwidacznia się, w stanach zagrożenia bezpieczeństwa państwa. Problemy takie jak: brak dostatecznie pogłębionych uogólnień dotyczących postrzegania infrastruktury telekomunikacyjnej jako elementu kształtowania bezpieczeństwa kraju, a przede wszystkim aktualność bezpieczeństwa ekonomicznego państwa na przełomie XX i XXI wieku, znalazły się w sferze zainteresowań autora, co skłoniło do zajęcia się nimi i opracowania ***pracy doktorskiej*** na temat: ***„Infrastruktura telekomunikacyjna jako element kształtowania bezpieczeństwa ekonomicznego Polski na przełomie XX i XXI wieku".***

Wybór takiego tematu pracy doktorskiej został więc podyktowany względami teoretycznymi, to jest brakiem dostatecznie pogłębionych uogólnień w kwestii roli infrastruktury telekomunikacyjnej w kształtowaniu bezpieczeństwa ekonomicznego państwa oraz względami praktycznymi wyrażającymi się aktualnością tej problematyki w rzeczywistości gospodarczej, politycznej i militarnej Polski na przełomie XX i XXI wieku.

Problem główny rozprawy doktorskiej sformułowany został w postaci pytania następująco: *jaka jest rola i ranga infrastruktury telekomunikacyjnej w kształtowaniu bezpieczeństwa ekonomicznego Polski na przełomie XX i XXI wieku?*

Rozwiązanie tego problemu badawczego wymaga wcześniejszego dania odpowiedzi na zbiór pytań szczegółowych, będących w istocie problemami szczegółowymi rozprawy. Są nimi następujące pytania:

1. *Jakie czynniki wpływają na kształtowanie bezpieczeństwa państwa?*
2. *Czy i w jakim zakresie o bezpieczeństwie państwa stanowi infrastruktura techniczno - ekonomiczna?*
3. *Jaka jest rola i miejsce infrastruktury telekomunikacyjnej w ogóle infrastruktury techniczno - ekonomicznej państwa?*

Szczególnego znaczenia nabiera łączność w okresie zagrożenia bezpieczeństwa państwa[3]. Ochrona i obrona ludzi oraz ich mienia, porządku publicznego, zapobieganie klęskom żywiołowym oraz obrona ustroju państwa jest konstytucyjnym obowiązkiem wszystkich organów władzy i administracji a także organizacji społecznych i gospodarczych. Odmienne i złożone warunki funkcjonowania państwa, charakterystyczne dla stanów nadzwyczajnych, stawiają przed łącznością wysokie wymagania. W celu zapewnienia możliwości ich realizacji niezbędne jest dokonanie w czasie pokoju stosownych przygotowań o charakterze prawnym, organizacyjno - mobilizacyjnym, technicznym i inwestycyjnym.

W procesie kierowania państwem w stanach nadzwyczajnych, zasadniczego znaczenia nabiera, szybkość przekazywania informacji, stopień jej wiarygodności i bezpieczeństwa. Będą to czynniki, które zadecydują o efektywności działań obronnych. Złożoność systemu kierowania obroną państwa, przy uwzględnieniu stosowania nowoczesnych środków technicznych a także środków obrony, zmusza do rozwoju jego materialnej bazy, systemu łączności państwa, opartego na nowoczesnej infrastrukturze telekomunikacyjnej kraju.

W związku z zachodzącymi w ciągu ostatnich lat zmianami jakościowymi (nowe techniki i technologie w telekomunikacji) istnieje pilna potrzeba nowego spojrzenia na systemy łączności. Dotyczy to szczególnie systemów zapewniających kierowanie państwem i dowodzenie siłami zbrojnymi.

Dotychczas funkcjonujący w kraju system łączności nie jest spójny, jak również podzielony na szereg podsystemów, np. sieci użytku publicznego, sieci resortowe, sieci zakładowe i inne. Podział ten stwarza znaczne utrudnienia w obiegu informacji, szczególnie w sytuacjach wykorzystania systemu łączności na potrzeby kierowania i zarządzania państwem, zarówno w czasie pokoju, jak i w warunkach zaistnienia potencjalnych zagrożeń.

Sieci telekomunikacyjne poszczególnych resortów lub instytucji centralnych budowane są własnymi środkami, często się dublują i opierają na różnych

---

[3]W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej. Konstytucja Rzeczpospolitej Polskiej art. 228.

Pomocnym zabiegiem w rozwiązywaniu problemów badawczych pracy oraz osiągnięciu celów pracy stała się weryfikacja hipotez roboczych sformułowanych zarówno o posiadaną wiedzę teoretyczną, jak i doświadczenie zawodowe.

W pracy zweryfikowane zostały następujące ***hipotezy robocze:*** *główna i cząstkowa.*

Hipoteza główna:

Wiele czynników i elementów kształtujących bezpieczeństwo ekonomiczne kraju decyduje o infrastrukturze państwa. W obszarze tym znaczące miejsce zajmuje infrastruktura telekomunikacyjna a szczególnie jej nowe techniki i technologie. Czynnik ten mimo pełnienia istotnej roli kreatywnej w kształtowaniu bezpieczeństwa ekonomicznego jest niedostatecznie postrzegany i oceniany.

Hipotezy cząstkowe:

1. *W polskiej rzeczywistości społeczno - gospodarczej infrastruktura telekomunikacyjna przynależna jest do najbardziej efektywnego, funkcjonującego działu gospodarki narodowej to jest łączności oraz do gałęzi, jaką jest telekomunikacja, która odgrywa znaczącą rolę w kształtowaniu bezpieczeństwa ekonomicznego Polski. Element ten w polskiej gospodarce na przełomie XX i XXI wieku wydaje się być tym, który generuje w największym zakresie nośniki postępu cywilizacyjnego, a w konsekwencji przyczynia się do kształtowania bezpieczeństwa ekonomicznego kraju.*
2. *Kształtowanie bezpieczeństwa ekonomicznego w przyszłości powinno być związane z budową modeli rozwojowych - w tym z modelem kształtowania bezpieczeństwa ekonomicznego kraju w oparciu o rozwój infrastruktury telekomunikacyjnej. Niezbędnym warunkiem staje się prawne, osobowe i kryptograficzne zabezpieczenie systemu infrastruktury telekomunikacyjnej.*
3. *Występuje niebezpieczeństwo zagrożenia systemów informacyjnych infrastruktury telekomunikacyjnej ze strony niedoskonałości osobowego i kryptograficznego zabezpieczenia.*

Rozważania podjęte i przeprowadzone w pracy zostały ograniczone zakresem podmiotowym, przedmiotowym, przestrzennym i czasowym.

4. *Jaka jest istota bezpieczeństwa ekonomicznego państwa?*
5. *Od jakich uwarunkowań zależą procesy kształtowania bezpieczeństwa ekonomicznego?*
6. *Co kryje się pod pojęciem infrastruktury telekomunikacyjnej?*
7. *W jaki sposób stan realny i funkcjonalny infrastruktury telekomunikacyjnej państwa wpływa na kształtowanie bezpieczeństwa ekonomicznego państwa?*
8. *Jakie znaczenie ma infrastruktura telekomunikacyjna dla kształtowania potencjału ekonomicznego państwa?*
9. *Jakie występują zagrożenia dla bezpieczeństwa państwa wynikające z niedoskonałości infrastruktury telekomunikacyjnej?*
10. *Jaki przyjąć system ochrony osobowej, kryptograficznej i prawnej dla zapewnienia bezpieczeństwa ekonomicznego państwa?*

Przyjęta formuła problemów badawczych pracy kierunkuje jej rozważania na osiągnięcie głównego celu badawczego pracy, to jest: *zbudowanie modelu kształtowania bezpieczeństwa ekonomicznego państwa, w oparciu o infrastrukturę telekomunikacyjną kraju.*

Z tak sformułowanego celu ogólnego wynikają następujące ***cele szczegółowe*:**

- *zidentyfikowanie problemów bezpieczeństwa ekonomicznego państwa;*
- *identyfikacja infrastruktury telekomunikacyjnej kraju;*
- *diagnoza stanu infrastruktury telekomunikacyjnej kraju;*
- *ocena stanu infrastruktury telekomunikacyjnej państwa;*
- *określenie wpływu infrastruktury telekomunikacyjnej kraju na kształtowanie bezpieczeństwa ekonomicznego państwa;*
- *wskazanie kierunki rozwoju infrastruktury telekomunikacyjnej w aspekcie bezpieczeństwa ekonomicznego Polski.*

Osiągnięcie założonych celów, wymagało więc poznania problemów bezpieczeństwa ekonomicznego państwa, zbadania istniejących struktur sieci telekomunikacyjnej, a przede wszystkim dokonania analizy i oceny technik i technologii telekomunikacji. Uogólnienia i wnioski wynikające z tej analizy i oceny, pozwoliły z kolei na przedstawienie modelu kształtowania bezpieczeństwa ekonomicznego państwa w oparciu o infrastrukturę telekomunikacyjną.

infrastruktury sieci telekomunikacyjnej i informatycznej (teleinformatycznej) oraz możliwości świadczenia usług teleinformatycznych, a także dokonać oceny jej wpływu na kształtowanie bezpieczeństwa ekonomicznego[4].

Wnioski, uzyskane z ***doświadczeń*** podczas eksploatacji sieci i systemów telekomunikacyjnych, a metoda badania sądów, ***ocen ekspertów*** posłużyła do zdefiniowania prognozy rozwoju i wpływu infrastruktury telekomunikacyjnej do określenia postulowanego modelu kształtowania bezpieczeństwa ekonomicznego.

Analizę i oceny ekspertów jako główne metody badawcze, zastosowano w trakcie studiowania literatury przedmiotu do opracowania wniosków z eksploatacji sieci telekomunikacyjnej, a także do badania elementów składowych bezpieczeństwa ekonomicznego państwa.

Synteza pozwoliła połączyć w określony zbiór, wszystkie badane elementy infrastruktury telekomunikacyjnej i kryteria bezpieczeństwa ekonomicznego w zakresie stawianych wymagań.

Indukcja znalazła wyraz w postrzeganiu zasadniczych elementów rzeczywistej infrastruktury telekomunikacyjnej jako jednego z wielu czynników kształtowania bezpieczeństwa ekonomicznego Polski i budowaniu na nich ogólnego obrazu związków i zależności związanych z bezpieczeństwem ekonomicznym kraju.

Dedukcja sprowadziła się do formułowania ogólnych założeń propozycji i wniosków dotyczących tej problematyki.

Zastosowano również inne metody teoretyczne takie jak**: *prognozowanie, abstrahowanie, porównanie, analogię, uogólnienie***, które wzbogaciły i uzupełniły metody empiryczne.

W określonych etapach badań okazało się bardzo pomocne ***abstrahowanie***, które pozwoliło wyeliminować cechy i elementy systemowe, nie wywierające istotnego wpływu w realizacji głównego celu badawczego.

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

---

[4]Por. J. Pieter, *Z zagadnień pracy naukowej*. Zakład Naukowy im. Osolińskich, Wrocław 1974, s. 23.

Podmiotem są:

- *w ujęciu węższym operatorzy, firmy i przedsiębiorstwa telekomunikacyjne odpowiadające za budowę i utrzymanie infrastruktury telekomunikacyjnej;*
- *w ujęciu szerszym instytucje rządowe i resorty kierujące politykę bezpieczeństwa ekonomicznego państwa i politykę telekomunikacyjną.*

Przedmiotem dociekań są:

- *zagadnienia i kwestie bezpieczeństwa ekonomicznego;*
- *stan infrastruktury telekomunikacyjnej kraju;*
- *relacje pomiędzy bezpieczeństwem ekonomicznym, a infrastrukturą telekomunikacyjną postrzeganą przez pryzmat analizy i oceny wzajemnego wpływu na siebie.*

Zakres przestrzenny podjętych rozważań:

- *obszar Polski.*

Zakres czasowy rozważań:

- *lata przełomu XX i XXI wieku.*

Rozważania podjęte w pracy zostały prowadzone w następujących płaszczyznach:

- ***teoretyczno - metodologicznej,*** na której dokonano identyfikacji istoty i charakteru bezpieczeństwa ekonomicznego oraz sformułowano postulowany model kształtowania bezpieczeństwa ekonomicznego opierając się na infrastrukturze telekomunikacyjnej;
- ***praktyczno - empirycznej,*** na której dokonano analizy i oceny stanu i wpływu infrastruktury telekomunikacyjnej w zakresie kształtowania bezpieczeństwa ekonomicznego.

Złożoność systemu telekomunikacyjnego, a szczególnie jej infrastruktury jest tak obszerna, że konieczne było zastosowanie wielu metod badawczych, które w odniesieniu do bezpieczeństwa ekonomicznego i badanych problemów były najskuteczniejsze i pozwoliły na objęcie wszystkich elementów tych dziedzin oraz wzajemnych powiązań między nimi wraz z otoczeniem zewnętrznym.

W badaniach zastosowano zarówno ***metody empiryczne***, jak i ***teoretyczne metody badawcze***. W metodach empirycznych wykorzystywano głównie ***obserwacje*** *(bezpośrednie i pośrednie),* które pozwoliły poznać budowę, jak i stan

b) publikacje i opracowania z obszaru bezpieczeństwa państwa a szczególnie bezpieczeństwa ekonomicznego;

c) publikacje i opracowania dotyczące infrastruktury telekomunikacyjnej kraju;

Ad. a) Publikacje, dotyczące metodologii badań naukowych stanowiły podstawę rozdziału pierwszego. Do najistotniejszych pozycji z tego zakresu należą: J. Pietera „Ogólna metodologia pracy naukowej" i „Z zagadnień pracy naukowej", M. Cieślaka „Prognozowanie gospodarcze", Cz. Kupisiewicza „Podstawy dydaktyki ogólnej", a szczególnie P. Sienkiewicza „Analiza systemowa".

Literatura ta, zwłaszcza z zakresu rozwiązania metodologicznego badanego problemu i podejścia systemowego, była niezwykle pomocna przy realizacji pracy.

Ad. b) Literatura z obszaru bezpieczeństwa państwa i bezpieczeństwa ekonomicznego została zaprezentowana głównie przez pozycje o charakterze podręcznikowym oraz opracowania i publikacje naukowe.

Wiadomości dotyczące bezpieczeństwa, strategii i obronności państwa zostały zaczerpnięte z opracowań: S. Koziej, F. Wołkowicz „Podstawowe założenia polityki bezpieczeństwa i strategii obronnej", B. Balcerowicz „Sojusz a obrona narodowa", „Patriotyzm Obronność Bezpieczeństwo" praca zbiorowa pod redakcją naukową E. A. Wesołowskiej.

Cennych informacji o teorii ekonomii, polityce gospodarczej i podstawach ekonomiki bezpieczeństwa państwa dostarczyły prace: Z. Stchowiaka „Ekonomia. Zarys podstawowych problemów", i „Ekonomia międzynarodowa wobec wyzwań cywilizacyjnych", J. Płaczka „Ewolucja polskiej myśli obronno-ekonomicznej w latach 1976-2000", „Wybrane problemy ekonomiki bezpieczeństwa", praca zbiorowa pod redakcją naukową Z. Stchowiaka i J. Płaczka.

Interesującą pozycją ze względu na nowoczesny nurt myślenia, traktującą obiektywnie otaczającą rzeczywistość jest praca zbiorowa wykonana pod naukowym kierownictwem B. Balcerowicza „Gospodarcze podstawy bezpieczeństwa państwa wobec wyzwań rozwojowych świata na początku XXI wieku".

W grupie prac naukowo - badawczych inną pozycją poświęconą problemom inżynierii zarządzania a szczególnie systemowi efektywnego wdrażania nowej

W badaniach zastosowano ***podejście systemowe***. Przedmiotem badań jest infrastruktura telekomunikacyjna – sieci telekomunikacyjne i informatyczne (teleinformatyczne), które tworzą system telekomunikacyjny kraju, funkcjonujący w określonym otoczeniu posiadający swą strukturę, a jego elementy m.in. węzły komutacyjne (np. centrale elektroniczne, urządzenia sieci), linie łączności (np. linie kablowe miedziane, światłowodowe, radiowe, satelitarne, itp.) i urządzenia końcowe (np. telefony, faksy, komputery, itp.) tworzą określone podsystemy. W literaturze spotyka się szereg definicji systemu. Jedna z nich najbardziej trafna i ogólna brzmi następująco: „System to uporządkowany wewnętrznie układ elementów tworzący określoną strukturę całościową, wyposażony w obowiązujący zespół norm i reguł, wraz ze środkami zapewniającymi mu funkcjonalność”[5].

Podstawę podjętych dociekań stanowił odpowiednio dobrany i wykorzystany zbiór materiałów źródłowych, który to został poddany krytycznej analizie. Studiowanie oraz analiza literatury naukowej (pozycje zwarte - książki, monografie, opracowania naukowe) i popularnonaukowej (pozycje periodyczne - artykuły prasowe; dokumenty opublikowane przez instytucje badawcze, gospodarcze, rządowe - krajowe i międzynarodowe, materiały statystyczne i inne), miała miejsce w trakcie całego procesu pisania pracy.

Autor zdaje sobie sprawę, że podczas dynamicznego rozwoju infrastruktury telekomunikacyjnej z jednej strony, a zachodzących zmian w jej architekturze funkcjonalnej i fizycznej, a także nowych uwarunkowań dotyczących bezpieczeństwa ekonomicznego państwa z drugiej strony, ukazują się ciągle i będą ukazywać się bieżące coraz nowsze publikacje wnoszące bardziej aktualne treści.

W trakcie badania literatury, dotyczącej podjętego tematu stwierdzono, że pomimo, iż jest ona dość bogata, to obejmuje jednak niektóre zagadnienia w sposób zbyt ogólny, lub też fragmentaryczny. Był to jeden z istotnych czynników, który skłonił do zastosowania metod empirycznych. Przy opracowywaniu pracy doktorskiej, szeroko korzystano z literatury przedmiotu i dokonano jej podziału na następujące grupy:

a) publikacje dotyczące pisarstwa i metodologii badań naukowych;

---

[5]Por. *Teoria systemów,* Praca zbiorowa, pod kier. nauk. D. J. Bema, Politechnika Wrocławska, Wrocław 1975, s. 7.

w tym zakresie były dostępne autorowi opracowania np. „Telekomunikacja w Polsce", „Telekomunikacja w Europie".

Istotne pozycje, dotyczące budowy i usług realizowanych w sieciach telekomunikacyjnych stanowiły: „Nowoczesne techniki i usługi telekomunikacyjne" J. Daneckiego, A. Jajszczyka, również M. Średniawy „Sieci inteligentne – architektura, usługi, zastosowania". Pozwoliły poznać strukturę funkcjonalną i fizyczną sieci inteligentnej, a także zgłębić spełniane funkcje przez określone węzły sieci, jak również poznać zachodzące procesy logiczne. Uzupełnieniem wiadomości o nowoczesnych systemach sieciowych a szczególnie o bezpieczeństwie i ochronie przekazywanych w nich informacji, dostarczyły biuletyny krajowych i zachodnich specjalistycznych firm telekomunikacyjnych.

Wykorzystywane w pracy były także materiały z rokrocznie organizowanego pod patronatem PAN, MŁ, TP S.A., Krajowego Sympozjum Telekomunikacji w Bydgoszczy. Tematyka tego sympozjum, obejmowała problemy rozwoju telekomunikacji w Polsce, na tle rozwoju światowego, problemy sieciowe (teletransmisyjne, komutacyjne, itp.), metodologie, aplikacje, protokoły sieci telekomutacyjnych, oceny niezawodnościowe, zarządzanie, sterowanie sieciami itd.

Zagadnienia projektowania, budowy i eksploatacji systemów telekomunikacyjnych i informatycznych są stałym tematem publikacji w „Przeglądzie Telekomunikacyjnym i Wiadomościach Telekomunikacyjnych", „Teleinfo" i „Telecomforum".

Osobną, charakterystyczną grupę stanowią materiały informacyjne (prospekty) producentów urządzeń i systemów telekomunikacyjnych, stanowiące bazę do analizy rozwiązań technicznych, eksploatacyjnych i utrzymaniowych oraz ekonomicznych.

Układ rozprawy doktorskiej *został podporządkowany przyjętym założeniom.* Praca składa się ze wstępu kreślącego ideę rozwiązania problemów podjętych w pracy, trzech rozdziałów części głównej, zakończenia, bibliografii, a także wykazu schematów, rysunków, tabel i wykresów.

Rozdział pierwszy zatytułowany *Identyfikacja problemu bezpieczeństwa ekonomicznego i infrastruktury telekomunikacyjnej* koncentruje uwagę na istocie i uwarunkowaniach kształtowania bezpieczeństwa ekonomicznego państwa, istocie

techniki w warunkach gospodarki rynkowej jest opracowanie W. J. Wesołowskiego „Metodyka inżynieryjna tworzenia struktur systemów gospodarczych". Natomiast teoria i praktyka zarządzania, szczególnie zarządzanie systemami informacyjnymi przedstawione w podręczniku R. W. Griffina „Podstawy zarządzania organizacjami".

Problemy optymalizacji, analizy i syntezy jak i reorganizacji przedsiębiorstw z punktu widzenia ekonomiki zostały opisane w pracy J. Pepparda, P. Rowlanda „Re-engineering".

Również materiały z seminarium i konferencji naukowych w AON i innych placówek dydaktycznych oraz naukowo – badawczych, stanowiły cenny materiał o mechanizmach kształtowania bezpieczeństwa ekonomicznego z punktu widzenia strategii obronnej.

Ad. c) Literatura dotycząca infrastruktury telekomunikacyjnej została zaprezentowana głównie przez pozycje o charakterze podręcznikowym, publikacje naukowe i techniczne. Wł. Majewski „Systemy sieci zintegrowanej", autor charakteryzuje systemy teletransmisyjne i komutacyjne z modulacją cyfrową. Przedstawia prognozy i etapy wdrażania ich do eksploatacji. Pozycja bardzo aktualna, zwłaszcza że krajowa sieć teletransmisyjna i komutacyjna jest rozbudowywana pod kątem przyszłościowej sieci zintegrowanej. Praca zbiorowa pod redakcją M. Dąbrowskiego „Sterowanie i oprogramowanie w telekomunikacyjnych sieciach zintegrowanych". W książce omówiono problemy współczesnych sieci telekomunikacyjnych ze szczególnym uwzględnieniem oprogramowania i sterowania w sieciach cyfrowych z integracją usług.

Podręczniki D. Bema „Systemy telekomunikacyjne" część 1 i część 2, A. Dąbrowskiego „Systemy i sieci SDH" pozwoliły pogłębić problematykę związaną ze współczesnymi sieciami telekomunikacyjnymi. Cennych informacji o miejscu i roli telekomunikacji w życiu społeczeństwa i jej wpływie na jego rozwój, dostarczyło opracowanie T. Goban - Klasa i P. Sienkiewicza „Społeczeństwo informacyjne - szanse, zagrożenia, wyzwania". Interesujące są w tej grupie, pozycje poświęcone systemom telekomunikacyjnym PDH, SDH i ATM. Opisane są problemy optymalizacji, analizy i syntezy sieci telekomunikacyjnej z punktu widzenia jej efektywności. Uzupełnieniem literatury

1. IDENTYFIKACJA PROBLEMU BEZPIECZEŃSTWA EKONOMICZNEGO I INFRASTRUKTURY TELEKOMUNIKACYJNEJ

1.1. Istota i uwarunkowania kształtowania bezpieczeństwa ekonomicznego państwa

1.1.1. Pojęcie bezpieczeństwa państwa

Procesy zachodzące w Europie i świecie, szczególnie w ostatnich latach, prowadzą do sytuacji, w której następują przeobrażenia ustrojowe, społeczno-polityczne, ekonomiczno-gospodarcze i militarne o trudnych do przewidzenia skutkach. Zachodzi zatem potrzeba modyfikacji poglądów dotyczących bezpieczeństwa narodowego lub państwa, jego zagrożeń oraz gwarancji tego bezpieczeństwa.

Bezpieczeństwo narodowe można rozpatrywać na wielu płaszczyznach. Po pierwsze, jako stan wynikający z określonej sytuacji: społecznej, politycznej, ekonomicznej i militarnej (wojskowej), który odzwierciedla poziom warunków zaspokajania podstawowych potrzeb oraz nadrzędne wartości danego narodu[6]. Po drugie, może być traktowane jako swoista sytuacja, w której sprzeczności (wewnętrzne lub zewnętrzne) interesów, dążeń, aspiracji i hierarchii uznawanych wartości nie prowadzą do wystąpienia niebezpiecznych zjawisk (zagrożeń, kryzysów lub konfliktów[7]). Wreszcie, może być traktowane jako proces zapewniający warunki do przetrwania i niezakłóconego rozwoju narodu znajdującego się w obliczu zagrożeń (wewnętrznych lub zewnętrznych) stabilności i suwerenności[8].

Bezpieczeństwo każdego państwa zawiera w sobie, oprócz treści wspólnych dla wszystkich krajów, pewne specyficzne elementy wnikające z uwarunkowań wewnętrznych i zewnętrznych, historii, tradycji, kultury i wartości uznawanych za nadrzędne. Znajduje to wyraz m.in. w definicjach bezpieczeństwa narodowego.

Podstawowym interesem każdego państwa i narodu jest jego bezpieczeństwo. Bezpieczeństwo jest wartością powszechną i często jako kategoria jest definiowane zarówno w naukach społecznych, jak i naukach ścisłych - od

---

[6]Por. A. D. Rotfeld, *Bezpieczeństwo Polski a Bezpieczeństwo Europy,* w: *„Sprawy Międzynarodowe"* 1984 nr 7, s. 39.

[7]Por. S. Koziej, F. Wołkowicz, *Podstawowe założenia polityki bezpieczeństwa i strategii obronnej*, AON, Warszawa 1998, s. 7.

[8]Por. C. Rutkowski. *Bezpieczeństwo i obronność: strategie-koncepcje-doktryny,* AON, Warszawa 1995, s. 27.

i uwarunkowaniach funkcjonowania infrastruktury telekomunikacyjnej oraz na relacjach infrastruktura telekomunikacyjna, a bezpieczeństwo ekonomiczne państwa.

Rozdział drugi pod tytułem *Analiza stanu infrastruktury telekomunikacyjnej i jej wpływu na kształtowanie bezpieczeństwa ekonomicznego w Polsce na przełomie XX i XXI wieku* przedstawia analizę stanu infrastruktury telekomunikacyjnej i uwarunkowania jej kształtowania, analizę i ocenę bezpieczeństwa ekonomicznego Polski na przełomie wieku oraz analizę i ocenę wpływu infrastruktury telekomunikacyjnej na kształtowanie bezpieczeństwa ekonomicznego Polski.

Rozdział trzeci noszący tytuł *Model kształtowania bezpieczeństwa ekonomicznego w oparciu o infrastrukturę telekomunikacyjną* proponuje formułę postulowanego modelu infrastruktury telekomunikacyjnej gwarantującej bezpieczeństwo państwa, w tym bezpieczeństwo ekonomiczne oraz programy kształtowania infrastruktury telekomunikacyjnej na początku XXI wieku.

Pracę zakończono ogólnymi wnioskami, przedstawionymi w *Zakończeniu* dotyczącymi postulowanego modelu infrastruktury telekomunikacyjnej i kierunkami jej kształtowania oraz prowadzenia dalszych prac badawczo - rozwojowych.

Pojęcie bezpieczeństwa nabiera ciągle nowego znaczenia, z czym idzie w parze różnorodność, a nawet dowolność jego wykładni. Owa pojemność znaczeniowa i możliwości interpretacyjne wynikają nie tylko z różnorakich tradycji, z różnic wielkości, położenia i szczególnych interesów państw, nie tylko z tendencji rozwojowych społeczności międzynarodowej, które wręcz wymuszają coraz szersze rozumienie owego pojęcia, lecz również z jego dotychczasowej, obiektywno-subiektywnej natury. Z jednej bowiem strony bezpieczeństwo jest stanem określonym przez zespół czynników wymiernych i okoliczności poddających się racjonalnemu osądowi, z drugiej zaś oznacza mniej lub bardziej subiektywne poczucie narodu i sił nim rządzących, iż państwo jest bezpieczne lub nie.

Współzależności między państwami, a także możliwości wpływania państw silnych na sytuację militarną, ekonomiczną i polityczną regionów geograficznie nawet odległych spowodowały wzajemną podejrzliwość. Wynika ona nie tylko z faktów, lecz – w większym zapewne stopniu - z wyobrażeń i przewidywań co do zachowań innych państw na arenie międzynarodowej, przede wszystkim sąsiadów oraz mocarstw mających pośredni wpływ na sytuację w sferze bezpieczeństwa danego kraju.

Bezpieczeństwo to z jednej strony pewien system wartości stanowiący o jego istocie, z drugiej zaś - zespół środków wartości te zabezpieczających. Do wartości podstawowych składających się na treść bezpieczeństwa należą przede wszystkim:

- przetrwanie państwa (narodu);
- integralność terytorialna;
- niezależność polityczna;
- suwerenność wyboru ustroju społeczno-politycznego;
- brak zagrożenia militarnego;
- możliwość podejmowania decyzji z zakresu polityki wewnętrznej i zewnętrznej;
- zachowanie stanu równowagi między zagrożeniem, wywołanym możliwością zaistnienia konfliktu a potencjałem obronnym zagrożonej strony;

filozofii i psychologii do nauk technicznych. Z tych to powodów bezpieczeństwo odnoszące się do różnych podmiotów i przedmiotów może być odmiennie interpretowane.

Zgodnie z definicjami i określeniami zawartymi w słownikach i encyklopediach ***bezpieczeństwo*** jest pojęciem interdyscyplinarnym występującym na gruncie różnych nauk, posiadającym wiele definicji dalekich od precyzji naukowej i trudnym do jednoznacznego zdefiniowania.

Bezpieczeństwo można rozumieć jako: stan niezagrożenia, spokoju, pewności; osobiste bezpieczeństwo; bezpieczeństwo kraju, obywateli; poczucie bezpieczeństwa; zapewnie komuś bezpieczeństwo; czuwanie nad czyimś bezpieczeństwem[9].

Bezpieczeństwo to stan, w którym jednostka, grupa społeczna, organizacja, państwo nie odczuwa zagrożenia swego istnienia lub podstawowych interesów; sytuacja, w której istnieją formalne, instytucjonalne, praktyczne gwarancje ochrony. Stąd pojęcia: bezpieczeństwo psychiczne, osobiste, publiczne, finansowe, ekonomiczne, socjalne, międzynarodowe[10].

Bezpieczeństwo - stan, który daje poczucie pewności, i gwarancje jego zachowania oraz szansę na doskonalenie. Jest jedną z podstawowych potrzeb człowieka i sytuacją odznaczającą się brakiem ryzyka utraty czegoś co człowiek szczególnie ceni, na przykład zdrowia, pracy, szacunku, uczuć, dóbr materialnych. Wyróżnia się m.in. bezpieczeństwo globalne, regionalne, narodowe; bezpieczeństwo militarne, polityczne, społeczne; bezpieczeństwo fizyczne, psychiczne, socjalne; bezpieczeństwo strukturalne i personalne[11].

Zgodnie z Konstytucją Rzeczypospolitej Polskiej jednym z podstawowych celów funkcjonowania naszego państwa i jego struktur jest zapewnienie bezpieczeństwa bytu i warunków rozwoju obywateli przy jednoczesnym poszanowaniu ich osobistej wolności[12].

---

[9]Por. M. Szymczak, *Komputerowy słownik języka polskiego*, PWN, Warszawa 2003.
[10]Por. R. Smolski, M. Smolski, E. H. Stadtmüller, *Słownik Encyklopedyczny. Edukacja Obywatelska,* Europa, Warszawa 1999.
[11]Por. *Słownik terminów z zakresu psychologii dowodzenia i zarządzania,* MON, Warszawa 2000, s. 17.
[12] Por. Artykuł 5 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997.

W teorii stosunków międzynarodowych mówiąc o bezpieczeństwie państwa, akcentuje się istnienie oraz pewność przetrwania (brak zagrożenia państwa i jego ochronę przed zagrożeniami). Natomiast mówiąc o bezpieczeństwie narodowym, w znaczeniu ogólnospołecznym, podkreśla się zaspokojenie takich potrzeb, jak: istnienie, pewność przetrwania, tożsamość, ochrona poziomu i jakości życia.

Utożsamianie pojęć bezpieczeństwa państwa i bezpieczeństwa narodowego znajduje uzasadnienie w logice związków państwo-naród. Jeśli przyjąć, że państwo jest globalną organizacją społeczeństwa kształtującą zachowanie obywateli (zamieszkujących dane terytorium) za pośrednictwem norm prawa, opatrzonych sankcją przymusu państwowego, to dopuszczalnym jest zmienne taktowanie pojęcia „państwo" takimi terminami jak kraj, naród, ojczyzna, społeczeństwo. Przy czym, we współczesnym ujęciu „naród" - to społeczeństwo obywatelskie, w odróżnieniu od „nacji" traktowanej jako synonim narodowości.

Stosując pewne uproszczenia państwo, to jego obywatele i terytorium[16]. Podstawowym warunkiem skutecznego działania w dziedzinie bezpieczeństwa i obronności jest jednolita interpretacja podstawowych pojęć i kategorii. W literaturze przedmiotu można znaleźć wiele definicji dotyczących bezpieczeństwa. Szereg z nich zostało przytoczonych.

Bezpieczeństwo narodowe, zgodnie z powszechnie przyjętymi zasadami, rozumiane jest szeroko jako stan uzyskany w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i niemilitarnymi, tak zewnętrznymi, jak i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin działalności państwa[17]. Bezpieczeństwo narodowe, jak wspominano uprzednio, często nazywane również bezpieczeństwem państwa, jest złożoną funkcją, obejmującą problematykę przeciwstawiania się wszelkim zagrożeniom dla istnienia oraz rozwoju narodu i państwa - zarówno zewnętrznym, jak i wewnętrznym.

Bezpieczeństwo państwa - stan uzyskany w wyniku zorganizowanej ochrony

---

[16]Por. Z. Stachowiak, *Identyfikacja bezpieczeństwa ekonomicznego państwa – jego istota, uwarunkowania i umiejscowienie w ogólnym problemie bytu narodu i państwa.* Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego Polski z punktu widzenia narodowej i sojuszniczej strategii obronnej. Praca zbiorowa, pod kier. nauk. Z. Stachowiaka, AON, Warszawa 2001, s. 16.

[17]Por. *Słownik terminów z zakresu bezpieczeństwa narodowego.* Praca zbiorowa, pod kier. nauk. J. Pawłowskiego, AON, Warszawa 2002, s. 173.

- jakość życia społeczeństwa - zachowanie odpowiedniego standardu życia (efektywność gospodarcza, stan środowiska naturalnego, konsumpcję dóbr i usług, zatrudnienie, stabilność cen);
- perspektywy wszechstronnego rozwoju.

Bezpieczeństwo jest naczelną potrzebą państw i systemów międzynarodowych, a jego brak wywołuje niepokój i poczucie zagrożenia. Wynika z tego, że o stanie bezpieczeństwa państwa nie stanowi tylko jego potencjał militarny, ale również sytuacja społeczno-polityczna, stan gospodarki itp.[13].

Bezpieczeństwo narodowe - stan świadomości społecznej, w którym istniejący poziom zagrożeń, dzięki posiadanym zdolnościom obronnym, nie budzi obaw, lęku o zachowanie (osiągnięcie) uznanych wartości[14]. Definicję tę rozumie się jako brak zagrożenia i poczucia zagrożenia podstawowych dla danego narodu wartości, a mianowicie politycznych, ideologicznych, gospodarczych, cywilizacyjnych oraz kulturalnych, zapewniających swobodny rozwój życia duchowego i tożsamości narodowej.

Bezpieczeństwo państwa - taki rzeczywisty stan stabilności wewnętrznej i suwerenności państwa, który odzwierciedla brak lub występowanie jakichkolwiek zagrożeń (w sensie zaspokajania podstawowych potrzeb egzystencjalnych i behawioralnych społeczeństwa oraz traktowania państwa jako suwerennego podmiotu w stosunkach międzynarodowych)[15]. Pojęcie to akcentuje kwestię woli przetrwania, a więc zachowania własnej egzystencji i tożsamości, suwerenności i integralności terytorialno-geofizycznej, politycznej, militarnej poprzez rozwój wewnętrzny lub ekspansję zewnętrzną.

Definicje bezpieczeństwa narodowego i bezpieczeństwa państwa formułowane są na podstawie realnych uwarunkowań historycznych, geopolitycznych, gospodarczych, demograficznych, cywilizacyjnych oraz ocen i przewidywań polityczno - wojskowych. Terminy bezpieczeństwa państwa i bezpieczeństwa narodowego, pomimo dostrzegalnych różnic, często używane są zamiennie, gdyż zakorzeniły się w naszej terminologii i powszechnie są stosowane.

---

[13]Por. S. Dworecki, *Od konfliktu do wojny*, BUWIK, Warszawa 1996, s. 13.
[14]Por. C. Rutkowski, ...wyd. cyt., s. 30.
[15]Por. S. Dworecki, *Zagrożenia bezpieczeństwa państwa*, AON, Warszawa 1994, s. 16.

zastosowania wobec niego przemocy zbrojnej (militarnej)[24]. Najogólniej można stwierdzić, bezpieczeństwo militarne to przeciwstawienie się zagrożeniom militarnym przy użyciu sił zbrojnych.

Zagrożenie niemilitarne – to rodzaj zagrożenia obejmujący taki splot zdarzeń w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju państwa, ewentualnie naruszenie jego suwerenności w wyniku zastosowania wobec niego przemocy niezbrojnej[25].

Zagrożenia wojenne są szczególnym rodzajem zagrożeń państwa, skierowane są bowiem w podstawy istnienia narodów i państw. Tworzy je zestaw różnorodnych zagrożeń występujących jednocześnie, wśród których główną rolę odgrywa zagrożenie militarne. Jest ono pojęciem szerszym niż zagrożenie militarne, ponieważ wojna, zwłaszcza wojna współczesna, obejmuje nie tylko działania zbrojne, ale także różnorodne działania pozazbrojne (społeczne, ekonomiczne, informacyjne itp.). Groźba agresji nie należy wprawdzie do zagrożeń dnia dzisiejszego, ale nie może być też wykluczona.

Zagrożenie polityczne – to stan, w którym nasilają się działania zorganizowanych grup społecznych (politycznych) uniemożliwiające wypełnianie przez państwo jego głównych funkcji, a przez to osłabiające lub niweczące działania organów lub instytucji realizujących cele i interesy narodowe[26].

Zagrożenie ekonomiczne (gospodarcze) – to rodzaj zagrożenia bezpieczeństwa państwa w wyniku którego może nastąpić osłabienie jego potencjału gospodarczego.

Zagrożenie ekologiczne – to rodzaj zagrożenia, w wyniku którego może nastąpić niebezpieczeństwo dla istot żywych, na skutek zmiany środowiska naturalnego.

Zagrożenie bezpieczeństwa państwa[27]– to splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w którym z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju

---

[24]Por. S. Dworecki, *Zagrożenia* ... wyd. cyt., s.25.
[25]Por. *Słownik terminów* ...wyd. cyt., s. 167.
[26]Tamże, s. 167.
[27]Por. S. Dworecki, *Zagrożenia*... wyd. cyt., s. 61.

i obrony przed możliwymi zagrożeniami, wyrażony stosunkiem potencjału obronnego do skali zagrożeń[18].

Zagrożenie – z jednej strony to pewien stan psychiczny lub świadomościowy wywołany postrzeganiem zjawisk, które subiektywnie ocenia się jako niekorzystne lub niebezpieczne, a z drugiej czynniki obiektywne powodujące stany niepewności i obaw[19]. Pojęcia „zagrozić", „zagrażać", oznaczają tyle „co postraszyć czymś kogoś, zapowiedzieć coś złego, ostrzec pod groźbą jakichś konsekwencji, stać się niebezpiecznym, groźnym dla kogoś, czegoś lub coś zagraża zdrowiu, bezpieczeństwu"[20].

Zagrożenie - sytuacja, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia[21]. Zagrożenia ze względu na ich źródło najogólniej dzieli się na zewnętrzne i wewnętrzne. W konsekwencji wyróżnia się bezpieczeństwo zewnętrzne i wewnętrzne. Przyjmując za podstawę dziedziny, w których może wystąpić zagrożenie, wyróżnia się: zagrożenia militarne i niemilitarne. Wśród zagrożeń niemilitarnych można z kolei wyróżnić: zagrożenie polityczne; zagrożenie gospodarcze; zagrożenie psychospołeczne, czy też zagrożenie ekologiczne i inne.

Zagrożenie zewnętrzne – to ten rodzaj zagrożenia, w wyniku którego zwiększone jest prawdopodobieństwo utraty lub ograniczenia suwerenności czy też integralności terytorialnej państwa. Źródłem tego zagrożenia jest inne państwo (najczęściej ościenne)[22].

Zagrożenie wewnętrzne – to ten rodzaj zagrożenia, w wyniku którego powstaje prawdopodobieństwo zmniejszenia się zdolności organów władzy do utrzymania ładu i porządku publicznego w państwie[23].

Zagrożenie militarne państwa - to splot zdarzeń w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju państwa, albo naruszenie bądź utrata jego suwerenności i integralności terytorialnej – w wyniku

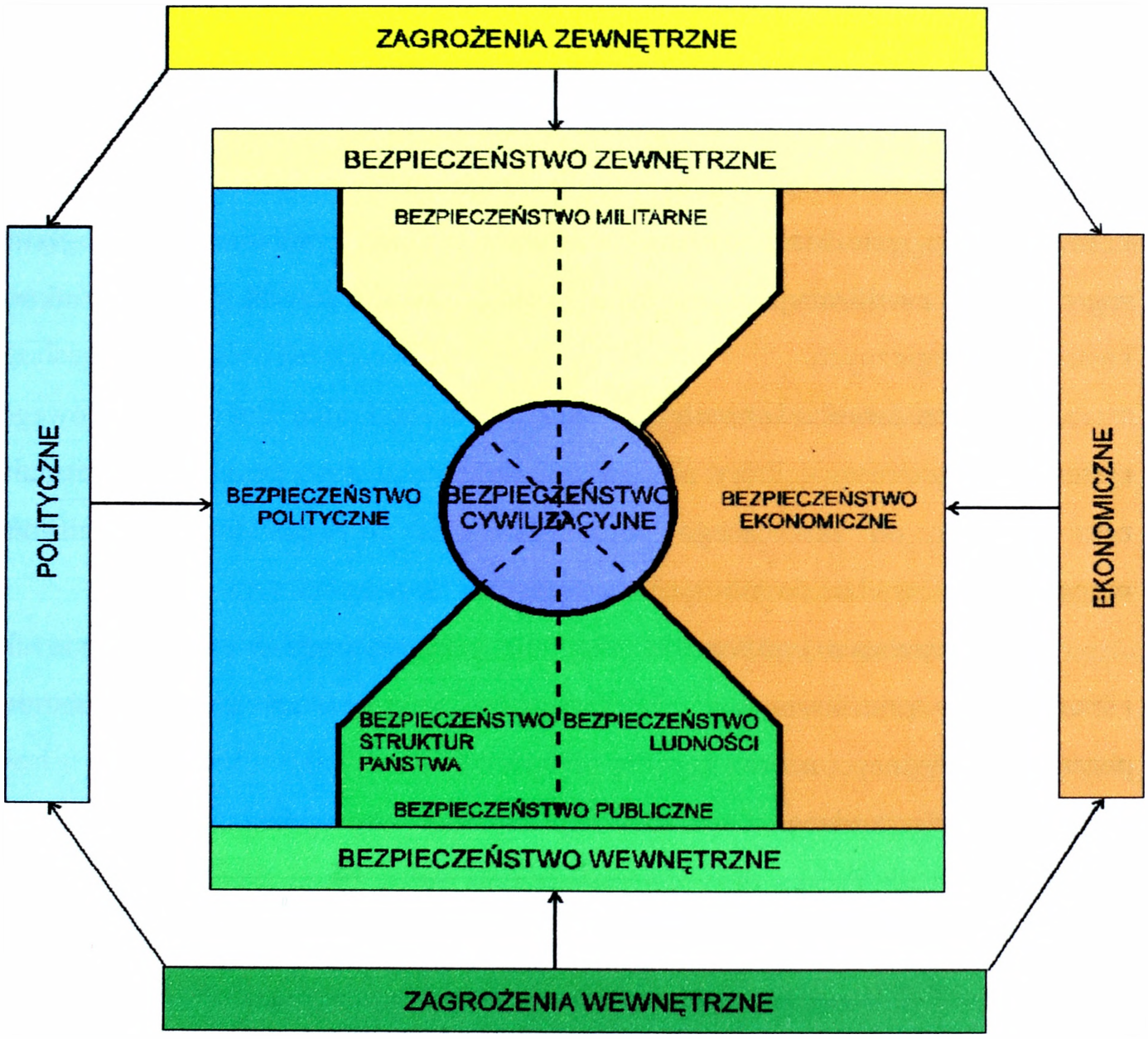
---

[18]Por. *Słownik podstawowych terminów dotyczących bezpieczeństwa państwa.* AON, Warszawa 1994, s. 6.
[19]Por. S. Korycki, *System bezpieczeństwa Polski*, AON, Warszawa 1994 s.54.
[20]Por. *Komputerowy słownik języka polskiego, PWN*, PWN, Warszawa 1998.
[21]Por. *Słownik terminów* ... wyd. cyt., s. 166.
[22]Tamże, s. 168.
[23]Tamże, s. 168.

Bezpieczeństwo zbiorowe - to system polityczno-prawny mający na celu utrwalenie pokoju przez ustanowienie zakazu agresji i zobowiązanie się do pomocy państwu, które padnie ofiarą agresji[29].

Schemat 1.1.

Idea bezpieczeństwa państwa



Źródło: S. Koziej, F. Wołkowicz, *Podstawowe założenia polityki bezpieczeństwa i strategii obronnej*, AON, Warszawa 1998, s. 9.

Bezpieczeństwo terytorialne oznacza integralność terytorialną kraju i nienaruszalność jego granic. Zależne jest ono od wielkości, wyposażenia i wyszkolenia sił zbrojnych, których zadaniem jest odstraszanie i obrona kraju.

---

[29]Por. M Szymczak, *Komputerowy...* wyd. cyt., s. 57.

wewnętrznego bądź naruszenie lub utrata suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych, w wyniku zastosowania przemocy politycznej, psychologicznej, ekonomicznej, militarnej itp.

Odwołując się do wskazanych cech bezpieczeństwa i zagrożeń dla niego, w określonym czasie możemy powiedzieć, że państwo jest lub nie będzie bezpieczne. Bezpieczne będzie, jeżeli jego byt niczym nie jest lub nie będzie zagrożony. W przeciwnym razie wystąpi stan zagrożenia, a w skrajnym przypadku może dojść nawet do sytuacji utraty bezpieczeństwa państwa. Faktyczny stan bezpieczeństwa państwa może być większy lub mniejszy niż jego subiektywne postrzeganie przez społeczeństwo.

Zagrożenie bezpieczeństwa państwa będzie tym większe, im większe będzie poczucie zachwiania stabilności wewnętrznej bądź utraty suwerenności, mogących powodować wystąpienie zagrożenia militarnego. Wydaje się, że wiele zjawisk stanowi zagrożenie, lecz istotny jest stopień ich szkodliwości - wpływu na byt i rozwój społeczny. Z tego też względu w czasie pokoju, kryzysu i wojny istnieją zagrożenia podobne lub różniące się co do skali i rodzaju, przy czym wojna sama w sobie stanowi najwyższą formę zagrożenia.

Specjalną odmianą zagrożeń, obecnie bardzo aktualną, są zagrożenia terrorystyczne będące następstwem kryzysu polityczno-militarnego w otoczeniu państwa, czyli w sytuacji, w której co prawda nie występuje groźba bezpośredniej agresji na dane państwo, ale która stwarza zagrożenia pośrednie.

Obecnie w Europie jak również na świecie jednym ze szczególnie istotnych problemów jest kształtowanie relacji między systemami bezpieczeństwa narodowego i międzynarodowego (Schemat 1.1.).

Bezpieczeństwo międzynarodowe, to „pewien układ stosunków międzynarodowych, zapewniający wspólne bezpieczeństwo państw. Wiąże się ze świadomymi działaniami społeczności międzynarodowych oraz jest wynikiem międzynarodowych procesów i zjawisk, które wpływają na eliminację konfliktów zbrojnych, stabilizację polityczną, zrównoważony rozwój gospodarczy, minimalizowanie skutków globalnych problemów”[28].

---

[28]Por. Smolski R., Smolski M., Stadtmüller E. H., *Słownik*... wyd .cyt., s. 39.

System obronny państwa należy rozumieć jako – skoordynowany wewnętrznie zbiór elementów organizacyjnych, ludzkich i materiałowych wzajemnie powiązanych i działających na rzecz obrony państwa[32].

Obronność – jedna z podstawowych dziedzin działalności państwa, mająca na celu przeciwdziałanie wszelkiego rodzaju zagrożeniom[33]. Jest ona szczególną dziedziną bezpieczeństwa narodowego, czyli taką funkcją państwa, która dotyczy przeciwstawiania się wszelkimi posiadanymi środkami (militarnymi i niemilitarnymi) zagrożeniom wojennym, a przede wszystkim militarnym, stanowiącym sedno zagrożeń wojennych (Schemat 1.2.).

Obrona narodowa to działalność mająca na celu odpowiednie przygotowanie i wykorzystanie sił i środków będących do dyspozycji państwa dla przeciwdziałania wszelkiego rodzaju zagrożeniom zewnętrznym i wewnętrznym godzącym w interes narodowy[34].

Kształtowanie obronności (obrony narodowej) odbywa się w ramach realizacji polityki, strategii i doktryny obronnej. Te trzy kategorie pojęciowe należą do podstawowych kategorii z zakresu obronności.

Polityka bezpieczeństwa narodowego jest elementem polityki państwa dotyczącej przedsięwzięć związanych z tworzeniem i wykorzystaniem potencjału obronnego w celu zapobiegania i przeciwdziałania różnego rodzaju zagrożeniom[35]. Jest to zespół działań informacyjno-propagandowych, dyplomatycznych, ekonomicznych, militarnych i innych prowadzonych przez państwo w celu przeciwstawienia się zagrożeniom i ich skutkom.

Strategia obronności – to dziedzina strategii bezpieczeństwa, obejmująca tworzenie, rozwój, przygotowanie i wykorzystanie potencjału obronnego państwa do przeciwdziałania zagrożeniom militarnym, zarówno w wymiarze narodowym jak i sojuszniczym, ujmowana w skali celów ogólnych i mająca charakter długofalowy[36]. Jest częścią polityki i jednocześnie częścią szerszej strategii bezpieczeństwa narodowego. Zajmuje się ona sposobami realizacji polityki

---

[32]Por. *Biuletyn informacyjny nr 1/159*, Szt. Gen. WP, Warszawa 1994, s. 7.
[33]Tamże, s. 84.
[34]Por. *Słownik terminów* ... wyd. cyt., s. 82.
[35]Tamże, s. 100.
[36]Tamże, s. 133.

Bezpieczeństwo militarne – to zdolność przeciwstawienia się zagrożeniom militarnym państwa przy użyciu sił zbrojnych.

Bezpieczeństwo polityczne - obejmuje przygotowanie naczelnych organów władzy i administracji państwowej do przeciwstawienia się zagrożeniom politycznym państwa (zarówno wewnętrznym, jak i zewnętrznym) w zakresie systemu politycznego, społecznego, gospodarczego i kulturalnego, według własnej tradycji z zachowaniem odrębności narodowej.

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

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

Bezpieczeństwo ekonomiczne państwa to taki stan rozwoju krajowego systemu gospodarczego, który zapewnia wysoką sprawność jego funkcjonowania oraz zdolność do skutecznego przeciwstawienia się zewnętrznym naciskom mogącym doprowadzić do zaburzeń rozwojowych[30].

Bezpieczeństwo publiczne - obejmuje przygotowanie i utrzymywanie sił i środków do przeciwstawienia się wszelkim zagrożeniom struktur państwa, porządku publicznego, ochrony życia i zdrowia obywateli[31].

Wraz ze zmianami w sferze polityczno - gospodarczej i militarnej w ostatnich latach Polska dąży do zapewnienia sobie bezpieczeństwa w ramach euroatlantyckich struktur bezpieczeństwa międzynarodowego. W tym celu Rzeczpospolita Polska utrzymuje i doskonali swój system bezpieczeństwa, a w tym głównie system obronny państwa. Skład, struktura i zasady funkcjonowania systemu obronnego w czasie pokoju i wojny uwarunkowane są szeregiem różnorodnych czynników, wśród których najistotniejsza jest ocena ewentualnych zagrożeń i wynikających z nich potrzeb obronnych, a także kierunku działań nakreślonych przez politykę bezpieczeństwa państwa.

---

[30]Por. Z. Stachowiak, *Bezpieczeństwo ekonomiczne*, w: *Ekonomika obrony*, Praca zbiorowa pod red. Stankiewicza, AON, Warszawa 1994, s. 186.
[31]Por. S. Koziej, F. Wołkowicz, *Podstawowe*... wyd. cyt., s. 8.

Relacje i zależności między bezpieczeństwem państwa a obronnością są hierarchicznie zależne, natomiast między polityką i strategią występują bardzo wyraźne wzajemne uwarunkowania. Praktyka rozwoju systemu obronnego państwa opiera się na podstawach teoretycznych obejmujących elementy zagrożeń i organizację przeciwdziałania. Istotą procesu decyzyjnego związanego z przeciwdziałaniem występowaniu sytuacji zagrożenia bezpieczeństwa państwa jest identyfikacja stanu zagrożenia oraz wybór racjonalnej strategii przeciwdziałania adekwatnej do stwierdzonej sytuacji zagrożenia.

Jak już poprzednio wspomniano, bezpieczeństwo państwa jest kategorią wielowymiarową i może być realizowane na wielu płaszczyznach. Stanowi ono zbiór wielu składowych elementów: politycznych, militarnych, terytorialnych, i ekonomicznych. Pozwala to z kolei wyróżnić jego podstawowe rodzaje, takie jak: bezpieczeństwo militarne, terytorialne, polityczne i ekonomiczne.

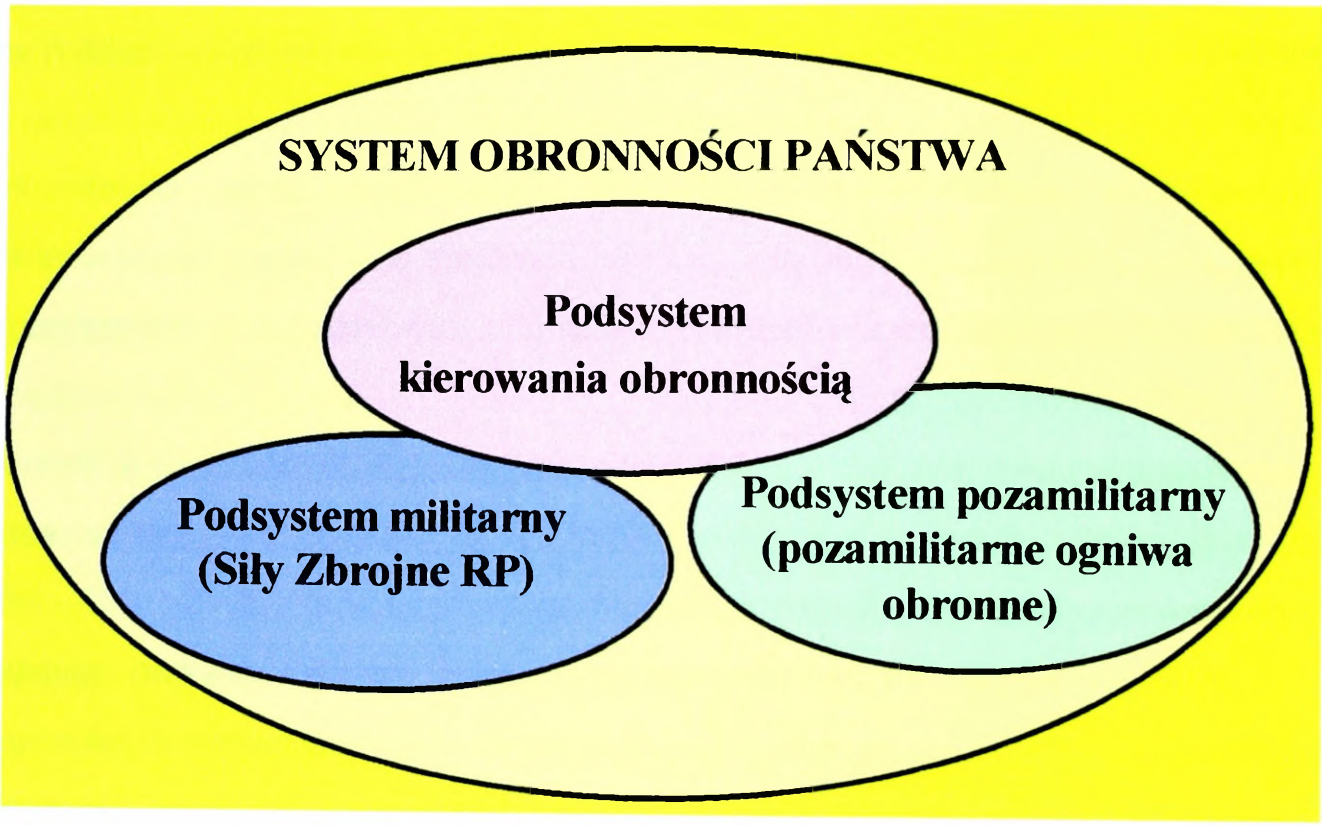
Bezpieczeństwo ekonomiczne jest istotną częścią, jednym z filarów bezpieczeństwa państwa, bowiem wartości w sferze ekonomicznej bardzo silnie wpływają na określenie racji stanu. Z tych powodów należy przedstawić sposoby rozumienia i umiejscowienia komponentu ekonomicznego bezpieczeństwa w strukturze bezpieczeństwa państwa. Na tej podstawie staje się możliwe określenie podstawowych wartości w płaszczyźnie ekonomicznej, które mogą stanowić podstawę analiz i ocen bezpieczeństwa ekonomicznego.

Pojęcie bezpieczeństwa ekonomicznego wyrosło z ogólnego ujęcia pojęcia bezpieczeństwa. Zostało dowartościowane w nim znaczenie zagrożenia jakości życia jednostki, grupy społecznej i państwa, a także dostrzeżono zagrożenia, jakie mogą mieć wpływ na jakość życia tych podmiotów. Zauważono również, iż zbytnie skoncentrowanie się na aspekcie militarnym bezpieczeństwa narodowego, może się przyczynić do utraty odpowiedniego poziomu w innych aspektach bezpieczeństwa począwszy od poziomu życia, a skończywszy na kulturze narodowej. Wpłynęło to na rozumienie zagrożeń jako zjawisk złożonych, mogących mieć wpływ na jakość życia jednostek, państw, organizacji państw, ale także jako zjawisk mogących mieć wpływ na poziom samodzielności podmiotów stosunków międzynarodowych - ekonomicznych i politycznych - w danym czasie.

obronnej. Jej istotą jest optymalizacja użycia sił i środków wydzielonych przez państwo do realizacji celów i zadań określonych przez politykę. Oznacza to stosowne korygowanie ustalonych celów, wydzielanych środków oraz przyjmowanych sposobów postępowania państwa w dziedzinie obronności.

Schemat 1.2.

System obronności państwa



Doktryna bezpieczeństwa państwa jest jedną z doktryn państwa, która jest oficjalnie przyjętym przez kierownictwo państwa systemem założeń i zasad działania w dziedzinie polityki bezpieczeństwa[37]. Stanowi ona polityczno-strategiczny zestaw obowiązujących w danym czasie celów obronnych oraz zasad i założeń ich osiągania. Jest jednocześnie częścią szerszej doktryny bezpieczeństwa narodowego. Doktryna opublikowana w oficjalnych dokumentach państwowych zawiera w swej istocie strategiczną decyzję co do podstawowych zasad i założeń polityki obronnej, czyli co do możliwości przeciwdziałania wszystkim zagrożeniom, a szczególnie zagrożeniom kryzysowym. W tej sytuacji problematyka reagowania kryzysowego staje się podstawowym składnikiem współczesnych koncepcji doktrynalnych w dziedzinie obronności.

---

[37]Tamże, s. 23.

- ogólny stan zależności ekonomicznych, określających stopień efektywności zewnętrznej ingerencji ekonomicznej w wewnętrzny rozwój gospodarczy, zdolność obronną i stabilność systemu społeczno-politycznego danego kraju;
- wyobrażenie, co do rzeczywistych, względnie potencjalnych zagrożeń gospodarczych kraju, które określają stopień efektywności rozwoju gospodarczego, zdolności obronnej i stabilności systemu społeczno-politycznego danego kraju;
- wyraz stopnia podatności danego państwa na przeniesienie przez płaszczyznę gospodarczą, głównie przez transmisję kanałami i mechanizmami, zależności ekonomicznych, działań o charakterze politycznym skierowanych na osłabienie bezpieczeństwa państwa[38].

Można stwierdzić że, bezpieczeństwo ekonomiczne jest wypadkową wielu czynników, w tym:

- przyszłości – która to charakteryzuje się dużym stopniem niepewności i wysokim stopniem nieprzewidywalności;
- położenia i obszaru państwa oraz posiadanych zasobów naturalnych;
- rozwoju gospodarczego, naukowo-technicznego, kulturowego itp.;
- międzynarodowych powiązań gospodarczych;
- płaszczyzn oddziałujących na kształt struktur państwa, tzn. społeczno-gospodarczej i wojenno-obronnej.

W literaturze przedmiotu można się spotkać z ujęciem bezpieczeństwa ekonomicznego jako instrumentu służącego do zapewnienia kontaktów z otaczającym dany podmiot środowiskiem oraz mającego wpływ na pozycję na arenie międzynarodowej. Występują także takie ujęcia tej problematyki, iż bezpieczeństwo ekonomiczne jest nie tylko instrumentem działalności zewnętrznej danego podmiotu, ale także ma wpływ na jego wnętrze. Wpływa bowiem nie tylko na poziom bezpieczeństwa sfery gospodarczej, ale posiada znaczący wpływ na sferę militarną, rozwój społeczno-kulturowy narodu, rozwój naukowo-techniczny, a także na poziom życia itd.

---

[38]Z. Stachowiak, *Bezpieczeństwo ekonomiczne,* w: *Ekonomika obrony,* pod red, W. Stankiewicza, AON, Warszawa 1994, s. 187-188.

Takie pojmowanie zagrożeń przyczyniło się do powstania współczesnego rozumienia bezpieczeństwa państwa jako zjawiska wielowymiarowego, interdyscyplinarnego, o znacznie uszczuplonym aspekcie militarnym - choć nie marginalizowanym - dającym równouprawnienie problematyce kulturowej, ekonomicznej, ekologicznej, ideologicznej i społecznej.

Znaczenie jakie przypisuje się poszczególnym rodzajom bezpieczeństwa jest wypadkową szeroko rozumianych uwarunkowań wewnętrznych i zewnętrznych w ujęciu politycznym, gospodarczym, kulturowym itd. Jednak wydaje się, iż szczególne znaczenie dla zachowania bezpieczeństwa państwa ma bezpieczeństwo ekonomiczne. Wynika to ze strategii, jaką przyjęły najbardziej rozwinięte państwa, które uważają, iż celem nadrzędnym jest zapewnienie dobrobytu jednostce i społeczeństwu przez harmonijny rozwój gospodarki narodowej i ekspansję na inne rynki narodowe.

Bezpieczeństwo ekonomiczne - jako jeden z wymiarów bezpieczeństwa państwa - przenika wszelkie sfery życia społecznego i państwowego. W ujęciu podmiotowym, można je rozpatrywać jako jeden z elementów bezpieczeństwa w odniesieniu do: jednostki (osobiste), grupy społecznej, narodu (państwa), grupy państw (regionalne), kontynentu (ponadregionalne), całej ludzkości (globalne).

Określenie istoty pojęcia *bezpieczeństwa ekonomicznego* wymaga uszczegółowienia jego zakresu. Z tego punktu widzenia może być ono postrzegane jako:

- zdolność systemu gospodarczego (państwa, grupy państw, regionu, świata) do takiego wykorzystania wewnętrznych czynników rozwoju i międzynarodowych współzależności ekonomicznych, aby zagwarantować w miarę możliwości rozwój;
- wypadkowa czynników rozwoju gospodarczego i ograniczających go barier, tkwiących we wszystkich czynnikach jego kształtowania;
- bilans potrzeb rozwojowych i możliwości ich zaspokojenia;
- stan gospodarki i jej struktur oraz stosunków gospodarczych i powiązań umożliwiających skuteczne przeciwstawienie się negatywnym oddziaływaniom zewnętrznym, które mogą osłabić rozwój gospodarczy, stabilność systemu społeczno-politycznego i zdolność obronną;

Bezpieczeństwo ekonomiczne można ujmować jako środek do uzyskania i utrzymania stabilności wewnętrznej oraz odgrywania stosownej roli w obszarze międzynarodowym, tak w ujęciu politycznym, jak i ekonomicznym.

Istota bezpieczeństwa ekonomicznego wskazuje, iż jego osiągnięcie może przebiegać dwoma drogami. Pierwsza droga, polega na tym, że bezpieczeństwo ekonomiczne byłoby kształtowane przez wzrost własnej siły ekonomicznej w stosunku do innych państw. Jest to jednak postawa konfliktogenna, powodująca narastanie szeregu sytuacji kryzysowych w stosunkach międzynarodowych, które mogą się uwidaczniać np. w sferze politycznej, militarnej, ekonomicznej, itd.

Druga droga, w swych założeniach sprowadza się do tworzenia między państwami (ugrupowaniami państw) szeregu powiązań, wytworzenia szerokiej współpracy. Stosunki gospodarcze będą korzystnie stymulowały relacje dwu- i wielostronne przez budowę głębokich powiązań gospodarczych, wykorzystywanie zaś siły zbrojnej w stosunkach międzynarodowych byłoby nieopłacalne dla uczestników konfliktu, zapewne też i dla krajów niezaangażowanych.

Bez względu na poziom z którego rozpatrujemy dany aspekt, bezpieczeństwo ekonomiczne (państwa, regionalne) ujawnia się na dwóch płaszczyznach:

- pierwszej - społeczno - ekonomicznej (nazywanej także ogólnogospodarczą), która odnosi się do takiego rozwoju gospodarki kraju, który jest w stanie zapewnić trwanie i rozwój gospodarki w międzynarodowej grze wolnorynkowej; z tej płaszczyzny wypływają następujące składowe bezpieczeństwa ekonomicznego: bezpieczeństwo socjalne, żywnościowe, finansowe, surowcowe, energetyczne i ekologiczne;
- drugiej - obronno - wojskowej, która jest zjawiskiem bardzo złożonym i wielowymiarowym, a przy jej rozpatrywaniu winno się zdefiniować pojęcie ekonomicznego bezpieczeństwa obronnego, postrzeganego jako zdolność systemu gospodarczego państwa (grupy państw złączonych wspólnym układem) do efektywnego niezagrożonego rozwoju potencjału obronno-ekonomicznego i funkcjonowania gospodarki obronnej.

Najbardziej trafną i najpełniejszą definicją *bezpieczeństwa ekonomicznego* wydaje się być definicja Z. Stachowiaka, który podkreśla, *że jest to taki stan rozwoju krajowego systemu gospodarczego, który zapewnia wysoką sprawność jego funkcjonowania - poprzez należyte wykorzystanie wewnętrznych czynników rozwoju oraz zdolność do skutecznego przeciwstawienia się zewnętrznym naciskom, mogącym doprowadzić do zaburzeń rozwojowych. Jego tworzenie i utrzymanie ma ograniczony charakter, a to ze względu na występowanie we współczesnym świecie współzależności i zależności ekonomicznych, wpływających ograniczająco na sferę krajowej suwerenności*[39].

Z prezentowanej definicji wynika, iż aby osiągnąć pożądany poziom bezpieczeństwa ekonomicznego państwa, należy skorelować ze sobą następujące elementy:

a) poziom kierowania (zarządzania) państwem, który będąc jednym z motorów napędowych rozwoju gospodarki narodowej, przyczyniłby się do osiągania pożądanego poziomu dobrobytu jednostki;
b) rozwój gospodarczy, zapewniający trwanie i rozwój państwa (narodu);
c) wielokierunkowy system przepływu informacji między wszelkimi sferami życia podmiotu i otaczającym go środowiskiem;
d) system wykrywania i likwidowania lub zmniejszania niekorzystnych skutków zagrożeń, zarówno zewnętrznych, jak i wewnętrznych.

Ogólnie można stwierdzić, że bezpieczeństwo ekonomiczne jest takim poziomem rozwoju gospodarki danego podmiotu gospodarczego (jednostki, państwa, organizacji itd.), który zapewnia mu harmonijny rozwój i efektywne wykorzystywanie szans i zagrożeń wypływających z otaczającego środowiska. Jednocześnie jest to świadome działanie na rzecz rozwoju własnego systemu gospodarczego, który może być postrzegany jako wyznacznik rozwoju innych dziedzin oraz generowania i wykorzystywania szeregu instrumentów ekonomicznych, które pozwoliłyby na trwanie i rozwój państwa (narodu), a także wzrost dobrobytu jednostki.

---

[39]Tamże, s. 189.

oddziaływania destrukcyjne;

- drugi, agresywny - określany mianem potencjału negatywnego, mający możliwości destrukcyjnego oddziaływania na inne podmioty.

Polska dąży do zapewnienia sobie bezpieczeństwa w ramach euroatlantyckich struktur bezpieczeństwa międzynarodowego. Poczucie bezpieczeństwa dotyczy wszystkich dziedzin życia i działalności człowieka tworząc wielowymiarowy wektor komfortu psychicznego ludzi „czujących się bezpiecznymi", stąd też i zagrożenia tegoż bezpieczeństwa obejmują całe spektrum zjawisk odbierających ten komfort w poszczególnych dziedzinach życia i działalności, bądź ich różnorodnej konfiguracji. Z większością zagrożeń zmuszeni jesteśmy radzić sobie sami, jednakże są zagrożenia, które przekraczają nie tylko możliwości pojedynczych osób, ale całych społeczeństw. Przeciwdziałanie tym zagrożeniom i usuwanie ich skutków wzbudza w ostatnich latach duże zainteresowanie wśród polityków i decydentów, którzy tym społeczeństwom przewodzą.

Należy podkreślić, że wejście w struktury wspólnego, euroatlantyckiego bezpieczeństwa nie jest celem samym w sobie, jest ono jedynie etapem i jednym z zadań strategicznych na drodze do zapewnienia możliwości osiągnięcia celu nadrzędnego, jakim jest zagwarantowanie suwerenności i nienaruszalności. Tak pokaźne obszary pozwalają na pokazanie uwarunkowań rządzących kształtem bezpieczeństwa ekonomicznego.

1.1.2. Uwarunkowania kształtowania bezpieczeństwa państwa

Obecnie we współczesnym świecie oprócz ustroju i systemu społeczno - ekonomicznego, na działalność państwa w odniesieniu do bezpieczeństwa i gospodarki narodowej oraz możliwości wyboru w tych dziedzinach, wpływa wiele czynników. Bezpieczeństwo Polski, na przestrzeni ostatnich kilku lat kształtuje się w zupełnie odmiennych niż dotąd warunkach. Zmiany, jakie zaszły w Europie Środkowej i Wschodniej, stworzyły nowe uwarunkowania bezpieczeństwa państwa. Polska znalazła się między zjednoczoną Europą, a państwami budującymi młode demokracje. Państwo funkcjonuje w bliższym lub dalszym otoczeniu międzynarodowym mającym wpływ na tworzenie się i funkcjonowanie różnych

W przytoczonej definicji wyróżnia się dwie płaszczyzny, mające bezpośredni wpływ na poziom ekonomicznego bezpieczeństwa obronnego[40]:

- zewnętrzną, czyli możliwość przeciwstawiania się zagrożeniom, jakie są generowane przez otaczające państwo środowisko;
- wewnętrzną, w której szczególny nacisk kładzie się na rozwój potencjału obronno-ekonomicznego wypływającego z potencjału ekonomicznego państwa, przy czym należy zaznaczyć, iż wzrost lub spadek jednego, nie pociąga w każdym wypadku analogicznego zjawiska w drugim obszarze.

Następnym problemem jest stwierdzenie, z jakich opcji jest kreowana istota bezpieczeństwa ekonomicznego państwa.

Pierwsza opcja - pozytywna - wyraża się postrzeganiem bezpieczeństwa ekonomicznego przez perspektywę elementów tworzących i decydujących o jego poziomie, tzn. dostrzeganie określonych cech i wartości kreujących bezpieczeństwo ekonomiczne, tj. określenie niezbędnego poziomu zaspokojenia potrzeb jednostki i narodu, wykreowanie systemu, który zapewniłby trwanie, rozwój, integralność terytorialną, niepodległość, suwerenność polityczną, ekonomiczną itd., tożsamość narodową, kulturową itd. oraz dobrobyt w skali państwa, a także jednostki. Opcja pozytywna posiada dwie sfery, które decydują o jej kształcie: realną, czyli to, co już istnieje, ze wszystkimi pozytywami i negatywami i regulacyjną, tj. sferę polityczną wraz z prognostycznym ujęciem.

Takie podejście pozwala na ujęcie bezpieczeństwa ekonomicznego jako zespołu właściwości gospodarki narodowej, na które można mieć wpływ.

Druga opcja - negatywna - sprowadza się do postrzegania bezpieczeństwa ekonomicznego z perspektywy, zarówno istniejących, jak i zakładanych zagrożeń, czyli definiowanie bezpieczeństwa ekonomicznego przez to, czym nie jest.

Z tak rozumianego bezpieczeństwa ekonomicznego można wygenerować dwa przeciwstawne obszary:

- pierwszy, obronny - generujący odpornościowe zachowania zagrożonego systemu, przez co gospodarka narodowa staje się mniej wrażliwa na

---

[40]Por. Z. Kołodziejak, *Bezpieczeństwo ekonomiczne - geneza, uwarunkowania, zakres pojęciowy aktualności* w: E. Frejtag – Mika, Z. Kołodziejak, W. Putkiewicz, *Bezpieczeństwo ekonomiczne we współczesnym świecie,* Radom 1996, s. 14.

Na tych podstawach budowana powinna być polska polityka bezpieczeństwa (Schemat 1.3.). Jej pochodną jest architektura bezpieczeństwa państwa (Schemat 1.4.).

Schemat 1.3.

Podstawy polskiej polityki bezpieczeństwa



Źródło: Opracowanie własne.

Korzystne przemiany nastąpiły w naszym bezpośrednim otoczeniu. Żyjemy w Europie pogłębiającej się integracji, w której aktywnie uczestniczymy. Większość naszych sąsiadów jest członkami lub podąża do członkostwa w zachodnich strukturach bezpieczeństwa.

Jednocześnie pojawiły się nowe niebezpieczeństwa i wyzwania, również w naszym najbliższym otoczeniu, związane przede wszystkim z naruszaniem praw człowieka i wolności obywatelskich, z napięciami gospodarczymi i konfliktami etnicznymi oraz próbami tworzenia alternatywy dla europejskiej integracji, opartymi na niektórych doświadczeniach byłego Związku Radzieckiego. W związku z tym zaistniała potrzeba aktualizacji obowiązujących dokumentów, a w rzeczywistości, wypracowania nowej postaci polityki bezpieczeństwa.

uwarunkowań dotyczących bezpieczeństwa jak i gospodarki narodowej.

Uwarunkowania bezpieczeństwa państwa ogólnie można podzielić na ***zewnętrzne i wewnętrzne.*** Bezpieczeństwo państwa wymaga ciągłej analizy, zarówno zewnętrznych, jak i wewnętrznych uwarunkowań i czynników, jakie mają wpływ na środowisko, w którym znajduje się Polska.

Do najistotniejszych ***zewnętrznych uwarunkowań*** bezpieczeństwa Polski, możliwych do identyfikacji dziś i możliwej do przewidzenia przyszłości w kontekście sytuacji międzynarodowej, należą:

- stosunki Polski z państwami sąsiednimi;
- obecność i pozycja Polski w strukturach euroatlantyckich;
- sytuacja legislacyjno-prawna stabilizująca europejskie bezpieczeństwo, w obliczu nowych wyzwań politycznych, ekonomicznych, militarnych i cywilizacyjnych[41].

Relacje Polski z państwami najbliższego otoczenia nie stwarzają bezpośrednich zagrożeń. Polska podpisała układy regulujące wzajemne stosunki z wszystkimi krajami sąsiadującymi. Nasze stosunki wolne są od jakichkolwiek wzajemnych roszczeń terytorialnych i sporów na tle mniejszości narodowych. Dodatkowym, pozytywnym czynnikiem, zmniejszającym zwłaszcza zagrożenia o charakterze militarnym, są ograniczenia i system monitorowania aktywności wojskowej, jakim podlegają państwa europejskie.

Prawdopodobieństwo wybuchu konfliktu zbrojnego w naszym regionie jest w chwili obecnej niewielkie. Ryzyko przeprowadzenia przez którekolwiek państwo niespodziewanego ataku jest dziś znikome. Wejście do Sojuszu Północnoatlantyckiego zmieniło geopolityczną pozycję Polski, przekreśliło ostatecznie skutki porządku jałtańskiego i podziału Europy na strefy wpływów.

Członkostwo w NATO dało Polsce najpełniejsze, trwałe gwarancje bezpieczeństwa. Uczyniło Polskę członkiem wspólnoty demokratycznych i stabilnych państw. Należy oczekiwać, iż przynależność tę ugruntuje uczestnictwo Polski w Unii Europejskiej i funkcjonowanie w jej strukturach.

---

[41]Por. S. Koziej, F. Wołkowicz, *Podstawowe założenia polityki bezpieczeństwa i strategii obronnej,* AON, Warszawa 1998, s.15.

- Strategii Obronności Rzeczypospolitej Polskiej[45];
- Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[46];
- Ustawie o stanie klęski żywiołowej z 18 kwietnia 2002 roku[47];
- Ustawie o stanie wyjątkowym z dnia 21 czerwca 2002 roku[48];
- Ustawie o stanie wojennym oraz kompetencjach Naczelnego Dowódcy SZ i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej z dnia 29 sierpnia 2002 roku[49];
- Rozporządzeniu Rady Ministrów w sprawie sposobu tworzenia gminnego zespołu reagowania, powiatowego i wojewódzkiego zespołu reagowania kryzysowego oraz Rządowego Zespołu Koordynacji Kryzysowej i ich funkcjonowania z dnia 3 grudnia 2002 roku[50];
- Rozporządzeniu Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym[51].
- Rozporządzeniu Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa[52].

Polska realizowała te cele z poszanowaniem prawa międzynarodowego, zgodnie z postanowieniami Karty Organizacji Narodów Zjednoczonych (ONZ) oraz dokumentów Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE). Respektując suwerenność innych krajów, Polska nie dąży do umacniania własnego bezpieczeństwa kosztem bezpieczeństwa innych państw. Polska realizuje własne interesy w zgodzie ze wspólnymi wysiłkami zmierzającymi do umocnienia bezpieczeństwa w Europie i na świecie oraz nie ma roszczeń terytorialnych wobec żadnego państwa. Nie traktuje żadnego państwa jako wroga. Wszelkie spory będzie rozwiązywać zgodnie z zasadami prawa międzynarodowego. Środowisko bezpieczeństwa Polski podlega ciągłym i dynamicznym zmianom. Mają one generalnie pozytywny kierunek i stwarzają korzystne warunki dla rozwoju

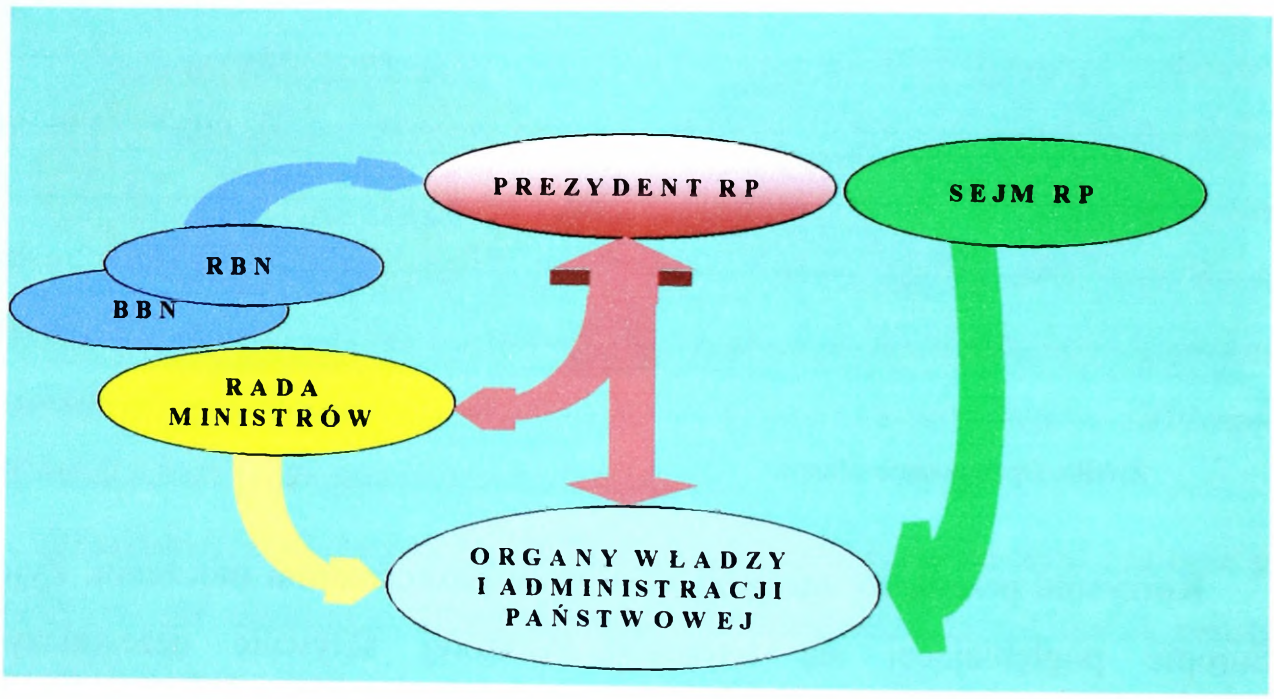
---

[45]Przyjęta na posiedzeniu Rady Ministrów w dniu 23 maja 2000 r.
[46]Przyjęta na posiedzeniu Rady Ministrów w dniu 8 września 2003 r.
[47]Dz. U. Nr 62 poz. 558 z 2002 r.
[48]Dz. U. Nr 113 poz. 985 z 2002 r.
[49]Dz. U. Nr 156 poz. 1301 z 2002 r.
[50]Dz. U. Nr 215 poz. 1818 z 2002 r.
[51]Dz. U. Nr 98 poz. 978 z 2004 r.
[52] Dz. U. Nr 180. poz. 1855 z 2004 r.

Konieczność zmian wynikała nie tylko z przemian, jakie się dokonały w sferze bezpieczeństwa europejskiego, ale także z potrzeby odpowiedniego przygotowania się do reagowania na kryzysy, które w bezpośredni bądź pośredni sposób zagrażałyby bezpieczeństwu i stabilności zarówno Polski, jak i jej najbliższego otoczenia. Członkostwo w NATO z czasem przestało być celem polskiej polityki bezpieczeństwa, a stało się instrumentem służącym realizacji polskiej racji stanu oraz sposobem wykorzystania nowych możliwości naszej polityki zagranicznej. Udział w strukturze sojuszniczej spowodował również zharmonizowanie naszej strategii i planów obronnych z wytycznymi przyjętymi w ramach wspólnego planowania strategicznego NATO[42].

Schemat 1.4.

Architektura bezpieczeństwa państwa



Źródło: Opracowanie własne.

Zmiany te znalazły odzwierciedlenie w podstawowych dokumentach dotyczących bezpieczeństwa państwa. Tworzy je zbiór następujących dokumentów:

- Konstytucja Rzeczpospolitej Polskiej[43];
- Strategii Bezpieczeństwa Rzeczypospolitej Polskiej[44];

---

[42]Por. R. Przemyski, *Strategia wojskowa Rzeczypospolitej Polskiej w kontekście bezpieczeństwa i obronności państwa,* Generalny Zarząd Planowania Strategicznego Sz. Gen. WP, Warszawa 2003, s. 7.
[43]Konstytucja RP z 02.04.1997 r., art. 5.
[44]Przyjęta na posiedzeniu Rady Ministrów w dniu 4 stycznia 2000 r.

znaczeniu, a także poważne zagrożenia środowiska naturalnego. Istnieje także zagrożenie ze strony obcych służb specjalnych. Działania podejmowane w tej dziedzinie mają nie mniej ważny aspekt sojuszniczy: nasza wiarygodność zależy również od naszej „szczelności" w tej sferze.

Ogólnie można stwierdzić, że na *płaszczyźnie zewnętrznej* uwarunkowania polityczne bezpieczeństwa ekonomicznego odnoszą się do ustroju politycznego oraz przynależności do określonego bloku państw (organizacji), a także do charakteru stosunków wypracowanych z innymi państwami i organizacjami (blokami państw).

Radykalne przemiany ustrojowe zawsze powodują okresowy wzrost zagrożeń wewnętrznych. W zbiorze ***uwarunkowań wewnętrznych*** polityki bezpieczeństwa państwa, dostrzec i wyróżnić trzeba przede wszystkim czynniki polityczne, ekonomiczne, społeczne itp., które mogą mieć zarówno charakter kreatywny, jak i destrukcyjny. Jeśli nabierają charakteru destrukcyjnego to nie tylko osłabiają one potencjał państwa ale również zwiększają jego podatność na presje zewnętrzne. Nieuniknione koszty społeczne kryzysu gospodarczego, przeprowadzanych głębokich reform rynkowych, a zwłaszcza bezrobocie, sprzyja szerzeniu się frustracji, rozprężenia, wzrostu przestępczości i innych patologicznych zjawisk społecznych. W tych warunkach może tworzyć się atmosfera sprzyjająca rozprzestrzenianiu się groźnych tendencji szowinistycznych lub nacjonalistycznych. Głównym środkiem przeciwstawienia się tym zagrożeniom jest maksymalne przyspieszenie procesu przemian i skracanie okresu przejściowego. Przedłużanie okresu przebudowy niosłoby ze sobą nieuchronnie pogłębienie napięć i zaburzeń społecznych.

Procesy demokratyzacji systemu politycznego, wprowadzenie gospodarki rynkowej i liberalizacja stosunków społecznych wymagają zmiany starych struktur i nawyków. Postęp przemian jest czasem hamowany zarówno przez niewydolność części aparatu administracyjnego, jak i przez świadomą opozycję sił eksternistycznych. Występują też nawyki świadomościowe, będące wynikiem długoletnich nawyków, a utrudniające społeczną adaptację do nowych warunków[54].

---

[54]Por. S. Koziej, F. Wołkowicz, *Podstawowe* ... wyd. cyt., s. 21.

współpracy z naszymi partnerami. Polska nie musi stawiać czoła w przewidywalnej przyszłości egzystencjalnemu zagrożeniu. Pozostają wszakże ryzyka i niepewności, które mogą przekształcić się w konflikty, w tym również w naszym bezpośrednim otoczeniu. Głównym czynnikiem stabilności polityczno-wojskowej na kontynencie jest Sojusz Północnoatlantycki. Polska będzie wnosić swój wkład w umacnianie Sojuszu, utrzymanie jego zdolności do wypełnienia podstawowych zadań bezpieczeństwa, to znaczy zapewnienie stabilnego euroatlantyckiego środowiska bezpieczeństwa, służenie jako forum konsultacji oraz instrumentu odstraszania i obrony, a także w ramach procesu wzmacniania bezpieczeństwa i stabilności - wnoszenia wkładu do zapobiegania konfliktom i opanowywania kryzysów oraz rozwijania partnerstwa, współpracy i dialogu z innymi państwami na obszarze euroatlantyckim. Priorytetem Polski jest zachowanie przez Sojusz zdolności do wypełniania jego funkcji jako organizacji obrony zbiorowej.

W naszej, a także sojuszniczej ocenie, agresja konwencjonalna na dużą skalę przeciwko Sojuszowi jest mało prawdopodobna, istnieje jednak możliwość pojawienia się takiego zagrożenia w dłuższym czasie. Polska wraz z pozostałymi sojusznikami jest wystawiona na różnorodne ryzyka militarne i niemilitarne, o wielokierunkowym i czasami trudnym do przewidzenia charakterze. Składa się na nie niepewność i niestabilność na obszarze euroatlantyckim i wokół niego, a także możliwość kryzysów regionalnych na obrzeżach Sojuszu. Niektóre państwa na tym obszarze znajdują się w obliczu poważnych trudności o podłożu ekonomicznym, społecznym i politycznym. Rywalizacje etniczne i religijne, spory terytorialne, nie wystarczające bądź nieudane próby reform, naruszenia praw człowieka, rozpad państw mogą prowadzić do lokalnej bądź nawet regionalnej destabilizacji.

Polska musi nadal brać pod uwagę znaczące siły konwencjonalne rozmieszczone w pobliżu jej granic oraz istnienie potężnych sił nuklearnych pozą Sojuszem Północnoatlantyckim[53]. Źródłem niepokoju jest rozprzestrzenianie broni masowego rażenia i środków jej przenoszenia. Interesy bezpieczeństwa Polski mogą być także wystawione na szwank poprzez akty terroru, sabotażu i przestępczości zorganizowanej, zakłócenia dostaw surowców o żywotnym

---

[53]Por. R. Przemyski, *Strategia wojskowa*...wyd. cyt., s. 9.

kryteriom sprawnie funkcjonującej demokracji. Zatem wszelkie czynniki opóźniające dopełnienie procesu demokratycznej transformacji kryją w sobie zagrożenie dla bezpieczeństwa państwa. Obecne stadium reform nie stwarza zagrożenia dla spoistości państwa oraz jego wiarygodności jako partnera współpracy gospodarczej. Stosunkowo najszybciej postępuje integracja polityczna nowego ustroju[55].

Odrębnym zagadnieniem są problemy związane z procesem prywatyzacji i reprywatyzacji. Nieprawidłowości oraz zahamowania w procesach prywatyzacji mogą w skali kraju spowodować niezadowolenie społeczne, które może stworzyć niebezpieczeństwo hamowania transformacji ekonomicznej. W płaszczyźnie międzynarodowej skutkować mogą zahamowaniem napływu inwestycji zagranicznych oraz opóźnieniem procesu integracji z Unią Europejską. Należy podkreślić, że obok zróżnicowania przestrzennego mamy w Polsce do czynienia z postępującą degradacją środowiska, która potęguje zagrożenia ekologiczne wywierające (nie do końca zbadany) wpływ na stan świadomości Polaków. O możliwościach zaspokajania finansowych i rzeczowych potrzeb systemu obronnego państwa, w tym sił zbrojnych RP, decydują warunki ekonomiczne. Możliwości finansowania systemu obronnego państwa decydują nie tylko o sytuacji sił zbrojnych, ale także determinują sytuację przemysłu obronnego, utrzymywanie i uzupełnianie strategicznych rezerw państwowych i specjalistycznych, w tym rezerw mobilizacyjnych.

Problematyka zagranicznych stosunków ekonomicznych (handel i zadłużenie) stanowi jeden z istotnych problemów związanych, zarówno z rozwojem ekonomicznym, jak i z bezpieczeństwem Polski. Głównymi partnerami handlowymi Polski są obecnie państwa Unii Europejskiej.

Ważny dla bezpieczeństwa państwa jest problem samowystarczalności surowcowej, a szczególnie w zakresie surowców energetycznych (węgla kamiennego, brunatnego, gazu ziemnego i ropy naftowej) oraz składników i komponentów dla przemysłu metalurgicznego, chemicznego, farmaceutycznego

---

[55]Por. S. Kurek, *Identyfikacja bezpieczeństwa ekonomicznego państwa*, w: Gospodarka wybranymi zasobami naturalnymi w Polsce, a bezpieczeństwo ekonomiczne, Praca zbiorowa pod kier. nauk. J. Płaczka, AON, Warszawa 1999, s. 33.

Przez dziesiątki lat pojęcie bezpieczeństwa narodowego nabrało w rozumieniu Polaków znaczenia swoistego kanonu. Ten stereotyp nadal funkcjonuje. Daje się zauważyć, iż zbyt wolno kształtuje się w świadomości Polaków całościowe rozumienie uwarunkowań bezpieczeństwa i składających się na nie czynników: politycznych, militarnych, gospodarczych i społecznych - zwłaszcza kwestii socjalnych, demograficznych, etnicznych, religijnych, światopoglądowych a szczególnie ekologicznych.

Stosunek społeczeństwa do spraw bezpieczeństwa i obronności jest na ogół pozytywny, choć zróżnicowany w zależności od wieku, wykształcenia i miejsca zamieszkania. Zdecydowanie największe znaczenie przypisujemy bezpieczeństwu granic i ich szczelności. Wojsko postrzegane jest przez zdecydowaną większość społeczeństwa jako jedna z głównych instytucji życia społeczno-politycznego, wnosząca decydujący wkład w zapewnienie bezpieczeństwa państwa. Z drugiej zaś strony znana jest niechęć do odbywania zasadniczej służby wojskowej. Jest to jednak sprzeczność pozorna, bowiem w dzisiejszych warunkach historycznych i kulturowych nie wydaje się ona tak konieczna, jak jeszcze kilkanaście lat temu.

Świadomość polityczna Polaków nie jest jeszcze w pełni jednoznacznie określona. Dotyczy to np. świadomości historycznej, będącej jednym ze wskaźników tzw. kultury politycznej. Przykładem jest tu wypełnianie „białych plam" w historii narodu. Prezentowane, obok rzeczowego kontekstu historii Polski, przykłady jednostronnej oceny zdarzeń - rodzą niepotrzebne podziały. Niekorzystne z punktu widzenia bezpieczeństwa państwa są też niekiedy uprzedzenia wobec mniejszości narodowych i religijnych. Daje się jeszcze zaobserwować zachowania o charakterze ksenofobicznym, które manifestują się okazywaniem jawnej niechęci wobec przedstawicieli mniejszości narodowych w Polsce. Nurt ten dominuje wśród ugrupowań skrajnych szermujących hasłami zagrożenia dla polskich interesów narodowych. Istotne znaczenie dla skuteczności i tempa przemian w Polsce ma przezwyciężanie recesji. Powodzenie przeobrażeń jest w znacznym stopniu uwarunkowane powodzeniem przeprowadzonych reform, stabilizacją struktur państwa i podniesieniem efektywności ich funkcjonowania.

Długofalowe bezpieczeństwo Polski zależy od jej integracji z instytucjami demokratycznego Zachodu, a ta dokona się jedynie pod warunkiem odpowiadania

Działalność ich jest jednak mocno rozproszona i nie spójna. Nie wszystkie powołane do tego instytucje potrafiły dostosować się do nowych warunków i znaleźć skuteczne formy oddziaływania edukacyjnego. Dotyczy to zwłaszcza nadzwyczajnych zagrożeń czasu pokoju i w pewnej mierze obrony cywilnej. Przykładem tego może być powódź w lipcu 1997 r.

System kształcenia obronnego został poważnie zniekształcony. Młodzież kończąca edukację na poziomie szkoły podstawowej nie spotyka się z problematyką obronności w systemie szkolnym. Ma to wyraźne, negatywne skutki w procesie przygotowania do obowiązku służby wojskowej.

Na *płaszczyźnie wewnętrznej* uwarunkowania polityczne bezpieczeństwa ekonomicznego są kreowane przez sferę polityczną - politykę bezpieczeństwa państwa i uwidocznianie się na płaszczyźnie społeczno-gospodarczej, a także w polityce bezpieczeństwa ekonomicznego przez określenie celów, zadań i systemu organizacyjnego.

Uwarunkowania polityczne bezpieczeństwa ekonomicznego są ściśle powiązane z uwarunkowaniami ekonomicznymi, gdyż wypływają z siebie wzajemnie i nie mogą samodzielnie występować. Ponadto przynależy im się rola kreatywnego i konstruktywnego kształtowania polityki bezpieczeństwa ekonomicznego, bowiem nadają one formę zinstytucjonalizowaną uwarunkowaniom kształtowania tego bezpieczeństwa[56]. Jednocześnie szerokość i głębokość powiązań między grupami uwarunkowań bezpieczeństwa ekonomicznego powoduje, iż stają się one dla siebie wzajemnie weryfikatorami.

Kolejną grupą uwarunkowań bezpieczeństwa ekonomicznego są *uwarunkowania obronno-militarne*. Zauważa się dużą złożoność tej grupy, gdyż składowe jej są pochodną uwarunkowań politycznych i ekonomicznych. Ten obszar uwarunkowań wypływa z założeń polityki bezpieczeństwa państwa przez nałożenie na gospodarkę narodową konieczności zaspokajania militarnych potrzeb państwa. Stanowią one duży zbiór czynników, które mogą warunkować utratę lub utrzymanie, a nawet wzrost poziomu bezpieczeństwa ekonomicznego państwa.

---

[56]Por. Z. Stachowiak, *Identyfikacja narodowej i sojuszniczej strategii obronnej i ich relacje do strategii bezpieczeństwa i bezpieczeństwa ekonomicznego* w: Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego Polski z punktu widzenia narodowej i sojuszniczej strategii obronnej, Praca zbiorowa pod kier. nauk. Z. Stachowiaka, AON, Warszawa 2002, s. 84.

itp. Polska jest samowystarczalna jeśli chodzi o zabezpieczanie potrzeb na węgiel kamienny i brunatny oraz gaz koksowniczy. Problemem natomiast może być zaspokojenie popytu na gaz ziemny, bowiem większość tego surowca importujemy z Rosji. W przypadku przerwania dostaw importowych oraz zachowania priorytetu zaopatrzenia odbiorców komunalnych znacząca liczba przedsiębiorstw, szczególnie w branży chemicznej, metalurgicznej i nawozów sztucznych musiałaby ograniczyć lub przerwać produkcję. W zakresie dostaw ropy naftowej istnieje możliwość zdywersyfikowania źródeł jej zakupu (Rosja, Norwegia, kraje arabskie). Niemniej zakłócenia w jej dostawach mogą rzutować negatywnie na zaopatrzenie rynku, w tym na funkcjonowanie przemysłu chemicznego, farmaceutycznego itp.

Import surowców nie energetycznych w całości zaspokaja potrzeby w zakresie dostaw rudy żelaza, rudy aluminium oraz składników i komponentów do wytwarzania uszlachetnionych gatunków stali niezbędnych dla przemysłu obronnego, łożyskowego, narzędziowego itp. w odróżnieniu od dostaw gazu i ropy naftowej zaopatrzenie przemysłu w importowane składniki i komponenty nie powinno stwarzać większych problemów, bowiem są one dostępne na wielu rynkach zagranicznych.

Istotnym czynnikiem wewnętrznym warunkującym bezpieczeństwo państwa jest świadomość i edukacja obronna. Wraz ze zmianą ustroju politycznego nastąpiła w Polsce zmiana świadomości społecznej obywateli. Jej wyznacznikiem jest prezentowany przez obywatela system wartości, obejmujący tak wiedzę, jak i opinie, poglądy, postawy i zachowania. Świadomość społeczna, a zwłaszcza świadomość obronna uległa generalnie obniżeniu. Obserwuje się swoistą niespójność postaw z jednej strony społeczeństwo bardzo wysoko ceni wojsko, jako instytucję społecznego zaufania, z drugiej zaś strony - absolutnie neguje potrzebę i chęć własnych świadczeń na rzecz wojska i obronności.

Edukacja i wychowanie proobronne społeczeństwa winny być istotnym czynnikiem polskiego modelu oświatowo-wychowawczego. Niestety, jesteśmy na początku drogi w budowie nowego ogólnokrajowego systemu kształcącego świadomość proobronną społeczeństwa. Funkcjonują luźno ze sobą powiązane ogniwa, takie jak: rodzina, szkoły, organizacje i stowarzyszenia, instytucje kulturalno-oświatowe, kościoły i związki wyznaniowe, wydawnictwa i media.

3. ***W stanie wojny*** - działania nadal będą się skupiać na obszarach realizacyjnym i weryfikacyjnym, lecz przy położeniu większego nacisku na ten ostatni, gdyż w trakcie działań wojennych będą narastały czynniki negatywne wymagające odpowiednich reakcji.

Na kształtowanie bezpieczeństwa ekonomicznego duży wpływ będą miały *uwarunkowania społeczne*, które skupiają w sobie szereg uwarunkowań socjalno-bytowych, kulturowych, oświatowych itp. Stanowią o nich warunki bytowe i społeczne ludności (ochrona zdrowia, system rentowo-emerytalny, kultura, oświata, sport itd.). Analiza tego obszaru uwarunkowań ukazuje poziom życia społeczeństwa oraz kierunki, które należy obrać, aby zapewnić dobrobyt jednostki. Uwarunkowania społeczne ściśle się wiążą z uwarunkowaniami politycznymi i ekonomicznymi i w dużym stopniu od nich zależą.

Duże znaczenie dla bezpieczeństwa ekonomicznego mają *uwarunkowania geostrategiczne.* Z jednej strony nie mamy żadnego wpływu na fizyczne ukształtowanie kraju, jego klimat, ilość zasobów naturalnych, położenie względem innych państw, z drugiej strony możemy kształtować liczbę ludności, sieć komunikacyjną itd. Z obszaru tych uwarunkowań, często w decydującym stopniu, wypływa miejsce zajmowane przez kraj w hierarchii światowej[57].

Bezpośredni wpływ na bezpieczeństwo ekonomiczne mają *uwarunkowania infrastrukturalne,* bowiem znajdują one odbicie we wszystkich omawianych dotychczas grupach uwarunkowań. Uwarunkowania te wpływają na kształtowanie bezpieczeństwa ekonomicznego w następujący sposób:

a) w wymiarze ekonomicznym koncentrują się na problemie niepodzielności nakładów w skali zaangażowania poszczególnych rodzajów kapitału, pracochłonności i kapitałochłonności przedsięwzięć, a także na kwestie zmian jakościowych;
b) w wymiarze społecznym są to działania administracji państwowej i samorządowej na rzecz zapewnienia odpowiedniej sytuacji prawno-ekonomicznej społeczeństwa;
c) w wymiarze techniczno-organizacyjnym są one odpowiedzialne za

---

[57]Tamże, s. 89.

Odnosi się to do wszystkich stanów, tzn. pokoju, zagrożenia militarnego i wojny. Czynniki z tego obszaru mogą, zarówno sprzyjać, jak i ograniczać kształtowanie się bezpieczeństwa ekonomicznego państwa. Wyszczególnione stany, w jakich może się znajdować państwo są wypadkową zaistniałych konfliktów społecznych i narodowościowych.

Czynniki wypływające z obszaru obronno-militarnego są bodźcem do tworzenia i ciągłej aktualizacji systemu działań w sferze gospodarczej, działającego pod kątem jej struktur do wymagań, jakie są stawiane przez określone podmioty bezpieczeństwa państwa. Oznacza to, że uwarunkowania obronno-militarnie są obszarem złożonym i rozwiązywalnym za pomocą działań wieloetapowych, gdyż wypływa to ze stopnia zmienności sytuacji, w jakiej się znajduje dany kraj.

Kształtowanie bezpieczeństwa ekonomicznego zależy od stanu, w jakim może się znajdować państwo. W każdym z nich ujawniają się inne problemy do rozwiązania:

1. ***W stanie pokoju*** - w skali makro - uwarunkowania bezpieczeństwa ekonomicznego skupiają się na trzech grupach:
   a) uwarunkowaniach kreacyjnych, które są związane z tworzeniem polityki bezpieczeństwa państwa, z uszczegółowieniem jego potrzeb w dziedzinie bezpieczeństwa ekonomicznego;
   b) uwarunkowaniach realizacyjnych (funkcjonalnych), które są zauważalne w trakcie urzeczywistniania polityki bezpieczeństwa, przy tworzeniu, utrzymaniu i rozwoju systemu obronnego;
   c) uwarunkowaniach weryfikacyjnych (korygujących) spełniających zadania badawczo-kontrolne wobec dwóch pierwszych grup uwarunkowań.
2. ***W stanie zagrożenia*** - uwarunkowania bezpieczeństwa ekonomicznego skupiają się na dwóch grupach: realizacyjnej i weryfikacyjnej (grupa kreacyjna jest wykorzystywana w ograniczonym stopniu). Działania te mają na celu zapewnienie niezbędnego minimum do przetrwania ludności. Sfera gospodarcza przygotowuje się do zaspokajania potrzeb w większym stopniu wojska niż ludności cywilnej.

Traktując bezpieczeństwo ekonomiczne państwa jako bilans potrzeb rozwojowych państwa i możliwości ich zaspokojenia, celowym jest wyróżnienie czterech obszarów funkcjonowania jego *wyznaczników,* a mianowicie:

a) możliwości rozwojowych;

b) potrzeb rozwojowych;

c) infrastruktury;

d) bilansowej.

Prezentację poziomów wyznaczników w tych obszarach umożliwia odpowiednio dobrany zbiór mierników i wskaźników w których należy dostrzegać wielkości opisujące pewien poziom cech zjawisk w gospodarce narodowej[58]. Ogół tych *wskaźników* podzielić można na dwie główne grupy: ***bezwzględne i względne***.

Wskaźniki bezwzględne opisują cechy mierzalne występujące w gospodarce. Jako przykładowe można wymienić takie jak: rozmiary PKB, kwoty przeznaczone na oszczędności i inwestycje, ilości importowanej ropy naftowej i gazu, wartość eksportu, suma środków finansowych przeznaczona na obronę narodową itd. Tego rodzaju wskaźniki występujące samodzielnie nie dają podstaw do wyrażania sądów wartościujących, chociaż są ich niezbędnym składnikiem.

Wskaźniki względne opisują stany i procesy gospodarcze poprzez zestawienie i porównanie ze sobą *wskaźników bezwzględnych*. W połączeniu z inną cechą lub innym związkiem czy też zależnością, pozwalają one stwierdzić obecność lub przewidzieć zaistnienie innych cech opisu lub zależności. Pozwalają one na budowanie sądów wartościujących a także na wykrywane zależności i związków. Stale powtarzające się zależności i związki są podstawą do budowania praw i prawidłowości. Odwołanie się do odpowiednich zbiorów wyznaczników bezpieczeństwa ekonomicznego państwa wiąże się z potrzebą dokonywania oceny ich poziomów, według przyjętych kryteriów. Uwzględniając specyfikę ***wyznaczników bezpieczeństwa ekonomicznego***, można wyróżnić dwa zasadnicze ich rodzaje, to jest ***ogólne i progowe.***

Wyznacznikami ogólnymi są te, które kryją w sobie istotę podstawowych

---

[58]Por. P. Kopania, *Wyznaczniki bezpieczeństwa ekonomicznego państwa,* w: *Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego Polski z punktu widzenia narodowej i sojuszniczej strategii obronnej*, Praca zbiorowa pod kier. nauk. Z. Stachowiaka, AON, Warszawa 2001, s. 139.

zarządzanie i koordynowanie procesów kształtowania bezpieczeństwa ekonomicznego, a także kształtowanie cech niezbędnych do realizacji tych przedsięwzięć, tj. dużej mobilności, żywotności przestrzennej, jedności funkcjonalnej itd.

Uwarunkowania infrastrukturalne winny zapewniać takie rozwiązania, które sprzyjałyby rozwojowi poziomu bezpieczeństwa jednostki, podmiotów gospodarczych, gałęzi przemysłu, aż do bezpieczeństwa narodowego.

1.1.3. Wyznaczniki i mierniki opisu bezpieczeństwa ekonomicznego państwa

Obecność Polski w NATO i uczestnictwo w strukturach UE nakłada określone obowiązki i stwarza ograniczenia co do charakteru, zakresu i tempa rozwoju społeczno-gospodarczego, jak również odpowiednie zadania dotyczące możliwości obronnych. Oznacza to, że potrzeby naszego systemu obronności muszą być zaspokajane proporcjonalnie do kondycji i realnych możliwości gospodarki narodowej.

Aby to zrealizować, ekonomiczny aspekt obronności musi mieć swoje odzwierciedlenie w spójnym, czytelnym i stabilnym planie rozwoju społeczno-gospodarczego państwa a szczególnie programie strategicznym, gwarantującym utworzenie trwałych podstaw dla szeroko rozumianego systemu bezpieczeństwa państwa, rozpatrywanym z punktu widzenia uwarunkowań zewnętrznych i wewnętrznych, w sferze politycznej, społecznej, gospodarczej i militarnej. Zagrożenia w sferze politycznej, militarnej, gospodarczej jak i społecznej wywołują określone skutki (konsekwencje) dla bezpieczeństwa państwa. Państwo kreując swoją politykę w tych dziedzinach opiera się na swojej strategii (doktrynie). W procesie planowania strategicznego analizowane są potrzeby państwa w celu eliminacji lub maksymalnego łagodzenia skutków realnych lub potencjalnych zagrożeń. Określane są również realne możliwości państwa w tym zakresie.

Kolejnym problemem jest określenie narzędzi, na podstawie których będzie można dokonać identyfikacji i określenia stanu (poziomu) bezpieczeństwa ekonomicznego państwa. Takie możliwości dają wyznaczniki bezpieczeństwa ekonomicznego państwa, powstałe jako wypadkowa czynników rozwoju gospodarczego i jego barier.

przeciwstawiać się transmisji niepożądanych zewnętrznych efektów w sferze ekonomicznej (np. w formie sankcji); nie jest w stanie utrzymać swojego osiągniętego już poziomu życia przy pomocy własnych środków; nie może zapewnić dostatecznych środków na zachowanie wojskowej zdolności obronnej; musi zrezygnować z własnej odrębności państwowej, z zachowania specyficznych wartości, struktur i mechanizmów charakterystycznych dla niego. Inaczej mówiąc kraj nie może postępować zgodnie ze swoją racją stanu i realizować naczelnych interesów społeczeństwa zorganizowanego w państwo.

Wyznaczniki progowe wyodrębnić można w dwóch zasadniczych płaszczyznach: ***podmiotowej i przedmiotowej***[59].

Na płaszczyźnie ***podmiotowej*** należy wyróżnić dwie grupy podmiotów:

- wewnętrzne (państwo, instytucje, organizacje gospodarcze, grupy społeczne itp.);
- zagraniczne (państwa, ugrupowania państw, organizacje i instytucje międzynarodowe formalne i nieformalne, przedsiębiorstwa zagraniczne i międzynarodowe itp.).

W związku z tym wyodrębnić można odpowiednie wyznaczniki progowe:

- na płaszczyźnie *podmiotowej zewnętrznej* te wyznaczniki występować będą w ramach współzależności i zależności rozwojowych. Umiejscowione są przede wszystkim w obszarze zaopatrzenia i zbytu, bilansu handlowego i płatniczego, pozyskiwaniu technologii i kapitałów, uregulowań stosunków, dostaw uzbrojenia itp.
- na płaszczyźnie *podmiotowej wewnętrznej* te wyznaczniki występować będą w ramach zasad podziału dochodu narodowego, stosowanych narzędzi polityki gospodarczej i mechanizmu funkcjonowania gospodarki. Umiejscowione są w obszarze proporcji podziału dochodu narodowego, zróżnicowania obciążeń fiskalnych, siły nacisku partykularnych grup interesów itp.

Na płaszczyźnie ***przedmiotowej*** wyznaczniki progowe występować będą w ramach bilansów dóbr finalnych i pośrednich, powiązań kooperacyjnych,

---

[59]Tamże, s. 141.

procesów rzeczywistości gospodarczej. Jej charakterystyka (wielkość, struktura, kierunki zmian, sposób wykorzystania) opisuje najważniejsze procesy ekonomiczne. Ze względu na obszar rzeczywistości, której dotyczą, można podzielić je na ***globalne, cząstkowe i szczegółowe***.

Wyznaczniki progowe, to konkretyzacja wyznaczników ogólnych poprzez wskazanie w nich tzw. „progów krytycznych". Progi krytyczne tradycyjnie odnosiły się do wartości i o charakterze podstawowym (istnienie, przetrwanie) i poziomu zaspokojenia potrzeb z tym związanych. Próg krytyczny to taki stopień zaspokojenia potrzeb (wielkość graniczna), przy którym staje się niemożliwe realizowanie określonej wartości. Wyznaczenie progów krytycznych dokonuje się poprzez zestawienie potrzeb i określenie minimum niezbędnych do ich zaspokojenia potrzeb. Ich podstawą mogą być określone subiektywnie kryteria (wyprowadzone z cenionych wartości) lub uogólnienie doświadczeń (np. ilość minimalna wypitego alkoholu po której następuje zgon).

Dokładne określenie krytycznego progu bezpieczeństwa ekonomicznego w praktyce jest trudne. O jego poziomie decydują bowiem różne płaszczyzny międzynarodowych powiązań i stabilność systemu społeczno-politycznego. Stąd też jego poziom jest zazwyczaj dalece przybliżonym. Krytyczne granice w płaszczyźnie gospodarczej można bowiem określić bardzo ogólnie i w kompleksowych związkach z innymi płaszczyznami. Przykładowo i najbardziej ogólnie można powiedzieć, że wyznaczniki progowe w sferze ekonomicznej (produkcji, podziału i wymiany zagranicznej) to takie wielkości i relacje, których przekroczenie uniemożliwi państwu decydowanie o własnym rozwoju, a społeczeństwu wolne, niczym nie obciążone decydowanie o zachowaniach konsumpcyjnych.

Próg krytycznego bezpieczeństwa ekonomicznego państwa odnosi się, zarówno do płaszczyzny społeczno-gospodarczej, jak i ekonomiczno-obronnej. Krytyczne progi bezpieczeństwa ekonomicznego mogą występować wewnątrz własnej gospodarki (produkcja, podział) jak również w relacjach gospodarki kraju z otoczeniem zagranicznym. Przekroczenie krytycznej granicy rodzi określone konsekwencje. Oznacza ono wejście w stan, w którym dany kraj nie może już autonomicznie decydować o własnym rozwoju gospodarczym; nie może skutecznie

i konsumpcyjnej[60].

Mierniki bezpieczeństwa ekonomicznego mogą mieć postać:

a) *syntetyczną* - przez ujęcie agregatywne umożliwiają przybliżenie ogólnego wymiaru wyznaczników; współokreślają całościowo poziom wskaźnika konkretnego wyznacznika, przez co przybliżają ocenę badanego stanu;

b) *analityczną* - przez którą określają ilościowe rozmiary poszczególnych czynników stanowiących o bezpieczeństwie ekonomicznym; współokreślają poziom podstawowych zasobów czynników kształtowania bezpieczeństwa ekonomicznego.

Mierniki mogą być stosowane (bez względu na metody: bilansową, statystyczną, normatywną itd.) przy konstrukcji i opisie wyznaczników bezpieczeństwa ekonomicznego.

Wskaźniki to wartości względne, które odnoszą się do określonej podstawy i przyjmują postać liczbową wyrażającą stosunek procentowy lub ilościowy do danej wielkości. Obrazują dane cechy przedmiotu lub zjawiska połączone z pewną inną jego cechą. Obliczanie wskaźników opiera się w praktyce na wybieraniu punktu wyjścia dla danego zjawiska, a następnie wskazaniu w stosunku do badanej podstawy wartości w procentach. Wyodrębnia się wskaźniki struktury, dynamiki, zasadnicze itd. Ogół tych *wskaźników* podzielić można na dwie główne grupy: *bezwzględne i względne*.

Wskaźniki bezwzględne opisują cechy mierzalne występujące w gospodarce. Jako przykładowe można wymienić takie jak: rozmiary PKB, kwoty przeznaczone na oszczędności i inwestycje, ilości importowanej ropy naftowej i gazu, wartość eksportu, suma środków finansowych przeznaczona na obronę narodową itd. Tego rodzaju wskaźniki występujące samodzielnie nie dają podstaw do wyrażania sądów wartościujących, chociaż są ich niezbędnym składnikiem.

Wskaźniki względne opisują stany i procesy gospodarcze poprzez zestawienie i porównanie ze sobą *wskaźników bezwzględnych* w połączeniu z inną

---

[60]Por. P. Kopania, *Wyznaczniki bezpieczeństwa ekonomicznego państwa a wyznaczniki strategii obronnej* w: *Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego Polski z punktu widzenia narodowej i sojuszniczej strategii obronnej,* Praca zbiorowa pod kier. nauk. Z. Stachowiaka, AON, Warszawa 2002, s. 81.

poziomu i struktury rezerw i zapasów. Mogą one uwzględniać wewnętrzne i zewnętrzne źródła zaopatrzenia i zbytu, dostępność w określonym czasie itp. Wyrażają potrzeby gospodarki lub jej segmentów o charakterze pierwotnym (surowcowo-energetycznym, żywnościowym itd.) i wtórnym (kapitału rzeczowego, technologii oraz w zakresie infrastruktury techniczno - ekonomicznej) w każdym z tych obszarów założone potrzeby konkretyzowane być mogą całym szeregiem wyznaczników, których rolą jest przede wszystkim sygnalizacja zagrożeń. Umożliwiają one z jednej strony określenie stanu bezpieczeństwa ekonomicznego kraju, z drugiej zaś obszarów i skali zagrożeń.

Takie rozróżnienie wyznaczników umożliwia kompleksowość ocen oraz uszczegółowienie ilustracji podstawowych makroekonomicznych czynników kształtowania bezpieczeństwa ekonomicznego kraju. Charakterystyczną cechą wskazanych wskaźników jest to, że dają one obraz związków i zależności bezpieczeństwa ekonomicznego w skrajnych jego wymiarach, bowiem *od stanu krytycznego po stan optymalny.* Rzeczywisty stan będzie opisywany wyznacznikami charakteryzującymi się różnym *stanem pozytywnych i negatywnych cech.* Wyznaczniki te powinny jednocześnie sprzyjać poszukiwaniom optymalnych rozwiązań między często sprzecznymi tendencjami.

Wyodrębnienie sfery bezpieczeństwa ekonomicznego nie daje jeszcze pełnego obrazu gospodarki narodowej. Prezentację poziomów wyznaczników w obszarach tych uwarunkowań gdzie należy dostrzegać wielkości opisujące pewien poziom cech zjawisk w gospodarce narodowej umożliwia odpowiednio dobrany zbiór mierników i wskaźników.

Mierniki mogą być ilościowe, wartościowe oraz czasowe. Pod tym pojęciem kryją się odpowiednio dobrane liczby bezwzględne, które pozwolą na przeprowadzenie analizy, porównań oraz sformułowanie ocen. Służą do poznania liczebności, określenia zjawisk i zdarzeń. Można je zdefiniować jako odpowiednio dobrane informacje w postaci liczbowej, które odzwierciedlają badane stany i zdarzenia sfery gospodarczej.

Mierniki te mogą być wykorzystywane globalni w skali gospodarki światowej, narodowej lub branży zarówno w odniesieniu do sfery produkcyjnej, jak

w procesie planowania budżetu obronnego państwa. Pamiętać przy tym należy, że wielkość wydatków obronnych państwa może wywierać zarówno pozytywny, jak i negatywny wpływ na procesy gospodarcze kraju, tworząc szansę i zagrożenia dla dynamiki rozwoju.

W sytuacji gdy gospodarka narodowa znajduje się w stanie kryzysu, depresji lub początkowego stanu ożywienia, najczęściej istnieją wolne moce produkcyjne (w postaci maszyn, urządzeń, linii produkcyjnych), a na rynku pracy znajdują się rezerwy wykwalifikowanej siły roboczej. Jeżeli do tego istnieją jeszcze nie wykorzystane zapasy surowców strategicznych to zwiększenie wydatków obronnych może dodatnio wpływać na koniunkturę gospodarczą kraju. W takiej sytuacji dla podjęcia produkcji na rzecz obronności nie potrzeba przemieszczania zasobów z gospodarki cywilnej do gospodarki wojskowej w tym wypadku zwiększenie wydatków obronnych uruchamia wolne moce produkcyjne, a na rynku pracy znajduje zatrudnienie wykwalifikowana siła robocza. Ożywienie w tej gałęzi gospodarki staje się wówczas bodźcem dla innych gałęzi, a wyprodukowane towary (środki walki) są bardzo dobrym towarem eksportowym (źródłem dewiz), dynamizującym i nakręcającym rozwój gospodarki. Ponadto właściwie zainwestowane środki finansowe z budżetu obronnego pozytywnie wpływają na rozwój logistycznej infrastruktury technicznej (sieć dróg, systemu łączności itp.). Jest zatem efektem pośrednich korzyści dla całej gospodarki[61].

Innym aspektem jest współzależność nakładów inwestycyjnych na wydatki obronne i postępu naukowo-technicznego. Postęp naukowo-techniczny umożliwia powstawanie nowych środków, które wpływają na zwiększenie możliwości skutecznego oddziaływania systemu obronnego państwa na realne lub potencjalne zagrożenia. Z drugiej strony zagrożenia są wyznacznikiem określonych potrzeb państwa, a te z kolei przy określonych nakładach inwestycyjnych wydatki obronne stymulują postęp naukowo-techniczny. Wielkość wydatków obronnych może mieć też negatywny wpływ na gospodarkę narodową. Pamiętać bowiem należy, że produkty przemysłu obronnego nie są dobrami powszechnej (ogólnej) konsumpcji. Przy ich nadmiernej produkcji (wykorzystywane będą surowce, zużywane

---

[61]Por. S. E. Dworecki, J. Kęsoń, M. Z. Kulisz, *Wskaźniki ekonomiczne obronności państwa*, AON, Warszawa 1999, s. 90.

cechą lub innym związkiem czy też zależnością, pozwalają one stwierdzić obecność lub przewidzieć zaistnienie innych cech opisu lub zależności. Pozwalają one na budowanie sądów wartościujących, a także na wykrywane zależności i związków. Stale powtarzające się zależności i związki są podstawa do budowania praw i prawidłowości.

Z punktu widzenia potrzeb obronności, a szczególnie wielkości i użyteczności potencjału obronnego, bardzo ważna jest polityka państwa prowadzona w dziedzinie bezpieczeństwa i obronności, określająca udział wydatków obronnych w produkcie krajowym brutto i budżecie oraz charakter i właściwości tych wydatków. Odzwierciedla to strategię spełnienia wymagań systemu obronnego państwa w nakładach finansowych na jego bezpieczeństwo militarne. Pozostają one w ścisłym związku z oddziaływaniem państwa na kierunki rozwoju społeczno-gospodarczego, a w szczególności na: stymulowanie konkurencyjności produktów krajowych, tworzenie rezerw dewizowych i zasobów zasileniowych, kształtowanie struktury popytu i podaży, zmiany technologii produkcji, wspieranie wolnego rynku, dofinansowanie wyrobów nierentownych, ale koniecznych z punktu widzenia potrzeb obronnych, dotowanie utrzymywania mocy produkcyjnych w przemyśle obronnym oraz rezerw strategicznych itp.

W przypadku gdy państwo posiada takie możliwości, zagrożenia eliminowane będą przy pomocy własnych instrumentów systemu obronnego państwa. Problem pojawia się, gdy prognozowane potrzeby przewyższają możliwości ich zabezpieczenia. W takiej sytuacji państwo może samodzielnie próbować łagodzić skutki pojawiających się zagrożeń, ale wówczas jego rozwój polityczno-gospodarczy ulega znacznemu zahamowaniu, a w ekstremalnych warunkach może doprowadzić nawet do utraty suwerenności.

Innym rozwiązaniem w takiej sytuacji jest zawarcie sojuszy. Rozwiązanie takie pozwala z jednej strony na wykorzystanie instrumentów systemu bezpieczeństwa zbiorowego, w naszym przypadku systemu bezpieczeństwa europejskiego (SBE), w celu wsparcia własnego systemu obronności państwa i eliminacji pojawiających się zagrożeń, ale z drugiej strony państwo musi liczyć się z określonymi zobowiązaniami sojuszniczymi (np. w postaci składek członkowskich, sojuszniczych akcji militarnych itp.). Koszty te należy uwzględniać

działów gospodarki narodowej"[64].

Infrastruktura to urządzenia i instytucje zapewniające prawidłowe funkcjonowanie gospodarki jako całości i poszczególnych jej dziedzin. Rozróżnia się infrastrukturę techniczną, ekonomiczną i społeczną. Obejmuje urządzenia pozwalające świadczyć usługi w zakresie komunikacji i transportu np. sieć drogowa, kolejowa, telekomunikacji, energetyki. itp.[65]

Infrastruktura to system urządzeń, działań i instytucji, które wspierają bezpośrednio lub pośrednio produkcyjną sferę gospodarki (zalicza się do nich np. budownictwo, transport, energetykę, komunikację) oraz tych, które są niezbędnym zapleczem dla funkcjonowania społeczeństwa (należą do nich np. oświata, administracja, ochrona zdrowia, organa bezpieczeństwa, bankowość)[66].

Oznacza to, że pojęcie *infrastruktury* obejmuje wszelkie obiekty i urządzenia oraz instytucje wraz z koniecznym wyposażeniem rzeczowym i osobowym, służące do zapewnienia materialnych i niematerialnych do różnego rodzaju działalności w ramach całej gospodarki kraju lub jej działów[67]. W ślad za tym można stwierdzić, że wszelkie usługi świadczone przez *infrastrukturę* mają doniosłe dla funkcjonowania państwa – postrzeganego w wymiarze gospodarki jak i społeczeństwa[68].

Konkretyzując pojęcie *infrastruktury* do infrastruktury państwa należy ją postrzegać jako zespół obiektów i urządzeń stałych i ruchomych (np. w dziedzinie transportu, komunikacji) oraz instytucji usługowych (np. w dziedzinie oświaty, ochrony zdrowia, łączności) niezbędnych do zapewnienia funkcjonowania produkcyjnych i nieprodukcyjnych działów gospodarki narodowej, a także zapewnienia odpowiednich warunków życia ludności oraz bezpieczeństwa państwa[69]. Uzasadnionym w tym momencie wydaje się podziału infrastruktury na

---

[64] *Słownik języka polskiego,* tom 1, PWN, Warszawa 1983, s. 789;
Encyklopedia Powszechna PWN, tom 2, PWN, Warszawa 1975, s. 272.

[65] *Encyklopedia internetowa WIEM*, Popularna Encyklopedia Powszechna Wydawnictwa Fogra, http://www.fogra.com.pl/.

[66] *Słownik współczesnego języka polskiego,* tom 1, Przegląd Reader`s Digest, Warszawa 2001, s. 322.

[67] Por. *Charakterystyka infrastruktury obronnej na terytorium RP,* Praca zbiorowa, AON, Warszawa 1991, s. 5.

[68] Por. *Mała encyklopedia ekonomiczna,* PWE, Warszawa 1974, s. 293.

[69] Por. *Encyklopedia popularna*, PWN, Warszawa 1996, s. 318;
W. Ślemp, *Infrastruktura państwa a wymogi obrony,* w: „Myśl Wojskowa" nr 2, s. 25.

maszyny) i ograniczonych możliwościach eksportowych, na rynku pojawi się znaczna ilość pieniądza. Wzrośnie popyt na dobra konsumpcyjne, a ten niezaspokojony - napędzi spiralę inflacji. Ponadto wzrost wydatków obronnych w sytuacji boomu w przemyśle prowadzić może do ograniczenia rozwoju gospodarki cywilnej. Wskazane problemy są bardzo ważne z punktu widzenia śledzenia kondycji gospodarki obronnej. Dlatego też do oceny *bezpieczeństwa państwa* (w różnych aspektach obronności państwa) proponuje się przyjąć *wskaźniki* makroekonomiczne, które mają odzwierciedlenie w trzech podstawowych sferach: finansowej, rzeczowej i społecznej.

Używając do pełnego zobrazowania *bezpieczeństwa ekonomicznego* państwa wymienionych wyznaczników, mierników i wskaźników, możemy otrzymać środek przydatny do przewidywania szeregu zagrożeń i wiążących się z nimi następstw. Będzie można przewidywać, jakie zachodzą związki i zależności zarówno wewnątrz obszaru bezpieczeństwa ekonomicznego, jak i na styku ze środowiskiem w różnych sytuacjach, tj. pokoju, kryzysu, wojny. Szerokie i elastyczne pojmowanie oraz wdrażanie do praktyki funkcjonowania państwa narzędzia jakim jest *bezpieczeństwo ekonomiczne*, pozwoli na pełniejsze i sprawniejsze wykorzystywanie posiadanych zasobów i możliwości.

1.2. Istota i uwarunkowania funkcjonowania infrastruktury telekomunikacyjnej

1.2.1. Pojęcie i charakter infrastruktury telekomunikacyjnej państwa

Zdefiniowanie pojęcia „infrastruktura telekomunikacyjna" i jego określenie wymaga wcześniejszego rozpoznania pojęć „infrastruktura" i „telekomunikacja". Pojęcie infrastruktury wywodzi się od łacińskich słów „infra"[62] oznaczającego „pod, poniżej, niższy, wewnątrz" oraz „structura"[63] (pochodzącego od *struere* - układać, wznosić, budować) oznaczającego „budowa, konstrukcja, ustrój". Współcześnie pod tym pojęciem występuje szereg definicji. Kilka z nich najbardziej trafnych zostanie przytoczonych.

Przez pojęcie ***infrastruktury*** należy rozumieć „zespół podstawowych urządzeń i instytucji usługowych, niezbędnych do należytego funkcjonowania

---

[62]W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych,* Muza S.A., Warszawa 2001, s. 229.
[63]Tamże, s. 475.

organów bezpieczeństwa państwa jest operatywnie i niezawodnie funkcjonująca łączność. Kierowanie obronnością państwa jest procesem bardzo złożonym, wymagającym posiadania odpowiednio przygotowanego systemu kierowania, funkcjonującego nieprzerwanie w okresie pokoju, kryzysu i wojny. Integralną część procesu kierowania i dowodzenia stanowią procesy informacyjne, które realizowane są w obszarze funkcjonowania systemu łączności.

System informacyjny to określony zorganizowany kompleks technicznych środków łączności, spełniający określone funkcje i realizujące postawione cele oraz obsługująca go kadra. Jego podstawowym zadaniem jest obsługa informacyjna, zgodna z wymaganiami narzuconymi przez użytkowników systemu. Potrzeby systemu informacyjnego określają czynniki: organizacyjne i kierownicze. Innymi słowy czynnik organizacyjny to otoczenie i infrastruktura telekomunikacyjna, struktura kierowania obronnością oraz jej wielkość i obszar. Do kierowania obronnością państwa niezbędne jest przekazywanie ***wiadomości***[75] przez system informacyjny. Dziś, jak nigdy przedtem w historii, decydującą rolę zaczyna odgrywać ***informacja***[76]. Staje się ona coraz cenniejszym zasobem i zaczyna być traktowana jak szczególnie pożądany towar.

Bazą systemu informacyjnego jest przede wszystkim system telekomunikacyjny kierowania obronnością (bezpieczeństwa) państwa. Dlatego też skuteczność systemu kierowania i zarządzania państwem, sterowania gospodarką narodową, dowodzenia siłami zbrojnymi oraz funkcjonowania organów bezpieczeństwa publicznego jest uzależniona od niezawodnie i efektywnie funkcjonującego systemu informacyjnego - łączności państwa.

Zdolność wykonania stojących przed nim zadań zależy między innymi od stanu rozbudowy infrastruktury systemu telekomunikacyjnego na obszarze całego

---

[75]Wiadomość, pojęcie występujące w teorii informacji i teorii komunikacji, związane z procesem emisji, przekazywania, przekształcania, przyjmowania i przechowywania (w pamięci) określonego ciągu elementów informacyjnych, tj. znaków, symboli, liter, cyfr, tonów, błysków itp. Każda wiadomość wysłana przez źródło wiadomości zawiera pewną ilość informacji; w teorii informacji miarą tej ilości jest wielkość zw. entropią informacyjną.

[76]Informacji teoria, teoria przekazywania wiadomości ze źródła wiadomości do obiektu ich przeznaczenia - odbiorcy; w szerszym znaczeniu także nauka zajmująca się wszechstronną analizą procesów przekazywania informacji za pomocą systemów znakowych w społeczeństwie oraz w zbiorowościach biologicznych. Rozróżnia się źródła: ziarniste (dyskretne) - np. źródło podające litery, binarne - podające jedną z 2 możliwości „tak" i „nie", ciągłe — podające dowolne wiadomości z ciągłego ich zbioru.

infrastrukturę ekonomiczną (nazywaną także gospodarczą), którą tworzą obiekty, urządzenia i instytucje świadczące usługi w zakresie produkcji, transportu, komunikacji, energetyki itp., drugą zaś w dziedzinie prawa, bezpieczeństwa, kształcenia, oświaty, administracji państwa itp. Innym podziałem, który trzeba przywołać jest wyróżnienie *infrastruktury ogólnej i technicznej*, czy też zapewniającej wewnętrzne jak i zewnętrzne[70].

Dla podjętych w pracy rozważań ważną kwestią jest uwzględnienie w nich także takich pojęć jak *infrastruktura narodowa, obronna, wojskowa* oraz *obrony cywilnej*. ***Infrastruktura narodowa*** to infrastruktura zabezpieczona i finansowana przez państwa członkowskie NATO, na jego własnym terytorium, wyłącznie na użytek jego własnych sił zbrojnych[71].

Z kolei ***infrastruktura obronna*** to część infrastruktury państwa obejmująca obiekty i urządzenia stałe oraz instytucje niezbędne do funkcjonowania systemu obronnego państwa, która to tworzona jest głównie w czasie pokoju, ale rozwijana również w okresie zagrożenia i wojny[72]. Natomiast ***infrastruktura wojskowa*** to element infrastruktury obronnej obejmujący wszystkie stacjonarne, a w wyjątkowych wypadkach także ruchome obiekty i urządzenia, które zgodnie ze swym przeznaczeniem służą do zaspokojenia potrzeb sił zbrojnych[73]. Zaś ***infrastruktura obrony cywilnej*** to wszystkie obiekty, urządzenia i instytucje warunkujące skuteczność wykonywania zadań obrony cywilnej[74].

Dokonana identyfikacja istoty pojęć infrastruktura, a następnie przyporządkowanie jej do różnych obszarów działalności państwa i społeczeństwa stworzyło możliwość podjęcia próby określenia pojęcia infrastruktury telekomunikacyjnej. Aby to jednak było możliwe, celowym i pożądanym staje się dokonanie identyfikacji istoty pojęcia telekomunikacji oraz innych pojęć ściśle z nim związanych

Niezbędnym elementem sprawnego kierowania państwem, zarządzania gospodarką narodową, dowodzenia siłami zbrojnymi oraz kierowania pracą

---

[70]Por. W. Ślemp, *Infrastruktura*...wyd. cyt., s. 24÷25.
[71]Por. *Słownik terminów i definicji NATO*, MON, Warszawa 1998, s. 208.
[72]Por. *Słownik terminów z zakresu bezpieczeństwa*...wyd. cyt., s. 48.
[73]Tamże, s. 49.
[74]Tamże, s. 48.

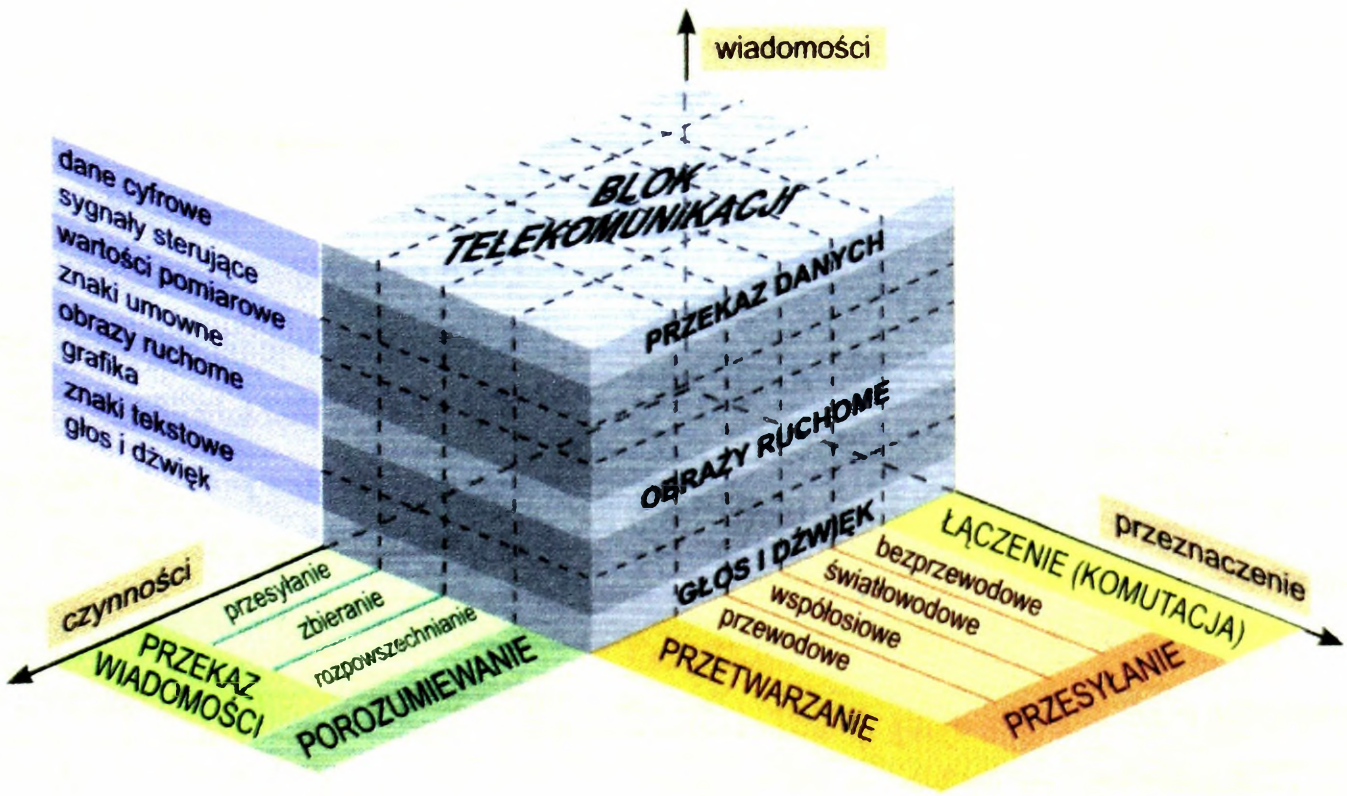
dwoma porozumiewającymi się abonentami jest sprawą umowną. Bowiem od zarania dziejów aż do współczesności wykorzystywano wszystkie możliwe zjawiska zachodzące w przyrodzie oraz środki transportowe umożliwiające przekaz wiadomości.

Telekomunikację można podzielić (Schemat 1.5.) ze względu na:

- przeznaczenie;
- rodzaj wiadomości;
- strukturę techniczną;
- rodzaje sygnałów;
- działalność gospodarczą.

Schemat 1.5.

Podział telekomunikacji



Źródło: *Net World Vademecum teleinformatyka cz. 1,* International Data Group Poland S.A., Warszawa 2004, s. 2.

Ze względu na ***przeznaczenie*** telekomunikację dzieli się na[81]:

---

[81] B. Zbierzchowski, P. Tomaszewicz, *Podstawy telekomunikacji cz. 1*, Instytut Telekomunikacji Politechniki Warszawskiej, Warszawa 2003, s. 4.

kraju i jego sprawności organizacyjno-technicznej funkcjonujących systemów, ich jakości, przepustowości i niezawodności. Staje się to możliwe, dzięki powszechnemu stosowaniu coraz nowocześniejszych środków łączności.

Łączność określa stopień doskonałości organizacyjnej społeczeństwa, obecnie społeczeństwa informacyjnego, które jest coraz bardziej uzależnione od stanu łączności, a przede wszystkim od zastosowanych systemów telekomunikacyjnych, informatycznych i mediów elektronicznych. Rozwijająca się telekomunikacja staje się jednym z podstawowych przedsięwzięć stanowiących istotny wkład w przyszłe społeczeństwo informacyjne. Obserwując światowe tendencje widzi się, że zmianom ulega samo pojęcie telekomunikacji.

Termin ***telekomunikacja*** wywodzi się z greckiego słowa *tele* (odległy) i łacińskiego *communicare* (dzielenie się z kimś, rozmowa), co łącznie oznacza przesyłanie wiadomości na odległość, bez wnikania, w jaki sposób i jakimi środkami zostanie to zrealizowane[77].

Telekomunikacja, dziedzina nauki i techniki oraz działalności ludzkiej dotycząca przekazywania na odległość wiadomości za pośrednictwem sygnałów elektrycznych[78].

Telekomunikacja, technika przekazywania wiadomości na odległość za pomocą impulsów elektrycznych, świetlnych lub fal elektromagnetycznych i nauka o tej technice[79].

We współczesnej terminologii termin telekomunikacja oznacza przesyłanie od nadawcy do odbiorcy głosu, dźwięku, sygnałów optycznych, danych, faksów, grafiki i obrazów ruchomych, umożliwiających odtwarzanie wiadomości.

Przesyłanie informacji na odległość za pomocą urządzeń elektronicznych zarówno w postaci sygnałów analogowych, jak i cyfrowych spełnia obecnie decydującą rolę jako podstawowy środek w komunikowaniu się między ludźmi[80].

Istotą telekomunikacji jest przesyłanie wiadomości na dalekie odległości, chociaż w obecnej terminologii określenie odległości między dwiema stacjami lub

---

[77]W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych,* Muza S.A., Warszawa 2001, s. 498 i 271.
[78]Por. *Internetowa encyklopedia PWN*, Praca zbiorowa, PWN, Warszawa 2003.
[79]Por. *Słownik Wyrazów Obcych*, Praca zbiorowa, pod kier. nauk., I. Kamińskiej-Szmaj, Warszawa 2001.
[80]Por. Net World *Vademecum teleinformatyka cz. 1,* International Data Group Poland S.A., Warszawa 2004.

z osiągnięciami telekomunikacji; pojęcie utożsamiane z technologią informacyjną.

Ze względu na ***strukturę techniczną*** telekomunikację dzieli się na:

- *urządzenia końcowe* – abonenci;
- *teletransmisja* - sieć dostępowa, łącza międzycentralowe;
- *teletransmisja impulsowa* (cyfrowa) - wyjątek;
- *telekomutacja* - centrale abonenckie (PABX)[83], centrale końcowe (CK), międzymiastowe (CMM), międzynarodowe(CMN).

Ze względu na ***rodzaj sygnału*** telekomunikację dzieli się na:

- *telekomunikację analogową*:
  - sygnały ciągłe;
  - teletransmisja analogowa;
  - komutacja przestrzenna (komutacja łączy);
- *telekomunikację cyfrową*:
  - sygnały impulsowe (cyfrowe, kodowane);
  - teletransmisja impulsowa (cyfrowa);
  - komutacja czasowa (komutacja kanałów, komutacja pakietów);
  - komutacja przestrzenna - wyjątek.

Ze względu na ***działalność gospodarczą*** telekomunikację dzieli się na[84]:

- *usługi* według Międzynarodowej Unii Telekomunikacyjnej (ITU-T)[85]
  - usługi interaktywne:
    - konwersacyjne;
    - przekaz wiadomości;
    - wyszukiwanie informacji.
  - usługi dystrybucyjne:
    - bez sterowania przez użytkownika;
    - ze sterowaniem przez użytkownika.

---

[83]Ang. Private Automated Branch Exchange – lokalny, automatyczny (najczęściej cyfrowy) system komutacji przeznaczony dla biur lub przedsiębiorstw do realizacji połączeń wewnętrznych i zewnętrznej publicznej sieci telefonicznej PSTN.

[84]B. Zbierzchowski, P. Tomaszewicz, *Podstawy telekomunikacji...* wyd. cyt., s. 7.

[85]ITU-T – ang. International Telecommunication Union Telecommunication Standarization Sector - Międzynarodowa Unia Telekomunikacyjna – organ tworzący światowe standardy technologii telekomunikacyjnych.

- *porozumiewawczą,* dotyczącą dwukierunkowego przekazywania wiadomości między dwoma lub więcej punktami (np. między aparatami telefonicznymi, usługi przywoławcze - paging – stanowią wyjątek);
- *rozsiewczą (dyfuzyjną),* dotyczącą jednokierunkowego przekazywania wiadomości z jednego punktu (np. radiostacji nadawczej, nadajnika telewizyjnego) do wielu punktów (np. odbiorników radiofonicznych, telewizyjnych);
- *zbiorczą*, dotyczącą jednokierunkowego przekazywania (zbierania) wiadomości z wielu punktów badawczych do odbiorczego (np. systemy nadzoru, monitoringu, teledetekcja, telemetria).

Ze względu na ***rodzaj wiadomości*** telekomunikację dzieli się na[82]:

- *telefonię* – która zajmuje się przesyłaniem na odległość dźwięku, głosu przy użyciu przewodów lub za pośrednictwem fal radiowych;
- *telegrafię* - zajmującą się przekazywaniem i reprodukowaniem treści dokumentów zawierających pismo, rysunki, fotografie itd., której to obecnie podstawową gałęzią jest symilografia, realizowana przy pomocy aparatów faksowych i telefaksowych;
- *radiofonię* - będącą system rozpowszechniania audycji radiowych; rozróżnia się radiofonię przewodową (tzw. radiowęzły, o znacznie ograniczonym zasięgu) realizowaną za pomocą odbiorników połączonych przewodami ze stacją nadawczą oraz bezprzewodową, wykorzystującą określone pasma częstotliwości fal radiowych;
- *telewizję* - zajmującą się przesyłaniem na odległość ruchomych obrazów wraz z towarzyszącym im dźwiękiem za pomocą sygnałów elektrycznych; rozróżnia się: telewizję programową oraz użytkową (obserwację zjawisk lub kontrolę procesów w badaniach naukowych);
- *teledację* – która dotyczy transmisji – z dużą wiernością - danych numerycznych lub alfanumerycznych;
- *telematykę* – to jest telekomunikację na usługach informatyki i odwrotnie; dziedzina nauki i techniki łącząca osiągnięcia informatyki

---

[82]Tamże, s. 5.

- *telekomutacją* – związaną z tworzeniem dróg połączeniowych, umożliwiającą tworzenie i likwidowanie zestawów łączy.

Najnowsza klasyfikacja ujmuje ***usługi telekomunikacyjne*** w dwie wzajemnie przenikające się grupy:

a) ***aplikacje telekomunikacyjne***[86];

b) ***usługi przenoszenia*** zwane również usługami transportowymi sieci.

Ad. a. W skład ***aplikacji telekomunikacyjnych*** wchodzą:

- telefonia;
- telegrafia (teleks, telegram);
- faksymile (fax);
- teleteks[87];
- wideoteks;
- wideotelefonia;
- telekonferencja;
- poczta elektroniczna, wymiana danych EDI (ang. Electronic Date Interchange);
- transmisja plików;
- łączenie sieci lokalnych LAN (ang. Local Area Network);
- dołączanie stacji roboczych do sieci LAN;
- dołączanie stacji roboczych lub sieci LAN do publicznych sieci komputerowych;
- dołączanie kas fiskalnych i bankomatów do sieci;
- bazy danych i elektroniczne wiadomości;
- transmisja nieruchomych obrazów;
- multimedia;
- telewizja;
- edukacja;
- biuro w domu (telepraca);

---

[86]Od łac. *applicare* – przymocować, przykładać się, inf. – częsta nazwa użytkowych programów komputerowych napisanych i przeznaczonych do określonych potrzeb i zadań np.: w telekomunikacji. Zob. w: W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych,* Muza S.A., Warszawa 2001, s, 42.

[87]Dodatkowa usługa głosowa oferowana w publicznej sieci telefonicznej polegająca na przekazywaniu abonentom komunikatów o charakterze informacyjno – rozrywkowym.

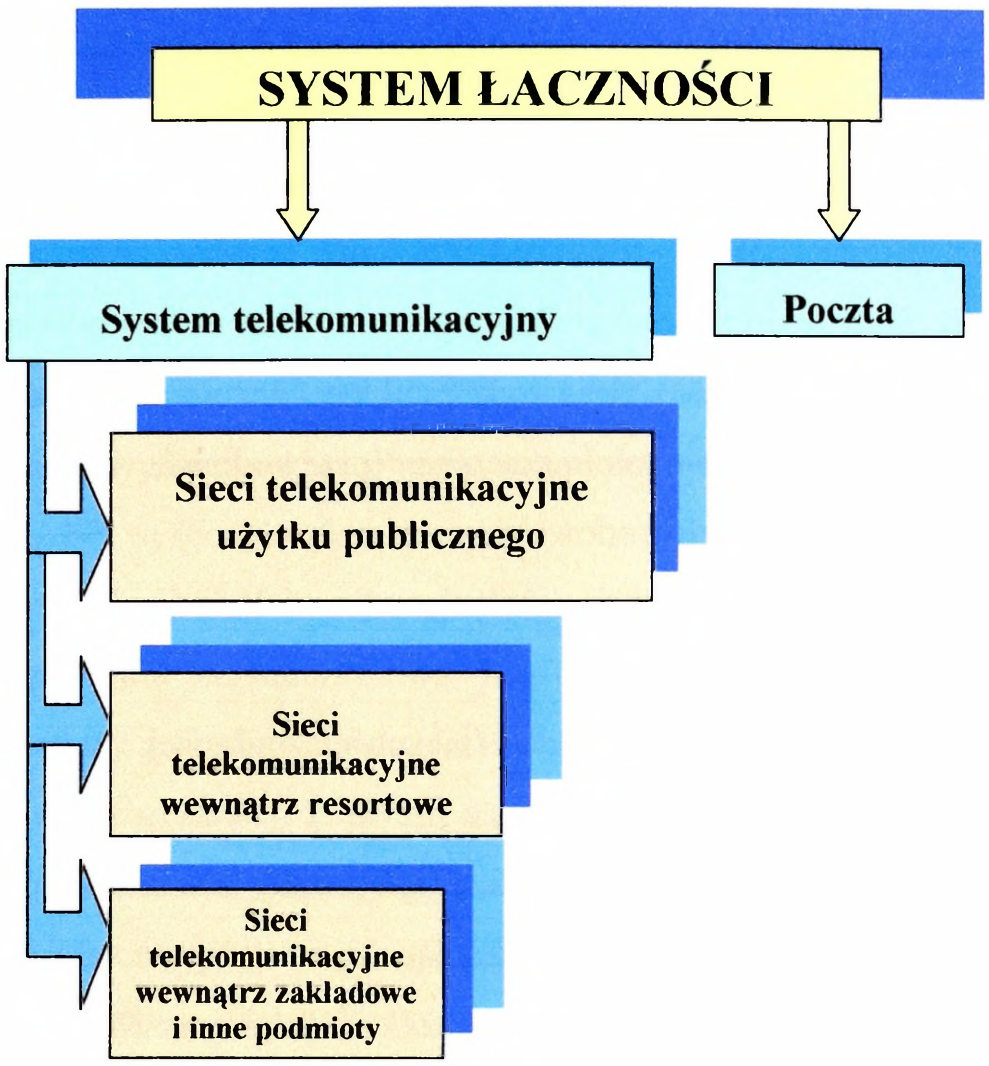
- *usługi* według TP S.A.:
  - usługi telefoniczne;
  - usługi w sieci ISDN (ang. Itegrated Services Digital Network);
  - usługi w sieci inteligentnej IN (ang. Intelligent Network);
  - usługi telegraficzne:
    - usługi telegramowe;
    - teleks;
    - miniteleks.
  - usługi transmisji danych;
  - usługi telematyczne;
  - usługi informatyczne;
  - usługi radiokomunikacji naziemnej;
  - usługi radiokomunikacji satelitarnej;
  - usługi wizyjne;
  - usługi multimedialne;
  - usługi dzierżawy;
  - dzierżawa łączy telekomunikacyjnych;
  - dzierżawa kanalizacji telekomunikacyjnej;
  - prywatna sieć wirtualna VPN (ang. Virtual Private Network).
  - inne:
    - książki telefoniczne;
    - systemy subskrypcji usług;
    - sprzedaż, serwis, instalacja urządzeń.
- *produkcja;*
- *kooperacja;*
- *doradztwo;*
- *inne.*

Ze względu na ***rodzaj wykonywanych operacji*** w procesie przekazywania wiadomości wyróżnia się odrębne dziedziny zajmujące się: techniką przetwarzania wiadomości na sygnał i odwrotnie:

- *teletransmisją* – związaną z przesyłaniem sygnałów po łączach;

Schemat 1.6.

System łączności państwa (Wariant)



Źródło: Opracowanie własne

System telekomunikacyjny to linie i urządzenia telekomunikacyjne zorganizowane według określonych zasad oraz współpracujące ze sobą i służące do nadawania, przenoszenia i odbioru mowy, dźwięków, znaków pisma, obrazów ruchomych i nieruchomych oraz innych postaci informacji za pomocą przewodów, fal radiowych lub innych systemów elektrycznych[89].

Sieć telekomunikacyjna to zespół funkcjonalnie powiązanych różnych linii i urządzeń telekomunikacyjnych, rozmieszczonych przestrzennie na określonym obszarze o dowolnej konfiguracji, tworzących węzły i połączenia międzywęzłowe a przeznaczonych do świadczenia usług telekomunikacyjnych.

Linia telekomunikacyjna to tor[90] przewodowy, światłowodowy, lub ich

---

[89]Zob. *Net World Vademecum teleinformatyka cz. 1,* International Data Group Poland S.A., Warszawa 2004, s. 57 i 66.

[90]Tor telekomunikacyjny- konstrukcja techniczna, będąca układem elektrycznym biernym w zasadzie linearnym, umożliwiająca realizację przestrzennego kanału telekomunikacyjnego.

- telezakupy;
- teleusługi socjalne i medyczne;
- teleakcje (telenadzór, telemetria, telealert itp.)
- inne aplikacje wspomagające.

Ad. b. ***Usługi przenoszenia*** (transportowe) zapewniające właściwy przekaz informacji to:

- analogowa publiczna sieć telefoniczna PSTN (ang. Public Switched Telephone Network) z komutacją łączy;
- cyfrowa publiczna pakietowa sieć transmisji danych PSDN (ang. Public Switched Date Network) z komutacją pakietów;
- cyfrowa sieć z integracją usług ISDN (ang. Integrated Services Digital Network);
- asynchroniczna sieć ATM (ang. Asynchronous Transfer Mode);
- linia dzierżawiona (miedziana lub światłowodowa) stała;
- łączność bezprzewodowa (analogowa lub cyfrowa);
- łączność satelitarna VSAT (ang. Very Small Aperture Terminal);
- transmisja rozgłoszeniowa (naziemna lub satelitarna).

Każdy zespół, organizacja dysponująca informacjami, wykorzystuje do ich przechowywania, przetwarzania i przesyłania systemy teleinformatyczne. Potrzeba świadczenia usług telekomunikacyjnych na całym obszarze kraju nie wpłynęła jednak na opracowanie ścisłych ustaw i przepisów prawnych, które stanowią podstawę efektywnej działalności sektora telekomunikacji i innych resortów w zakresie wymiany informacji pomimo, że obowiązują już od dawna we wszystkich krajach wysoko rozwiniętych.

Przesyłanie informacji w systemie informacyjnym państwa realizowane jest przez system[88] łączności państwa, który obejmuje system telekomunikacyjny i pocztę (Schemat 1.6.).

System łączności państwa jest to zbiór współpracujących ze sobą urządzeń i linii telekomunikacyjnych, środków i linii pocztowych, środków sygnalizacyjnych zgodnie z obowiązującymi zasadami współdziałania.

---

[88]System to uporządkowany wewnętrznie układ elementów tworzący określoną strukturę całościową, wyposażony w obowiązujący norm reguł, wraz ze środkami zapewniającymi mu funkcjonalność.

- publiczna sieć telefoniczna z komutacją łączy PSTN (Public Switched Telephone Network);
- publiczna sieć z komutacją kanałów CSPDN (Curcuit Switched Public Data Network);
- publiczna sieć z komutacją pakietów PSPDN (Public Switched Packed Data Network);
- sieć telegraficzna (Telex);
- radiotelefoniczne sieci komórkowe MT (Mobile Telephony);
- sieci wydzielone o charakterze lokalnym lub prywatnym (PABX, LAN[92], dyspozytorskie, specjalne).

Publiczne sieci telekomunikacyjne są ważnym środkiem łączności mającym ważne znaczenie dla bezpieczeństwa państwa. Do walorów użytkowych sieci publicznych należy jednolitość usług wynikająca szerokiego zakresu normalizacji krajowej i międzynarodowej. Z uwagi na otwartość pozwalają na komunikacje ze wszystkimi podmiotami. Stanowią także zapasowy środek łączności dla użytkowników sieci wydzielonych. Wszystkie jednostki administracji publicznej wyposażone są w systemy łączności korzystające z publicznej sieci telefonicznej. Sieć ta umożliwia wykonywanie połączeń telefonicznych w ruchu miejscowym, krajowym i międzynarodowym.

Większość jednostek posiada dostęp do Internetu. Powoduje konieczność stosowania środków ochrony bezpieczeństwa teleinformatycznego, zatrudniania wysokiej klasy specjalistów i wyposażenia w urządzania firewall[93]. Posiadanie specjalizowanego personelu, w przypadku rozdrobnienia jednostek administracji publicznej nie zawsze może być spełnione.

Dodatkowe zagrożenia stwarza nagminne używanie zewnętrznych serwerów bezpłatnych kont poczty elektronicznej (wobec niewystarczającej liczby kont w wydzielonych serwerach) do wymiany dokumentów służbowych. Stwarza to poważne zagrożenie bezpieczeństwa teleinformatycznego. W łączności

---

[92]Ang. Local Area Network – Komputerowa sieć o charakterze lokalnym, łącząca grupę użytkowników pracujących na stosunkowo niewielkim obszarze (grupa robocza, budynek, przedsiębiorstwo, kampus) stanowiąca metodę przekazywania wiadomości tekstowych i informacji cyfrowych.

[93]Zapora ogniowa zapewniająca bezpieczeństwo i ochronę dostępu do sieci, informacji, węzłów sieci i baz danych.

zespół (np. falowody, linie świetlne), wraz z konstrukcjami i urządzeniami, rozmieszczonymi wzdłuż określonej trasy, służącymi do przesyłania informacji na odległość.

Sieci telekomunikacyjne, stanowią zasadniczą część infrastruktury telekomunikacyjnej państwa i przeznaczone są do świadczenia usług na potrzeby ogółu społeczeństwa, gospodarki narodowej oraz organów władzy państwowej i administracji. Sieci te, mogą być analogowe lub cyfrowe. Sieci telekomunikacyjne mogą być utworzone przez:

- obiekty i linie telekomunikacyjne (przewodowe, kablowe, radiowe, falowodowe, światłowodowe);
- obiekty teletransmisyjne (stacje wzmacniakowe, stacje radioliniowe, regeneratory, itp.);
- obiekty radiokomunikacyjne (łączności radiowej, radiotelefonicznej, radiofonii i telewizji);
- naziemne stacje łączności satelitarnej i satelity komunikacyjne.

Najstarsza, nadal jeszcze funkcjonująca infrastruktura telekomunikacyjna o charakterze publicznym PSTN *(Public Switched Telephone Network)* jest oparta na komutacji łączy (linii telefonicznych). Podstawowa oferta usług w sieci PSTN, a obejmująca tylko automatyczną komutację kanałów rozmównych, jest stopniowo powiększana o usługi rozszerzone i dodatkowe - związane z wprowadzeniem bardziej inteligentnych cyfrowych systemów komutacji. Należą do nich:

- usługi podstawowe - zestawianie połączeń za pomocą aparatów z tarczą numerową lub tonową, restrykcje zestawień, taryfikacja itp.);
- usługi rozszerzone - rozmowy trójstronne, telekonferencje, przekierowanie rozmów, audioteks, gorąca linia, in.);
- usługi dodatkowe - poczta głosowa, poczta elektroniczna, usługa Centrex[91], usługi ISDN oraz usługi sieci inteligentnej IN).

W kraju działa wiele typów sieci telekomunikacyjnych o charakterze publicznym:

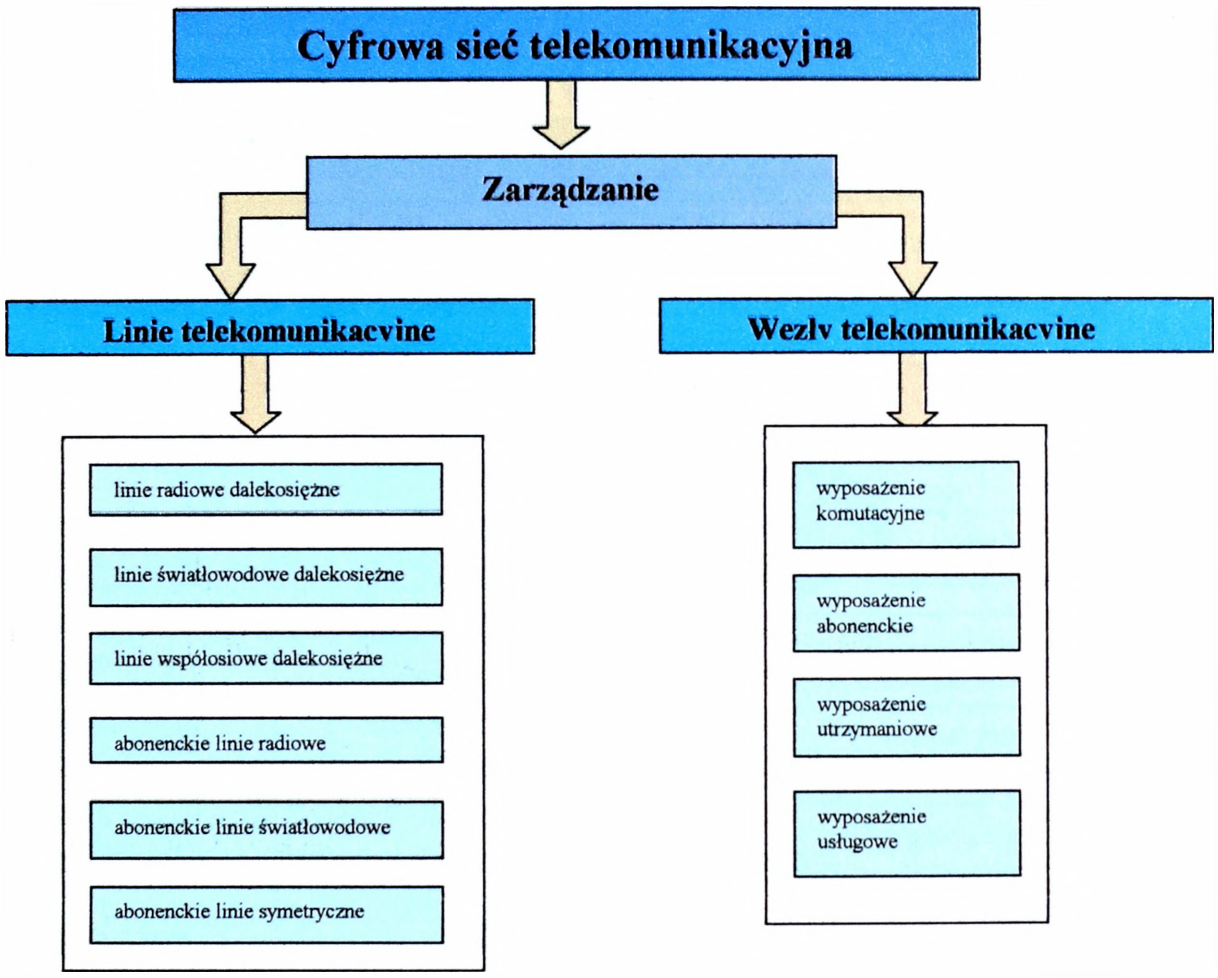
---

[91]Usługa Centrex realizuje funkcję centrali abonenckiej PABX w publicznej centrali telefonicznej lub systemie komutacji. Połączenia abonenckie w ramach przedsiębiorstwa są automatycznie przekierowywane do centrali publicznej, tam komutowane i kierowane z powrotem do przedsiębiorstwa lub do innej grupy abonentów w innym obszarze.

teletransmisyjne i węzły komutacyjne o strukturze międzynarodowej i międzymiastowej, strefowej, które tworzą wyspecjalizowane usługowo sieci telefoniczne, telegraficzne, transmisji danych, radiokomunikacyjne, radiofoniczne, i telewizyjne.

Schemat 1.8.

Ogólny podział cyfrowych sieci telekomunikacyjnych



Źródło: Opracowanie własne na podstawie: J. Michniak, Z. Fiołna, *Sieć łączności państwa,* AON. Warszawa 2001, s. 15.

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

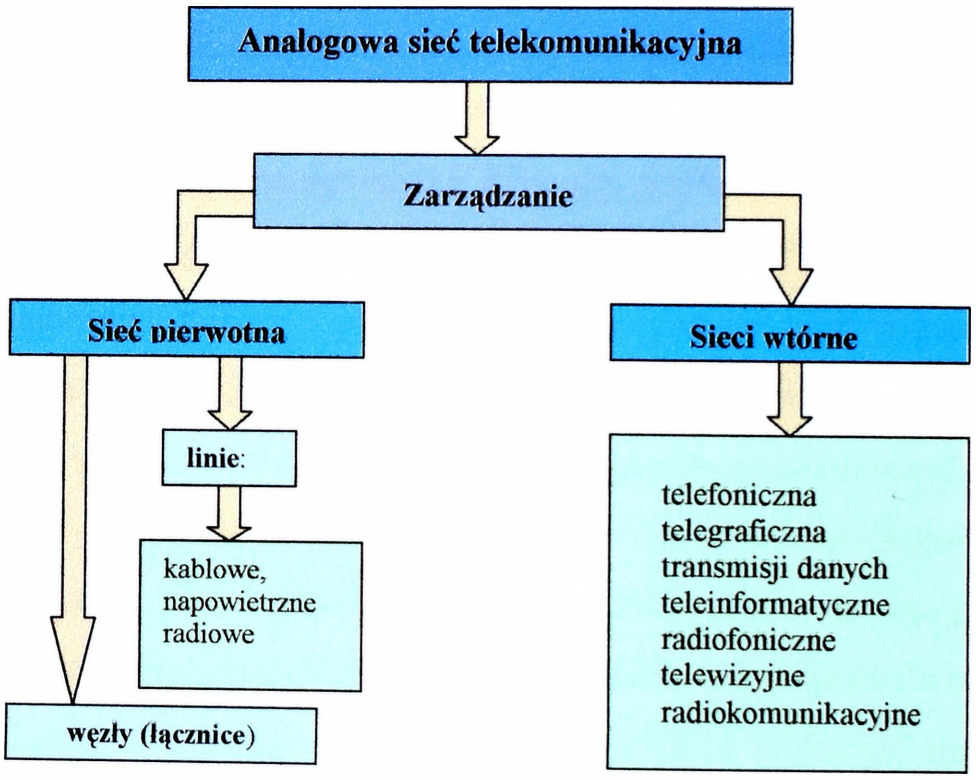
- system Strowgera (w zaniku na poziomie central okręgowych);
- system krzyżowy (Pentaconta 1000C, K66, LNI.) na poziomie central okręgowych, międzymiastowych, także zespolonych;
- system elektroniczny (E-10A) na poziomie central okręgowych;
- nowoczesne systemy komutacji cyfrowej:
  - Alcatel 1000 S12;
  - Lucent Technologies 5ESS/7RE;

bezprzewodowej (analogowej lub cyfrowej) szeroko wykorzystywane są sieci komórkowe GSM oprócz rozmów telefonicznych także przez Państwową Straż Pożarną, Policję i Straż Graniczną dla potrzeb transmisji danych oraz stanowią także główny środek łączności dla współdziałania ze służbami np.: porządku publicznego i ratownictwa technicznego.

W analogowych publicznych sieci telekomunikacyjnych (Schemat 1.7.) przy odwołaniu się do kryterium zarządzania ogólnie można wyróżnić sieć pierwotną i sieci wtórne.

Schemat 1.7.

Ogólny podział analogowych sieci telekomunikacyjnych



Źródło: Opracowanie własne na podstawie: J. Michniak, Z. Fiołna, *Sieć łączności państwa*, AON. Warszawa 2001, s. 14.

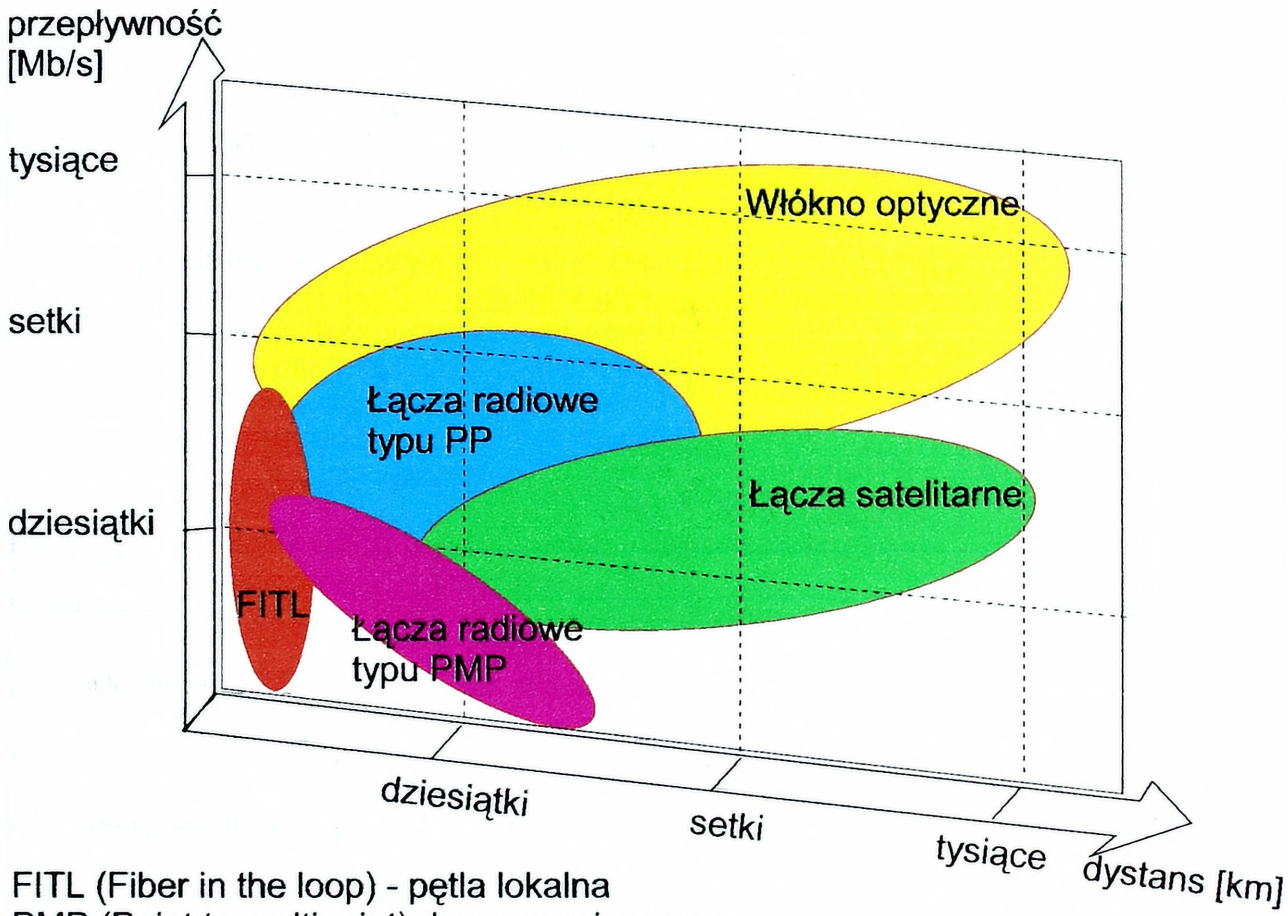
Natomiast sieci cyfrowe (Schemat 1.8.) w oparciu o te same kryterium można podzielić na linie telekomunikacyjne i węzły telekomunikacyjne. Działają one na najwyższych i środkowych warstwach sieci telekomunikacyjnej, na poziomie łączy międzynarodowych, central międzymiastowych i niektórych zespolonych central okręgowych.

W ***sieci telekomunikacyjnej użytku publicznego*** (Schemat 1.9.) stanowiącej podstawowe ogniwo systemu telekomunikacyjnego państwa można wyróżnić linie

i tłumików zakłóceń do przesyłania sygnałów o wyższych częstotliwościach. Dlatego też, do realizacji określonych usług przeznaczone są różne rodzaje ***łączy telekomunikacyjnych***[94], które posiadają różne przepływności i zasięg (Schemat 1.10.), a szczególnie cechy użytkowe (Tabela 1.1.).

Schemat 1.10.

Typowe przepływności i zasięgi łączy telekomunikacyjnych



FITL (Fiber in the loop) - pętla lokalna
PMP (Point to multipoint) -łącza rozsiewcze
PP (Point to point) - radiolinie

Źródło: Net World *Vademecum teleinformatyka cz. 1*, International Data Group Poland S.A., Warszawa 2004, s. 3.

Sieć telekomunikacyjna użytku publicznego nadal charakteryzuje się dużą różnorodnością wykorzystywanego w niej sprzętu: od przestarzałych analogowych systemów do systemów cyfrowych, od przewodowych systemów po systemy satelitarne. Pomimo szybkiego rozwoju techniki i technologii telekomunikacyjnych oraz szerokiej gamy usług, to jeszcze nadal dominującą rolę spełnia jednak rynek telefonicznych usług telekomunikacyjnych.

---

[94]Łącze - zespół środków technicznych umożliwiających przesyłanie sygnałów od punktu do punktu, przeznaczony do określonego rodzaju usługi telekomunikacyjnej, jednej i tylko jednej w danej chwili, przy założeniu, że zespół ten w warunkach eksploatacyjnych nie podlega podziałowi na krótsze odcinki.

– Siemens EWSD;

– DGT 3450.

Schemat 1.9.

Uproszczona struktura sieci telekomunikacyjnej użytku publicznego



Źródło: Opracowanie własne na podstawie: J. Michniak, Z. Fiołna, *Sieć łączności państwa*, AON. Warszawa 2001, s. 19.

W sieciach telekomunikacyjnych do połowy lat siedemdziesiątych stosowano powszechnie technikę przesyłania sygnałów analogowych za pomocą kanałów telefonicznych w podstawowym paśmie przenoszenia lub przez kosztowne międzycentralowe urządzenia zwielokrotnienia częstotliwościowego o niewielkiej krotności kanałów rozmównych. Jako linie przesyłowe w łączach telekomunikacyjnych stosowano wyłącznie pary kabli miedzianych o ograniczonej częstotliwości pracy, wymagające skomplikowanych filtrów, korektorów linii

Tradycyjna telekomunikacja oparta na komunikacji porozumiewawczej obejmującej usługi telefoniczne, telegramowe i teleksowe wymagała kanałów o niewielkiej przepływności, wykorzystujących prawie wyłącznie analogowe linie telefoniczne z podstawowym pasmem przenoszenia w zakresie 300 ÷ 3400 Hz.

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

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

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

Od kilku lat rośnie też zainteresowanie budową i modernizacją resortowych sieci telekomunikacyjnych, a w ostatnim czasie przede wszystkim nowych sieci o technologii multimedialnej[95]. To z kolei spowodowało wzrost zainteresowania centralami wyposażonymi w możliwość świadczenia usług ISDN i zaawansowanych usług multimedialnych (Schemat 1.11). W aktualnej ofercie dostawców cyfrowych central abonenckich wyposażenie tych urządzeń telekomunikacyjnych w możliwość świadczenia usług ISDN jest już prawie standardem.

Szeroka identyfikacja obszaru „telekomunikacji", a wcześniej również pojęcia infrastruktura upoważnia do zidentyfikowania jednego z dwóch głównych przedmiotów dociekań a mianowicie pojęcia (terminu) infrastruktura telekomunikacyjna.

---

[95]Środowisko umożliwiające równoczesne przekazywanie i prezentację kilku usług telekomunikacyjnych, za pomocą tych środków technicznych oddziaływujących na zmysły człowieka.

Tabela 1.1. Rodzaje i cechy użytkowe łączy telekomunikacyjnych

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

Źródło: Opracowanie własne na podstawie: *Metody oceny efektywności systemów łączności na potrzeby obronności państwa. Synteza wyników badań.* Praca naukowo – badawcza, pod kier. nauk. M. Krauze, AON, Warszawa 1998, s.72.

podjętych w rozprawie rozważań rozumieć należy: *zbiór obiektów i urządzeń telekomunikacyjnych zapewniających poprzez przekaz informacji (wiadomości) należyte funkcjonowanie społeczeństwa we wszystkich obszarach jego działalności.*

Odnosząc tak rozumianą infrastrukturę telekomunikacyjną[97] do bezpieczeństwa ekonomicznego, podkreślić trzeba, że jest ona infrastrukturą państwa ujawniającą zarówno charakter społeczny, ekonomiczny, techniczny jak i obronny. Charakter ten z kolei generuje określone wymagania i oczekiwania wobec infrastruktury telekomunikacyjnej.

Obecnie ***infrastruktura teleinformatyczna*** kraju obejmuje dwie do niedawna odrębne, a obecnie coraz bardziej przenikające się hierarchiczne struktury komunikacyjne: rozległe ***cyfrowe sieci komputerowe*** oparte na strukturach sieciowych typu LAN, MAN[98] i WAN[99] oraz ***sieci telekomunikacyjne***, dla których centralnym punktem nadal pozostają cyfrowe systemy komutacji (centrale) wraz z różnorodnymi sieciami dostępu abonenckiego.

*W **sieciach komputerowych*** podstawową strukturę teleinformatyczną dostępu lokalnego tworzą sieci LAN typu Ethernet (10 Mb/s i 100 Mb/s, 1000 Mb/s), Token Ring (4 i 16 Mb/s) i FDDI[100] (100 Mb/s), przeznaczone dla indywidualnych lub grupowych użytkowników z wykorzystaniem zasobów multimedialnych. Fragmenty tych homogenicznych i heterogenicznych sieci komunikacyjnych są łączone między sobą za pomocą węzłów (mosty, huby, routery, multipleksery) umożliwiających tworzenie sieci szkieletowych w budynkach wielokondygnacyjnych, jak i magistrali telekomunikacyjnych (PDH, SDH, ATM).

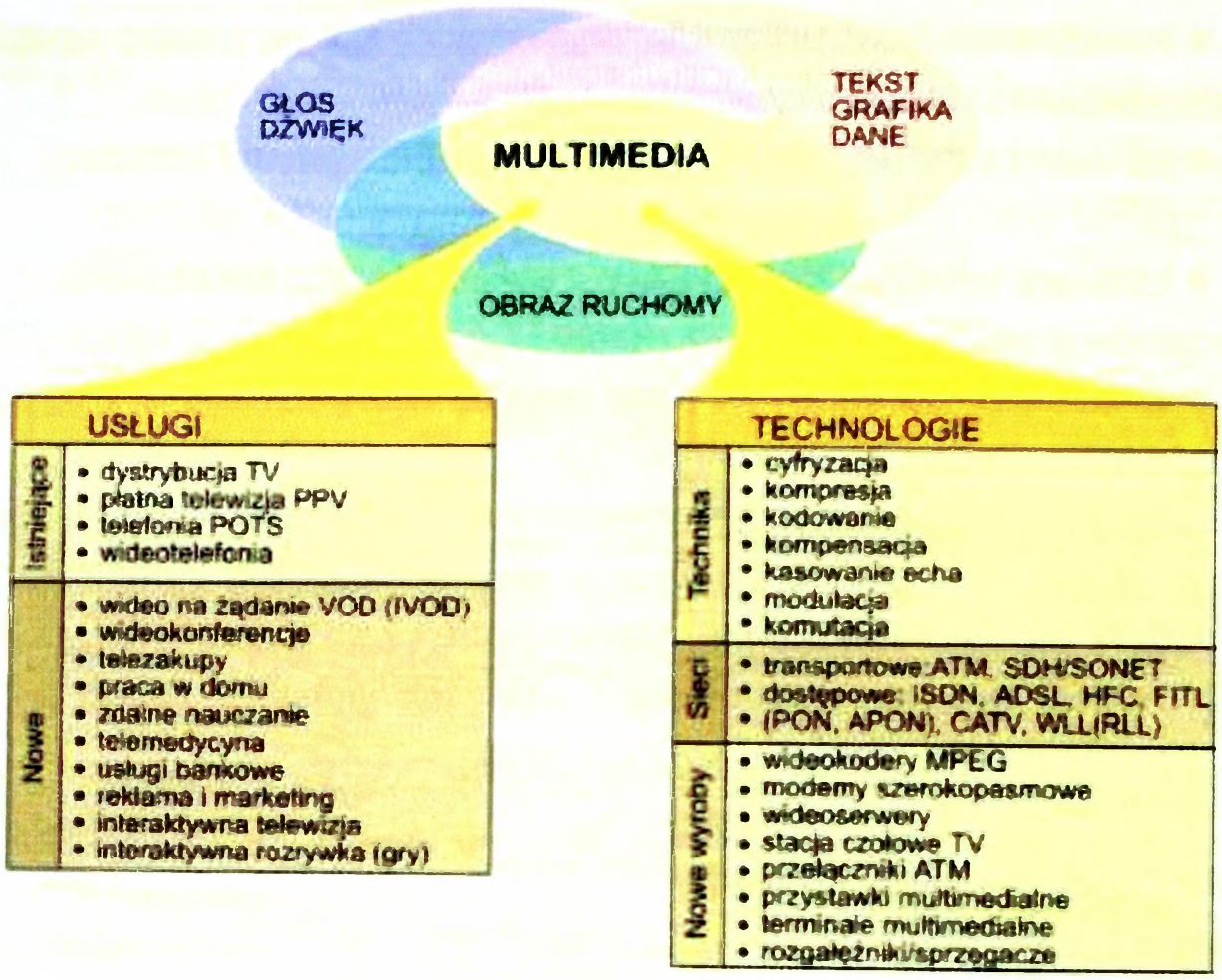
W ***sieciach telekomunikacyjnych*** zaczyna dominować warstwowa struktura komunikacyjna (Schemat 1.12.) w wyższych poziomach transportowych (PDH, SDH, ATM, DTM[101]) całkowicie oparta na przekazach cyfrowych, a poszczególne

---

[97]Por. *Prawo telekomunikacyjne*, Ustawa z dnia 16 lipca 2004 r., (Dz. U. Nr 171 poz.1800, art. 2 pkt 8.).
[98]Ang. Metropolitan Area Network - Miejska lub kampusowa szkieletowa sieć komputerowa nie przekraczająca łącznie długości 100 km.
[99]Ang. Wide Area Network - Rozległy system komunikacyjny () łączący miejskie sieci komputerowe MAN.
[100]Ang. Fiber Distributed Data Interface - Światłowodowa sieć cyfrowa o topologii podwójnego pierścienia stosowana w sieciach LAN i MAN.
[101]Ang. Dynamic Synchronous Transfer Mode – technologia dynamicznie i dyskretnie skalowanej transmisji o wysokiej przepływności od 512 kb/s do 2,5Gb/s do transmisji obrazów w czasie rzeczywistym.

Schemat 1.11.

Usługi i technologie multimedialne



Źródło: Net World *Vademecum teleinformatyka cz. 1,* International Data Group Poland S.A., Warszawa 2004, s. 3.

Uzasadnionym wydaje się przy próbie zdefiniowania przyjęcie dwóch wstępnych ustaleń: pierwszego, że pod pojęciem „infrastruktury" rozumieć należy obiekty, urządzenia stałe i ruchome oraz instytucje usługowe (krajowe i międzynarodowe) niezbędne do należytego funkcjonowania społeczeństwa, to znaczy zarówno produkcyjnych jak i nieprodukcyjnych działów gospodarki oraz bezpieczeństwa ludności[96]; drugiego, że telekomunikacja będzie postrzegana w ujęciu systemowym, to jest jako zespół działań społecznych zmierzających do przekazania za pomocą odpowiednich technik impulsów elektrycznych, świetlnych lub fal elektromagnetycznych, wiadomości na odległość.

W ślad za tym, pod pojęciem infrastruktury telekomunikacyjnej, dla potrzeb

---

[96]Por. Słownik terminów z zakresu bezpieczeństwa ...wyd. cyt., s. 47.

- torami światłowodowymi, przez sieci optyczne FITL lub za pomocą techniki hybrydowej HFC i modemów DSL. Odrębną grupę stanowią bezprzewodowe sieci dostępu abonenckiego RRL funkcjonujące w kilku standardach europejskich, specjalizowane sieci teledacyjne, przywoławcze i komórkowe (NMT, GSM, DCS), jak i systemy komunikacji i nawigacji satelitarnej (VSAT, GPS, UMTS, i inne).

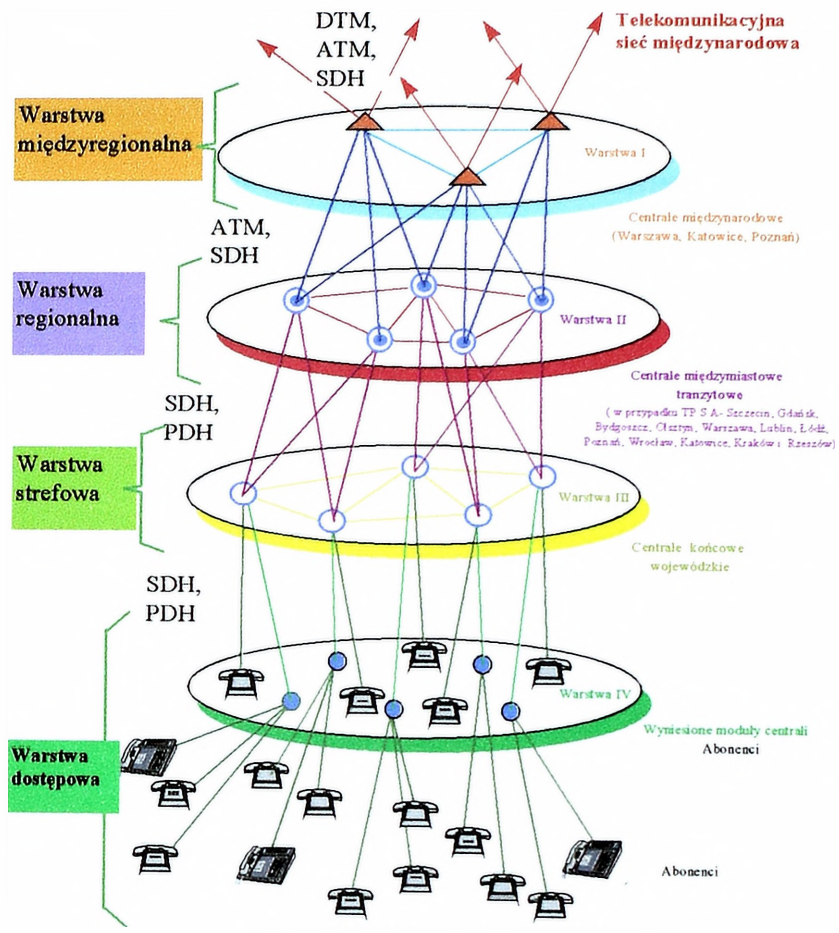
Już dziś jest jasne, że obecność w NATO oraz uczestnictwo w strukturach Unii Europejskiej wymuszają na nas konieczność posiadania infrastruktury i systemu telekomunikacyjnego, kompatybilnego z systemami tych organizacji. Wynika stąd potrzeba konsultacji i wymiany doświadczeń w dziedzinie organizacji i zabezpieczenia funkcjonowania systemu łączności państwa z przedstawicielami państw Europy Zachodniej.

Telekomunikacja niemal od początków swojej historii miała charakter międzynarodowy. Może ona pełnić swoją funkcję tylko w warunkach jednolitości standardów umożliwiających współpracę sieci i systemów wszystkich krajów. Wielkość i dynamika rozwoju rynku telekomunikacyjnego powoduje konieczność uzgadniania i stosowania standardów obowiązujących wszystkich, którzy działają na tym rynku. Jednolitość standardów zwiększa także możliwości swobodnego dostępu do rynku wielu dostawców sprzętu i usług. Zasady standaryzacji stały się podstawą obowiązujących obecnie uregulowań prawnych w Unii Europejskiej podstawą uregulowań są ujednolicone procedury dotyczące uznawania standardów telekomunikacyjnych (Wspólne Europejskie Regulacje Techniczne) oraz procedury badań technicznych i wydawania certyfikatów zgodności sprzętu z obowiązującymi standardami. Przyjęcie zasady wzajemnego uznawania certyfikatów przez kraje członkowskie Unii prowadzi do tego, że urządzenia telekomunikacyjne pochodzące z poszczególnych krajów Unii mogą być sprzedawane i użytkowane na terenie krajów Unii. Należy zauważyć, że stosowany w UE wymóg certyfikacji końcowych urządzeń telekomunikacyjnych jest bezwzględny, a zasada wzajemnego uznawania certyfikatów nie obejmuje krajów nie będących członkami UE. Utrzymywanie jednolitości systemów telekomunikacyjnych jest jedną z głównych funkcji Międzynarodowego Związku Telekomunikacyjnego (franc. Union International des Telekomunications – UIT), którego częścią jest Międzynarodowy Doradczy

poziomy są łączone ze sobą również za pomocą węzłów (krotnice synchroniczne, mltipleksery, krotnice PCM, routery).

Schemat 1.12.

Uproszczony warstwowy schemat infrastruktury telekomunikacyjnej kraju



Źródło: Opracowanie własne na podstawie E. Piedziuk *System łączności w stanach nadzwyczajnych z punktu widzenia potrzeb obronnych państwa,* RCSC, AON, Warszawa 1998, s. 37.

Na najniższym poziomie komutacji funkcjonują systemy komutacji (cyfrowe) i centrale telefoniczne (głównie analogowe), a także analogowe i cyfrowe centrale abonenckie PABX. Oddaleni indywidualni użytkownicy mają możliwość włączenia się do sieci teleinformatycznej:

- komutowaną lub dzierżawioną linią telefoniczną za pośrednictwem modemów i central telefonicznych PABX;
- kanałami cyfrowymi ISDN, przez centralę lub systemem komutacji cyfrowej;
- kanałami telewizji kablowej, z wykorzystaniem kanału zwrotnego i modemów szerokopasmowych RF (Radio Frequency), zwanych kablowymi;

inaczej jest skonstruowany system obronności państwa, w konsekwencji również podsystem kierowania nim i jego system łączności. Aby system łączności kierowania obronnością państwa i dowodzenia siłami zbrojnymi zapewnił najwyższym organom władzy i administracji państwa skuteczne i efektywne kierowania i dowodzenie to przewiduje się organizowanie określonych węzłów, sieci łączności i linii łączności dla stacjonarnych i mobilnych (polowych) stanowisk kierowania i dowodzenia takich jak: SKOP - 1,2,3, prezydenta; SK: premiera, ministrów (urzędów centralnych i instytucji) i wojewodów oraz SD, ZSD, WSD, PSD, CSD, ZCSD, PŁSD, PD, PDO dowódców: SZ, RSZ, OW, ZO jak również kierowanie z dotychczasowych miejsc pracy (DMP) i organizowanych zapasowych miejsc pracy (ZMP).

Oznacza to, że wcześniej powinny być przygotowane siły i środki umożliwiające zorganizowanie stanowisk kierowania i dowodzenia. W związku z tym należy przygotować infrastrukturę telekomunikacyjną określonych rejonów kraju i posiadać osobne, mobilne węzły łączności przeznaczone uzupełnienia struktury stacjonarnej jak i do zabezpieczenia pracy doraźnie organizowanych stanowisk kierowania obroną państwa oraz mobilnych (polowych) stanowisk i punktów dowodzenia sił zbrojnych. Wskazane uwarunkowania wynikają z przewidywanego charakteru ewentualnych przyszłych działań w systemie obronności oraz możliwości zapewnienia większego bezpieczeństwa łączności organom kierowniczym i dowódczym w odpowiednio przystosowanych i przygotowanych obiektach. Stanowiska kierowania i dowodzenia określonych szczebli w zależności od potrzeb ich osób funkcyjnych przewiduje się wyposażyć w urządzenia końcowe łączności i informatyki o różnych możliwościach świadczonych usług. Uwarunkowania te wynikają z przewidywanego charakteru przyszłych działań obronnych oraz możliwości zapewnienia większego bezpieczeństwa łączności organom kierowniczym i dowodzenia w odpowiednio przystosowanych i przygotowanych obiektach.

W systemie łączności powinny być przewidziane wielotorowe i niezależne przekazywanie informacji między osobami funkcyjnymi lub zautomatyzowanymi miejscami ich pracy z uwzględnieniem struktury powiązań funkcjonalnych

Komitet Telegrafii i Telefonii (franc. Comite' Consultatif International Telegraphique et Telephonique – CCITT) z siedzibą w Genewie. Korzystanie z wyników prac CCIT, a w szczególności z materiałów roboczych, jest niezbędnym elementem działań praktycznych w dziedzinie telekomunikacji. Pozwala bowiem zarówno na poznawanie problemów i możliwości ich rozwiązywania, jak i na obserwację ich opracowywania w CCIT, a także utrzymanie spójności swojej działalności a przede wszystkim rozwoju telekomunikacji z tendencjami światowymi.

1.2.2. Uwarunkowania kształtowania infrastruktury telekomunikacyjnej państwa

Rola i znaczenie kierowania oraz dowodzenia w systemie bezpieczeństwa państwa stale wzrasta, a sam proces staje się coraz bardziej złożony. Spowodowane jest to postępem w technice i technologii teleinformatyki ostatnich lat, a także zmianami w sposobach prowadzenia działań w systemie obronności państwa. Dlatego też doskonalenie systemu kierowania oraz dostosowanie go do wymagań bezpieczeństwa państwa wynika między innymi ze wzrostu stopnia złożoności warunków, w jakich kształtuje się system obronności państwa, zmian ilościowych i jakościowych w treści kierowania czy dowodzenia oraz coraz krótszego czasu na przedsięwzięcia organizacyjne w działaniach. Wszystko to stwarza potrzebę wprowadzenia do infrastruktury teleinformatycznej kraju również nowoczesnych technicznych środków i metod kierowania czy też dowodzenia.

Skuteczność systemu kierowania i zarządzania państwem, sterowania gospodarką narodowa, dowodzenia siłami zbrojnymi oraz funkcjonowania organów bezpieczeństwa publicznego jest uzależniona od niezawodnie i efektywnie funkcjonującego systemu łączności państwa. Zdolność wykonania stojących przed nim zadań zależy między innymi od stanu rozbudowy infrastruktury systemu telekomunikacyjnego (łączności) na obszarze całego kraju i jego sprawności organizacyjno-technicznej. Natomiast szczególne znaczenie przypada łączności w okresie szczególnych zagrożeń państwa a przede wszystkim w czasie stanów nadzwyczajnych (zagrożeń).

Zagrożenia, bezpieczeństwa państwa i działania w okresie sytuacji kryzysowych będą zdecydowanie inne niż dotychczas przyjmowane, a zatem

- wielkość traktów (liczba kanałów), potrzebnych do przekazania określonej ilości strumieni informacyjnych z wymaganą jakością;
- liczba, typ (rodzaj) linii łączności;
- zapewnienie kontroli i przydziału częstotliwości;
- zapewnienie terminowej wymiany wszystkich rodzajów informacji z wymaganą wiarygodnością i skrytością;
- automatyczne utajnianie informacji przekazywanych w relacjach, traktach (kanałach) łączności.

Przedstawione ogólne uwarunkowania i zadania dotyczące łączności i systemu łączności odnoszą się również do węzłów, gdzie powinny być rozważone takie zagadnienia jak:

- wyprzedzająca gotowość obronna;
- zapewnienie wewnętrznej łączności na SK i SD;
- zapewnienie wymiany wszystkich rodzajów informacji (wiadomości) w ustalonym czasie z niezbędną wiarygodnością;
- trwałość funkcjonowania w warunkach oddziaływania środków rażenia przeciwnika i wojny radioelektronicznej;
- wysoka mobilność polowych węzłów łączności;
- ścisła realizacja przedsięwzięć bezpieczeństwa łączności.

Dla systemu kierowania obronnością państwa w sytuacjach zagrożeń, a szczególnie stanach nadzwyczajnych ważna jest jego najkorzystniejsza struktura, gwarantująca trwałość i niezawodność procesów informacyjnych. Wpływ na planowanie infrastruktury teleinformatycznej i kierowanie wywiera również wewnętrzna struktura oraz organizacja funkcjonowania stanowisk kierowania, ich mobilność oraz sprawność działania poszczególnych grup, zespołów organów kierowania i dowodzenia. System teleinformatyczny (łączności) podsystemu kierowania i dowodzenia powinien zawierać, najkorzystniejsze rozwiązania organizacyjno - techniczne i funkcjonalne.

W systemie obronnym państwa łączność występuje jako podstawowy środek kierowania państwem i dowodzenia siłami zbrojnymi. Podmiotem procesów kierowania są najwyższe organa kierownicze państwa, a ich bazę organizacyjno-techniczną stanowią stanowiska kierowania i dowodzenia wyposażone

pomiędzy organami stanowisk kierowania i dowodzenia[102]. Procesy innowacyjne należy rozpatrywać następująco:

- wewnętrzny obieg informacji, tj. pomiędzy stanem osobowym danego stanowiska kierowania i dowodzenia;
- zewnętrzny obieg informacji, tj. pomiędzy różnymi stanowiskami kierowania i dowodzenia, zachowaniem hierarchii w poszczególnych pionach funkcjonalnych i pomiędzy pionami.

Ze względu na różnorodność i ważność informacji dla realizowanych procesów kierowania i dowodzenia, każdy rodzaj przesyłanych wiadomości będzie posiadał adres uwzględniający priorytet szybkości obsługi oraz odpowiednią do klauzuli utajniania ochronę informacji.

Różnorodność zadań jakie spełnia system kierowania obronnością państwa w działaniach na obszarze kraju, manewrowy charakter przyszłych prowadzonych operacji, ciągłe zmiany i złożoność sytuacji, spowodują wzrost ilość informacji niezbędnej w procesie kierowania i dowodzenia, a przesyłanej za pośrednictwem systemu łączności. Przed tym systemem stawiane są także zadania w zakresie obiegu informacji, których spełnienie będzie decydować o powodzeniu prowadzonych działań czy operacji obronnych. Dlatego też w systemie teleinformatycznym (łączności) należy uwzględniać następujące problemy:

- dokonać analizy i ustalić jakie są wymagania podsystemu kierowania i dowodzenia w zakresie wymiany informacji, wynikające głównie z zakresu prac na określonych szczeblach zarządzania;
- uwzględnić prawdopodobieństwo ruchu generowanego przez osoby kierownicze oraz funkcyjne organów, zespołów kierowania i dowodzenia podsystemem kierowania obronnością państwa.

Parametrami systemu teleinformatycznego, który może zabezpieczyć przekazywanie informacji będą między innymi:

- ilość i rodzaj węzłów łączności w strukturze systemu teleinformatycznego spełniających ustalone wymagania ilościowe i jakościowe w zakresie przesyłanych informacji;

---

[102]Por. *Kierowanie obronnością państwa w stanach nadzwyczajnych, Praca studyjna,* Pod kier. nauk. M. Krauze, AON, Warszawa 2000, s. 188.

- zdolność przekazywania informacji z określoną mocą kryptograficzną;
- możliwość przesyłania sygnałów alarmowych oraz szybka łączność operacyjna w formie pisemnej z automatycznym jej zobrazowaniem i dokumentowaniem;
- współdziałanie z systemami różnych operatorów sieci telekomunikacyjnych;
- zapewnienie bezpośredniej, konferencyjnej i indywidualnej łączności między osobami funkcyjnymi;
- wymiana informacji opracowanej w planowanych systemach zautomatyzowanego wspomagania procesu kierowania i dowodzenia;
- możliwość kontroli i automatycznej rejestracji stanu eksploatowanych łączy.

Wymagania, które musi spełniać system telekomunikacyjny, to między innymi:

- świadczenie usług telekomunikacyjnych z żądanymi normami, sprawnością usługową;
- zapewnienie wiarygodności przekazywanych informacji to oznacza: wymaganego stopnia zgodności treści wiadomości odebranej z nadaną;
- zapewnienie wysokiej żywotności systemu;
- przesyłanie wiadomości według określonych priorytetów i stopni pilności;
- właściwa reakcja systemu na nierównomierność obciążenia ruchem;
- duża niezawodność wiązek łączy i węzłów komunikacyjnych;
- zapewnienie odpowiedniej szybkości transmisji, stosownie do potrzeb i oczekiwań użytkowników;
- możliwość utajniania informacji.

Ten sposób podejścia do uwarunkowań systemów łączności nie uwzględnia wszystkich, zwłaszcza celowych narażeń, którym może być poddany system łączności. Do najistotniejszych wymagań, jakie powinien spełniać system łączności

w techniczne środki wspomagania oraz zabezpieczenia kierowania (dowodzenia), sprzężone w spójny system za pomocą środków łączności.

Wymagania systemu kierowania obronnością państwa wobec telekomunikacji i informatyki w zakresie bezpieczeństwa państwa, a szczególnie poziomów gotowości obronnej są szczególne i dotyczą[103]:

- ☐ zapewnienia przekazywania terminowo, wiernie i skrycie informacji w wymaganych postaciach, w obiegu wewnętrznym i między strukturami organizacyjnymi;
- ☐ żądania pełnej gotowości systemu w każdej sytuacji kryzysowej w okresie pokoju, zagrożenia wojennego i wojny;
- ☐ bezpieczeństwa i ochrony systemu;
- ☐ szybkiej reakcji systemu;
- ☐ integracji rozwiązań;
- ☐ efektywności ekonomicznej rozwiązań.

Współczesny, a zwłaszcza perspektywiczny, system łączności cyfrowej powinien posiadać cechy, pozwalające spełnić szereg wymagań, między innymi:

a) w sferze organizacyjnej:

- wyprzedzająca gotowość łączności do działania w stosunku do systemu kierowania obronnością państwa i działania wojsk;
- wysoki poziom żywotności oraz stabilności systemu bez względu na powstałą sytuację bojową;
- gwarantowany poziom utajniania i bezpieczeństwa łączności;
- duża mobilność i elastyczność systemu.

b) w sferze technicznej:

- duża niezawodność i wierność transmisji danych;
- automatyczne uzyskanie połączeń bezpośrednich i obejściowych;
- możliwość zestawiania priorytetowych połączeń dalekosiężnych;
- odporność na zakłócenia radioelektroniczne;

---

[103]Por. *System kierowania obronnością państwa w stanach nadzwyczajnych w kontekście wykorzystania w nim środków i systemów łączności najnowszej generacji, Praca studyjna*, Pod kier. nauk. M. Krauze, AON, Warszawa 2003, s. 238.

najwyższym organom władzy i administracji państwa, jednostkom wojsk operacyjnych, obrony terytorialnej, obrony regionalnej itp., mieć zdolność zmiany konfiguracji oraz wydzielenie określonego podsystemu łączności zapewniającego kierowanie podczas zagrożeń (stanów nadzwyczajnych) i dowodzenie określonymi siłami przeznaczonymi do działania na wskazanym kierunku.

1.2.3. Wyznaczniki i mierniki charakteryzujące infrastrukturę telekomunikacyjną państwa

System łączności działa w niezwykle złożonych warunkach. Łączność powinna więc spełniać szereg kryteriów, do których należy zaliczyć wskaźniki jej oceny takie jak: terminowość, wierność i skrytość łączności, natomiast do kryteriów oceny systemu łączności należy zaliczyć: gotowość obronną, przepustowość, mobilność, trwałość (do której zalicza się: żywotność, odporność na zakłócenia i niezawodność) oraz bezpieczeństwo łączności[105]. System łączności bezpieczeństwa państwa realizowany jest głównie przy wykorzystaniu hierarchicznego i niehierarchicznego systemu łączności.

Specyfiką systemu jest konieczność tworzenia bezpośrednich relacji łączności (kanałów łączności) pomiędzy współpracującymi stanowiskami kierowania, a nawet i poszczególnymi miejscami pracy osób funkcyjnych. W efekcie tego może powstawać skomplikowana struktura połączeń, odzwierciedlająca, w sposób niemal wierny, hierarchiczny system kierowania obronnością państwa.

W strukturze hierarchicznej, na której opierał się analogowy (przestarzały) system łączności nie było możliwe spełnienie wymogów między innymi mobilności. Natomiast struktura niehierarchicznych systemów łączności oparta jest na dowolnej konfiguracji ich elementów. W strukturze tej zmiana dyslokacji lub przeznaczenia poszczególnych węzłów nie powoduje zmian w strukturze całego systemu. Zmiana funkcji węzła związana ze zmianą działania obsługiwanego przez nią stanowiska kierowania obronnością związana jest ze zmianą numeracji węzła i wykonywana jest bezzwłocznie. Prawdopodobieństwo terminowej zmiany

---

[105]Por. *Metody oceny systemów łączności na potrzeby obronności państwa pk. "WENA-1.* Praca naukowo-badawcza, pod. kier. nauk. M Krauze, AON, Warszawa 1998, s. 41.

w zakresie bezpieczeństwa państwa, należy zaliczyć między innymi[104]:

- wyprzedzającą gotowość w stosunku do systemu kierowania obronnością;
- dużą mobilność i elastyczność umożliwiającą zmianę struktury systemu;
- wysoki poziom żywotności i stabilności pracy bez względu na sytuację operacyjną;
- odporność na rozpoznanie i niszczenie przez przeciwnika;
- jednorodność wynikającą ze stosowania cyfrowych jednorodnych kanałów abonenckich;
- możliwość stosowania radiodostępu abonenckiego z zachowaniem jednorodności kanału;
- zapewnienie ciągłości utajniania w całym łańcuchu telekomunikacyjnym (nie wyłączając radiodostępu);
- możliwość stosowania systemu kryptograficznego umożliwiającego przekazywanie informacji o najwyższych klauzulach tajności;
- zdolność przekazywania informacji (w tym również transmisji danych) w czasie zbliżonym do rzeczywistego;
- możliwość stosowania automatycznego ruchu abonenckiego;
- możliwość realizacji cyfrowych zintegrowanych kanałów abonenckich umożliwiających naprzemienne przesyłanie sygnałów mowy i danych;
- zapewnienie priorytetowego dostępu najważniejszych abonentów do zasobów sieciowych;
- możliwość automatycznego poszukiwania abonenta w sieci, niezależnie od miejsca przebywania abonenta;
- możliwość stosowania systemów zarządzania zasobami transmisyjnymi i komutacyjnymi sieci;
- możliwość przekazywania informacji w trybie komutacji pakietów i kanałów.

Jest oczywistym, że organizowany na obszarze kraju system łączności kraju powinien spełniać te wymagania, aby móc świadczyć usługi telekomunikacyjne

---

[104]Tamże s. 243.

czas samego zestawiania połączenia nie odgrywa specjalnej roli.

Prawdopodobieństwo realizacji połączenia będzie więc zależeć nie tylko, jak w systemach analogowych, od wielkości wiązek łączy i natężenia ruchu w określonej relacji, lecz głównie od sposobu realizacji procedur poszukiwania drogi połączeniowej w sieci (realizacji routingów) i zakresu stosowania odpowiednich preferencji i ograniczeń ruchu. Zakłada się przy tym, że dla abonenta o największym priorytecie obsługi, poprawnie opracowany system powinien być zawsze zdolny do odszukania i zestawienia żądanego połączenia, z innym aktualnie istniejącym abonentem systemu.

Wierność łączności określa stopień zgodności informacji odebranej z informacją nadaną, przy istniejących liniach łączności, zakłóceniach i zniekształceniach. W odniesieniu do kanałów analogowych wierność definiowana była jako zrozumiałość logotomowa i jako prawdopodobieństwo skażenia znaku kombinacji kodowej w odniesieniu do kanałów teledacyjnych.

W systemach cyfrowych wskaźnik ten należy rozpatrywać dwuaspektowo w odniesieniu do kanału sygnalizacji międzycentralowej i w odniesieniu do transmisji sygnałów w kanale abonenckim. W pierwszym wypadku producent określa maksymalną jednostkową stopę błędów akceptowaną przez centrale, powyżej której kanał jest uznawany jako niesprawny i wyłączony z obsługi. Udostępnienie abonentom jednorodnego kanału cyfrowego tranzytowanego przez wiele węzłów komutacyjnych i zakończonego obustronnie przetwornikami analogowo - cyfrowymi powoduje, że jakość kanałów abonenckich zależy od jednostkowej stopy błędów poszczególnych traktów cyfrowych. Wpływ wartości elementarnej stopy błędów na jakość kanału fonicznego jest ściśle określony i zależny od stosowanej metody kodowania mowy.

Jak wynika z badań, modulacja delta jest najbardziej odporna na zakłócenia występujące w kanale transmisyjnym. W wypadku transmisji danych w kanałach cyfrowych stosowane procedury kontrolne czy też kody korekcyjne, uzależniają jej jakość od elementowej stopy błędów. W systemach cyfrowych istnieje możliwość kontroli stanu traktów transmisyjnych a w razie ich uszkodzeń, zdalnego ich eliminowania.

konfiguracji struktury połączonej ze zmianą dyslokacji końcowego mobilnego węzła łączności, z uwagi na małą liczbę realizowanych relacji i praktycznie brak procedur alokacji w systemie jest bardzo wysokie.

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

Tworzenie wydzielonych systemów nie pozwalało na prowadzenie racjonalnej polityki wykorzystywania posiadanego potencjału, zwłaszcza w jego warstwie transmisyjnej i to transmisji międzywęzłowej. Dopiero zastosowanie urządzeń techniki cyfrowej umożliwiło realizację określonych celów i zadań w tym zakresie. Wszystko to wymusiło stworzenie specyficznych wskaźników oceny systemu telekomunikacyjnego. Wskaźniki te, w pełni odzwierciedlają specyfikę i charakter systemu łączności państwa, tworząc kompletny opis jego podstawowych parametrów[106].

Terminowość łączności - zdolność do przekazywania i dostarczania informacji oraz prowadzenia bezpośrednich rozmów w określonym czasie. W systemach analogowych terminowość była definiowana generalnie, jako prawdopodobieństwo zestawienia połączenia w określonym czasie. Dla systemów łączności w pełni cyfrowych, opartych głównie na bezobsługowych urządzeniach komutacyjnych oraz stosowaniu węzłów tranzytujących ruch i dużych wiązek łączy transmisyjnych, pojęcie terminowości utożsamia się z prawdopodobieństwem odnalezienia drogi, po której zostanie zestawione żądane połączenie, przy czym

---

[106]Tamże, s. 58.

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

Przepustowość systemu łączności charakteryzuje potencjalną możliwość sieci w przekazywaniu ilości informacji w jednostce czasu. Powinna ona odpowiadać potrzebom kierowania i dowodzenia w tym zakresie. Można ją określać dla każdego kierunku łączności, odcinka lub całości systemu łączności.

W cyfrowych systemach łączności zdolność przepustowa jest określana jako przepływność cyfrowych strumieni grupowych łączących poszczególne węzły komutacyjne sieci. Wartość ta, w skali lokalnej, również określa liczbę bezpośrednich kanałów łączności. w skali makro, czyli całego systemu, wielkość ta jest jedynie elementem pomocniczym umożliwiającym ocenę zdolności przepustowej całego systemu.

Automatyczna komutacja połączeń oparta na dynamicznym wyznaczaniu dróg połączeniowych umożliwia praktycznie wykorzystywanie całego potencjału sieci czyli wszystkich dostępnych dróg połączeniowych.

Trwałość systemu łączności określana jest jej zdolnością do pracy przy oddziaływaniu na niego wszystkich czynników rażenia przeciwnika, czy innych narażeń, związanych z klęskami żywiołowymi, kataklizmami i atakami terrorystycznymi, wyraża się żywotnością, odpornością na zakłócenia oraz niezawodnością środków i elementów sieci[107].

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

---

[107]Tamże, s. 62.

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

W cyfrowych systemach łączności stosuje się najczęściej obligatoryjne utajnianie wszystkich międzycentralowych kanałów grupowych jako pierwszy stopień utajniania. Jako drugi stopień utajniania stosuje się, dodatkowo dla wybranych abonentów, indywidualne systemy utajniania typu punkt - punkt, instalowane bezpośrednio u użytkowników. Miarą skrytości systemu będzie więc głównie nie współczynnik utajniania kanałów a wprost skuteczność urządzeń utajniających definiowana jako ich moc kryptograficzna.

Skrytość w rozumieniu prawdopodobieństwa wykrycia obiektu, np. węzła komutacyjnego, z uwagi na niehierarchiczność struktury oraz stosowanie kratowej struktury powiązań węzłów, miniaturyzację urządzeń i zmniejszenie liczby samodzielnych elementów, uległa znacznemu przewartościowaniu. Zapewnienie odpowiednio niskiego prawdopodobieństwa wykrycia w odpowiednim czasie węzła cyfrowego jest dużo łatwiejsze niż w wypadku analogicznego węzła analogowego. Niehierachiczność struktury systemu spowodowała dodatkowo zmniejszenie roli poszczególnych węzłów w systemie, a więc i zminimalizowanie negatywnych skutków ich uszkodzenia (eliminacji).

Gotowość obronna systemu łączności jest to zdolność do terminowego przejścia z danego stanu w inny, niezbędny do zapewnienia kierowania systemem obronności. Powinna ona wyprzedzać gotowość obronną samego systemu obronności państwa. Nowoczesny stacjonarny cyfrowy system łączności, będący w stałej gotowości obronnej jest dostosowany, z przyczyn ekonomicznych, do realizacji z określonym prawdopodobieństwem ruchu abonenckiego, mierzonego np. w erlangach. Zwiększenie stanu gotowości obronnej systemu będzie związane głównie z jego rozbudową spowodowaną:

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

fałszywej informacji. Jest ono określane przez odporność na rozpoznanie oraz niedostępność elementów systemu łączności (niedostępność do informacji przesyłanych w systemie).

Osiąga się ją poprzez terminową realizację przedsięwzięć organizacyjnych i technicznych polegających głównie na fizycznej ochronie elementów i środków łączności, ograniczaniu poziomu elektromagnetycznej emisji ujawniającej i szyfrowaniu przesyłanych informacji[109].

W systemach niehierarchicznych struktura systemu jest praktycznie skryta. Drogi połączeniowe są zapisane w tablicach routingów procesorów sygnalizacyjnych poszczególnych węzłów komutacyjnych. Wiadomości te są fragmentaryczne i nie informują o strukturze całego systemu. Dodatkowo, najczęściej w sposób obligatoryjny dokonuje się utajniania wszystkich traktów grupowych, co uniemożliwia włączenie się do systemu osób postronnych.

Wskaźniki te przyjmowane w sposób obligatoryjny były weryfikowane za pomocą symulacji modeli komputerowych oraz przez praktyczną realizację, podczas badań określających specyficzne cechy systemu[110]. Do wskaźników tych należy zaliczyć:

- prognozowanie ruchu;
- wybór stosowanej metody kodowania mowy;
- ustanowienie gradacji abonentów w postaci odpowiednich priorytetów realizacji połączeń;
- wprowadzenie limitowanego dostępu abonentów do sieci;
- ograniczenie czasu trwania niektórych połączeń;
- określenie procedur zestawiania połączeń (algorytmu komutacji poszukiwania abonentów w sieci);
- algorytm szyfrowania sygnałów.

Jak wcześniej wspomniano, efektem właściwego doboru wymienionych wskaźników jest możliwość wykorzystania przez abonentów, przy realizacji połączeń, całego dostępnego im potencjału komutacyjnego i transmisyjnego sieci.

---

[109]Por. W Gawlikowski, *Zagrożenia systemu telekomunikacyjnego w czasie pokoju, kryzysu i wojny*, w: „Zeszyty Naukowe AON", 1997 nr 3, s.34.

[110]Por. *Metodyka badania Krajowego Systemu Łączności KSŁ-P.* Praca naukowo-badawcza, pod. kier. nauk. M. Krauze, AON, Warszawa 1996 s. 63.

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

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

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

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

Struktura niehierarchicznych cyfrowych systemów łączności oparta jest na systemie o dowolnej konfiguracji jego elementów tworzących nieregularną siatkę[108]. W strukturze tej zmiana dyslokacji lub przeznaczenia poszczególnych węzłów nie powoduje zmian w strukturze całego systemu. Zmiana funkcji węzła związana ze zmianą funkcji obsługiwanego przez nią stanowiska kierowania obronnością związana jest ze zmianą numeracji węzła i wykonywana jest bezzwłocznie.

Prawdopodobieństwo terminowej zmiany konfiguracji struktury połączonej ze zmianą dyslokacji końcowego mobilnego węzła łączności, jak wcześniej wspomniano, z uwagi na małą liczbę realizowanych relacji i praktycznie brak procedur alokacji w systemie jest bardzo wysokie.

Bezpieczeństwo systemu łączności jest to zdolność przeciwstawienia się wszystkim rodzajom rozpoznania przeciwnika oraz próbom wprowadzenia

---

[108]Tamże, s. 67.

(łączności radiowej i radiofonicznej, radiofonii oraz telewizji), a także naziemne stacje łączności satelitarnej. W istniejącej sieci telekomunikacyjnej można wyróżnić linie łączności przebiegające ze wschodu na zachód i rokady biegnące z północy na południe. W punktach przecięcia tych linii znajdują się stacje wzmacniakowe bądź teletransmisyjne.

Obecny stan telekomunikacji jest niezadowalający zarówno pod względem ilościowym, jak i jakościowym czego dowodem jest niewłaściwa struktura organizacyjna przez zagęszczenia i rozrzedzenia linii telekomunikacyjnych w różnych regionach kraju, mała skuteczność ochrony i obrony przed zagrożeniami, szczególnie przed rozpoznaniem i obezwładnianiem a zwłaszcza radioelektronicznym, duża różnorodność stosowanych technik i technologii telekomunikacyjnych[111]. Obieg informacji oparty jest na sprzęcie, pochodzącym przede wszystkim z importu. Sieci łączności niektórych resortów i instytucji funkcjonują na podstawie różnych rozwiązań technicznych.

Przez to eksploatowany system łączności jest mało spójny i podzielony na zbyt wiele podsystemów resortowych. Nie zapewnia to wymaganej koordynacji i kompatybilności systemowej. Stwarza znaczne utrudnienia w przekazywaniu informacji i naraża na niebezpieczeństwo utraty informacji jak również powoduje duże niedogodności w organizowaniu łączności na potrzeby obronności i zapewnieniu bezpieczeństwa państwa.

W miarę rozwoju infrastruktury telekomunikacyjnej sieci stają się coraz większe, wprowadza się do nich nowe techniki i korzysta coraz więcej użytkowników. W związku z tym zmieniają się również, wymagania dotyczące tych sieci, z których najważniejszymi są: dostępność w każdym miejscu, szybkość transmisji, niska cena, bezpieczeństwo oraz niezawodność. W związku z tym, że sieć jest strukturą złożoną, jej niezawodność jest zależna od niezawodności jej elementów składowych. Sieci telekomunikacyjne często ulegają uszkodzeniom i nie spełniają wymaganych funkcji w danych warunkach, w danej chwili lub w danym przedziale czasu.

---

[111]Tamże, s. 65.

Jednocześnie, przy wystąpieniu rozległych uszkodzeń struktur, jest zagwarantowana możliwość realizacji połączeń dla najważniejszych abonentów systemu.

1.3. Infrastruktura telekomunikacyjna, a bezpieczeństwo ekonomiczne państwa

1.3.1. Niedoskonałości infrastruktury telekomunikacyjnej, a zagrożenie bezpieczeństwa ekonomicznego państwa

Wzrost ilości informacji we wszystkich obszarach i płaszczyznach ludzkiej działalności spowodował, że stanowi ona obok materii i energii trzeci element otaczającej nas rzeczywistości. Istota kierowania państwem, dowodzenia siłami zbrojnymi i zarządzanie gospodarką narodową, jak też organizacja bytu społecznego polega na sprawnym przesyłaniu informacji (wiadomości) na odległość za pomocą różnych systemów łączności. Wysoka jakość łączności jest podstawowym, a wręcz koniecznym warunkiem sprawnego kierowania i zarządzania państwem, w celu efektywnego wykorzystania potencjału gospodarczego, kulturalnego, naukowego do zapewnienia do dalszego rozwoju kraju, a tym samym zapewnienia godziwego bytu społeczeństwa.

Przyjęcie strategii obronnej i usprawnienie systemu obronności państwa, stwarza sprzyjające warunki przygotowania zawczasu na obszarze kraju środków i urządzeń telekomunikacyjnych do zapewnienia trwałej, niezawodnej oraz wiarygodnej łączności. Łączność na terytorium kraju zapewnia system łączności państwa. Jego potencjał powinien zaspokajać potrzeby i wymagania wszystkich organów kierowniczych państwa i administracji publicznej oraz całego systemu obronności kraju w sytuacjach szczególnych zagrożeń. Jak powszechnie wiadomo, składa się on z sieci telekomunikacyjnej użytku publicznego, sieci niezależnych operatorów i sieci resortowych (np. MON, MSWiA, MI i innych) oraz zakładowych, a także poczty.

Sieć telekomunikacyjną tworzą: obiekty i linie telekomunikacyjne (kablowe, światłowodowe, radiowe, a nawet jeszcze napowietrzne) obiekty teletransmisyjne (stacje wzmacniakowe, przełączalnie) i radiokomunikacyjne

Sieci telekomunikacyjne są budowane do różnych zastosowań: dla tradycyjnej sieci PSTN, ogólnoświatowej sieci teleinformatycznej Internet, do łączenia sieci korporacyjnych LAN, transmisji sygnałów multimedialnych, np. DVB, oraz dla sieci telefonii komórkowej, np. UMTS, mającej charakter sieci pakietowej. W ubiegłym roku kilku dużych operatorów telekomunikacyjnych stwierdziło, że ruch związany z transmisją danych w sieciach pakietowych (teleinformatycznych) jest większy od ruchu pochodzącego z komutacji kanałów w sieci PSTN. Ruch pochodzący z sieci PSTN prawie się nie zmienia, natomiast ruch pakietowy wykazuje dużą dynamikę przyrostu - rzędu 50% rocznie. Stąd przy budowie lub modernizacji sieci telekomunikacyjnych dominującym problemem jest uwzględnianie teleinformatyki[112].

Rozwój systemów i sieci teleinformatycznych nie jest traktowany jako moda. Analizy rozwoju wskazują na ścisłą zależność pomiędzy parametrami rozwoju gospodarczego państwa z rozwojem systemów informacyjnych, a zatem i systemów teleinformatycznych, przy czym wskaźniki rozwoju teleinformatyki rosną znacznie szybciej od wskaźników rozwoju gospodarczego. Dlatego warto jednak pamiętać o uwarunkowaniach ekonomicznych. Inwestycje telekomunikacyjne są z reguły bardzo kosztowne i wymagają takiego zaplanowania, aby przez jakościowe i ilościowe ich dopasowanie do potrzeb były na każdym etapie ekonomicznie efektywne.

Kolejne przedsięwzięcia w rozbudowie powszechnej sieci teleinformatycznej powinny być tak planowane w obszarze telekomunikacji, aby obniżać cenę własną usług i pozwalać na gromadzenie funduszu na przedsięwzięcia następne. Jednym z najistotniejszych czynników kosztu systemu jest między innymi: efektywność wykorzystania przepustowości kanałów transmisyjnych, stopień rozbudowy systemu teletransmisyjnego, liczba łączy w danej relacji itp.

Zysk na efektywności uzyskany z poprawy metod gospodarowania zasobami sieci pozwala na wzbogacanie metod, przy równoległym, umożliwiającym ich wprowadzanie, rozwoju ilościowym. Podobne efekty gospodarowania zasobami systemów przynosi także, jego sieciowa architektura.

---

[112]Zob. *System kierowania obronnością...*wyd. cyt., s. 171.

Główne czynniki powodujące niezdatność w sieci telekomunikacyjnej oraz ich parametry niezawodnościowe to:

- sprzęt łączności;
- oprogramowanie komputerów i sieci;
- wpływ szczególnych zagrożeń i środowiska;
- błędy personelu obsługującego sieć.

Zapobieganie niedoskonałościom sieci telekomunikacyjnych kraju i poprawę ich infrastruktury powinny obejmować przedsięwzięcia o charakterze: organizacyjnym, inwestycyjnym i technicznym w sieci telekomunikacyjnej nie tylko użytku publicznego, ale również w sieciach operatorów niezależnych. System telekomunikacyjny powinien być rozbudowywany stosownie do potrzeb wynikających z planów obronności państwa.

Wykorzystywane w okresie zagrożeń bezpieczeństwa systemy łączności są projektowane już w czasie pokoju a następnie modyfikowane zgodnie ze stosownymi planami. Uczestnictwo Polski w NATO i UE wymusza konieczność ścisłego współdziałania z krajami Europy mającego na celu stworzenie jasnych i kompetentnych struktur w zakresie organizacji współpracy w dziedzinie telekomunikacji.

1.3.2. Wpływ rozwoju infrastruktury telekomunikacyjnej na stan bezpieczeństwa państwa

Jak już uprzednio podano, telekomunikacja to przesyłanie informacji (wiadomości i transmisji danych) na odległość za pomocą sygnałów elektrycznych. Informatyka to dziedzina wiedzy o przetwarzaniu i przechowywaniu informacji. Jest przy tym rzeczą charakterystyczną, że ze wzrostem stopnia komputeryzacji znaczenie telekomunikacji wzrasta, ponieważ komputery muszą się ze sobą komunikować poprzez łącza telekomunikacyjne. Ogólnie mówi się o połączeniu telekomunikacji z informatyką w teleinformatykę. Proces łączący te dziedziny przebiega w sposób dość złożony, w różnych krajach nie jednakowo. Różnice dotyczą zarówno metod, jak i czasu występowania poszczególnych etapów. Proces ten nie jest zakończony, stąd też brak jednoznacznej i praktycznej interpretacji terminu teleinformatyka.

telekomunikacja, nie tylko ułatwia zarządzanie państwem, ale jest siłą napędową rozwoju gospodarczego i staje się jednym z podstawowych elementów bezpieczeństwa ekonomicznego państwa[113].

Niezbędnym warunkiem rozwoju teleinformatyki jest równomierny wzajemnie dopasowany ilościowo i jakościowo rozwój telekomunikacji i informatyki, każde zakłócenie hamuje ten rozwój. Niemal jest regułą, że telekomunikacja we wszystkich krajach znajduje się pod państwową administracją łączności.

W przyszłości, gdy metody, zarządzania komputerowego staną się dominujące, posiadanie dobrze rozwiniętej telekomunikacji będzie warunkować zarządzanie państwem. Wymiana bieżących informacji politycznych, gospodarczych, handlowych, kulturalnych i naukowych przyczynia się do lepszego porozumienia, współpracy społeczeństw i narodów, a tym samym wzmaga i stymuluje proces rozwoju infrastruktury telekomunikacyjnej.

1.3.3. Wpływ stanu bezpieczeństwa ekonomicznego na kształtowanie i rozwój infrastruktury telekomunikacyjnej

Nowoczesne społeczeństwo informacyjne jest coraz bardziej uzależnione od zastosowań systemów telekomunikacyjnych i informatycznych. Stąd też jednym z głównych problemów bezpieczeństwa ekonomicznego państwa jest zbudowanie odpowiedniego potencjału teleinformatycznego na poziomie krajowym i międzynarodowym, zapewniającego ciągłość działania infrastruktury telekomunikacyjnej na rzecz wsparcia najważniejszych funkcji społeczeństwa oraz stworzenie możliwości wykorzystania jej w czasie sytuacji kryzysowych i wojny.

System telekomunikacyjny do realizacji połączeń w sieci powinien być maksymalnie odporny na oddziaływania zewnętrzne, zapewniać alternatywny wybór tras, różnorodną dystrybucję kanałów. Każdy kraj będzie chciał sprawować pewnego rodzaju kontrolę nad połączeniami przychodzącymi z zewnątrz do jego sieci, poprzez połączenia automatyczne i półautomatyczne. Poszczególne ogniwa gospodarczo-obronne już w czasie pokoju, a przede wszystkim podczas zagrożeń bezpieczeństwa państwa są zobowiązane do realizacji następujących zadań:

---

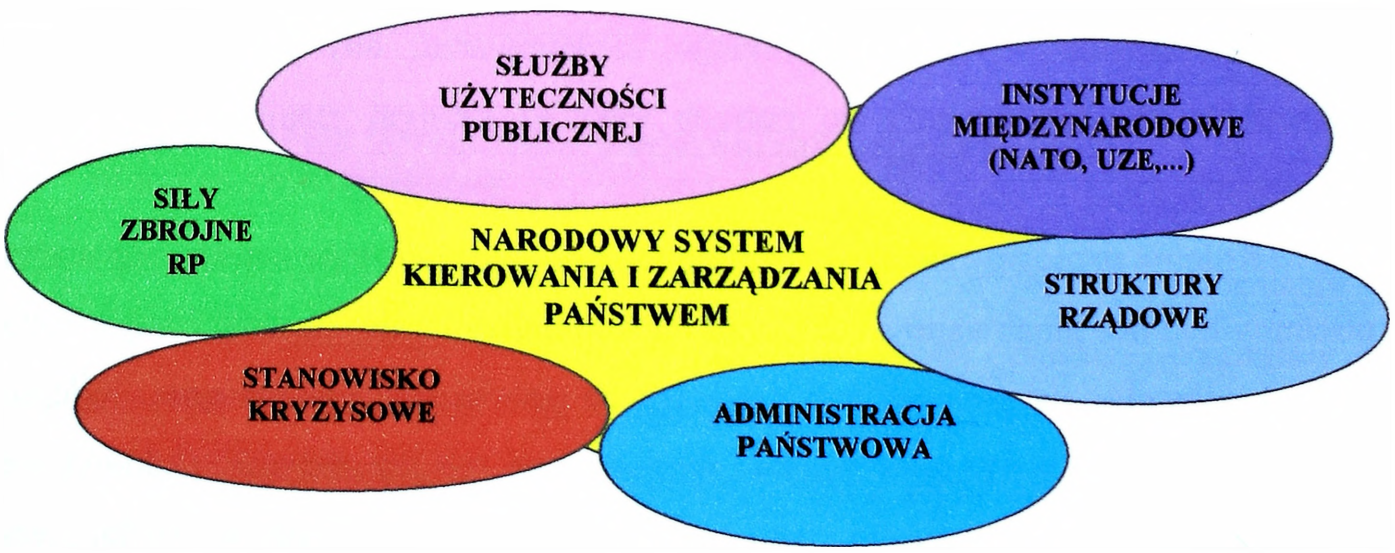
[113]Por. T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo*...wyd. cyt., s. 39.

Pomimo rozwoju niezawodnych metod i systemów techniki cyfrowej, światłowodowej, komutacji wiadomości z zastosowaniem komputerów, różnych metod i urządzeń kodowania, zwiększonej sprawności, tajności i możliwości obsługi ruchu, wdrażanie nowoczesnych, zintegrowanych i szerokopasmowych systemów informacyjnych na potrzeby kierowania obronnością państwa odbywa się powoli. Obok różnych aspektów, decydującym jest aspekt ekonomiczny. Można śmiało stwierdzić, że w miarę upływu czasu koszty znacznie zmalały i będą dalej obniżać się.

Kierowanie i zarządzanie państwem odbywa się w układzie organizacyjno - funkcjonalnym obejmującym: organa władzy, administrację rządową i samorządową z ich ustawowymi kompetencjami, jak również infrastrukturę gospodarczą - współużytkowników systemu teleinformatycznego (Schemat 1.13.).

Schemat 1.13.

Współużytkownicy systemu teleinformatycznego



Źródło: Opracowanie własne.

Instytucje rządowe i administracji państwowej, gospodarka, przemysł, mieszkania obywateli są połączone w celu przekazywania informacji słownych, danych i obrazów. Odbywa się rozpowszechnianie informacji do wszystkich form w postaci dźwiękowej, transmisji danych i wizualnej. Obecnie, dobrze rozwinięta

- opracować zasady rozpływu ruchu z uwzględnieniem właściwości elementów komutacyjnych i posiadanych zasobów sieci;
- zaprojektować dopuszczalną strukturę sieci z uwzględnieniem zweryfikowanych wymagań, rozpływu ruchu i wskaźnika jakości obsługi;
- w zbiorze dopuszczalnych struktur przeprowadzić badania analityczne niezawodności, trwałości i przepustowości, a na tej podstawie określić suboptymalną strukturę obiektu docelowego.

System bezpieczeństwa państwa powinien posiadać dobrze przygotowany personel, organy (zespoły) zorganizowane w odpowiednie struktury, procedury zarządzania i mechanizmy na potrzeby działania i odtwarzania swoich sieci, jak również usług w sytuacjach szczególnych zagrożeń. Wykorzystanie infrastruktury telekomunikacyjnej do świadczenia usług na rzecz bezpieczeństwa państwa wymaga określenia:

- stanu istniejącego pod kątem przydatności na potrzeby sytuacji szczególnych zagrożeń, kryzysu i wojny;
- koordynacji i opracowania w czasie pokoju sposobu wykorzystania sił i środków w celu zapewnienia ciągłości świadczenia usług telekomunikacyjnych w czasie kryzysu i wojny, zarówno na potrzeby militarne, jak i cywilne.

Większość krajów w zakresie kierowania obronnością dysponuje połączeniami telekomunikacyjnymi pomiędzy władzami rządowymi, wojskowymi i cywilnymi, a ważnymi użytkownikami przy wykorzystaniu publicznej sieci telekomunikacyjnej. Połączenia te, traktowane jako podstawowe, są niezbędne w celu zwiększenia ilości połączeń w sytuacji, gdy usługi telekomunikacyjne będą ograniczone z uwagi na uszkodzenia, zatory lub usterki. Ponadto dysponują krajowymi planami preferencji, które umożliwiają funkcjonowanie tego istotnego ruchu krajowego.

Jednakże sprawą znaczącej wagi dla NATO jest wsparcie krajów członkowskich w czasie kryzysu, co wiąże się z zapewnieniem interoperacyjności umożliwiającej łączność pomiędzy ważnymi użytkownikami w jednym kraju, a jego korespondentami w innym.

- utrzymywanie zabezpieczenia materiałowo-technicznego stacji i obiektów telekomunikacyjnych, traktów i łącz dzierżawionych;
- przygotowanie zmilitaryzowanych jednostek przeznaczonych do odtwarzania w toku działań bojowych, naruszonego systemu telekomunikacyjnego;
- utrzymywanie adaptacyjnego i spójnego systemu telekomunikacyjnego;
- świadczenie usług telekomunikacyjnych i pocztowych na potrzeby poszczególnych szczebli kierowania i zarządzania państwem;
- planowanie, gromadzenie i utrzymywanie rezerw państwowych, gospodarczych i specjalistycznych.

Niezbędnym i jednym z najważniejszych zadań w ramach przygotowań obronnych w telekomunikacji jest systematyczne szkolenie i uczestnictwo władz krajowych, odpowiedzialnych za telekomunikację, operatorów, jednostek remontowo - budowlanych, dostawców usług i producentów sprzętu w ćwiczeniach krajowych i międzynarodowych. W celu lepszego przystosowania systemu telekomunikacyjnego do spełnienia zadań i wymagań systemu kierowania i zarządzania państwem należałoby dążyć do zapewnienia[114]:

- bezpieczeństwa przekazywanych informacji;
- dostępu radiowego dla abonentów będących w ruchu;
- możliwości łączenia między sobą abonentów, węzłów lub podwęzłów za pośrednictwem łączy satelitarnych;

Aby system telekomunikacyjny mógł realizować określone zadania i cele wskazane jest wykonanie następujących czynności:

- zweryfikować zbiór użytkowników i ruch przez nich generowany (postacie wiadomości, ich priorytety, potrzeby w zakresie bezpieczeństwa informacji itp.);
- zweryfikować i uzupełnić wymagania techniczne na obiekty;
- ustalić zasoby, które mogą być wykorzystywane z sieci TP S.A i innych operatorów;

---

[114]Zob. *System kierowania obronnością*...wyd. cyt., s. 126.

2. ANALIZA STANU INFRASTRUKTURY TELEKOMUNIKACYJNEJ I JEJ WPŁYW NA KSZTAŁTOWANIE BEZPIECZEŃSTWA EKONOMICZNEGO W POLSCE NA PRZEŁOMIE XX I XXI WIEKU

2.1. Analiza i ocena stanu infrastruktury telekomunikacyjnej i uwarunkowania jej kształtowania

2.1.1. Analiza rodzajowa infrastruktury telekomunikacyjnej

Współczesna telekomunikacja ma za zadanie zapewnić możliwość niezawodnego porozumiewania się ludzi i urządzeń np. komputerów w każdych warunkach, bez względu na miejsce, w którym się znajdują np.: na lądzie, morzu, powietrzu, kosmosie i bez względu na to, czy są w ruchu, czy w stanie spoczynku. Szczególnie wymagania w tym zakresie są stawiane przed telekomunikacją na potrzeby bezpieczeństwa państwa. Możliwości wprowadzanych nowych technik i technologii stworzyły warunki i umożliwiły gwałtowny rozwój w dziedzinach:

- telekomunikacji – objawiających się wprowadzaniem nowych sieci telekomunikacyjnych wykorzystujących najnowsze technologie komutacji i transmisji, umożliwiających efektywne wykorzystanie dostępnych pasm częstotliwości (przez dowolne media transmisyjne: kablowe, światłowodowe, radiowe, satelitarne itp.) oraz zapewniających większe bezpieczeństwo wymiany informacji;
- informatyki - objawiający się ciągłą miniaturyzacją oraz zwiększaniem mocy obliczeniowych komputerów, unifikacją sprzętu komputerowego i peryferyjnego – pozwalającą wykorzystywać również na potrzeby sił zbrojnych sprzętu komercyjnego i coraz bardziej złożonego oprogramowania.

Użytkownicy sieci telekomunikacyjnych oczekują możliwości realizacji wielu różnorodnych usług w sposób możliwie najprostszy, niezawodny i tani. Przekaz głosowy, usługi telegramowe i teleksowe w systemie analogowym przez dziesiątki lat były podstawą komunikowania się między ludźmi, istotne zmiany zaszły w telekomunikacji po opanowaniu techniki cyfrowej, a przede wszystkim po włączeniu do sieci telekomunikacyjnej elementów pochodzących z technologii komputerowych. Ideałem, do którego dążą aktualne rozwiązania jest powszechna sieć cyfrowa, która zapewnia świadczenie wielu usług telekomunikacyjnych np.: klasycznych, usług ISDN, przenoszenia, multimedialnych i innych, dostępnych dla

Większość istniejących krajowych programów preferencji cywilnych przeznaczona jest do uruchomienia w sytuacjach szczególnych zagrożeń. Mogą jednak mieć miejsce sytuacje, gdy zaistnieje potrzeba uruchomienia międzynarodowego programu preferencji w kraju, w którym wydaje się być to zbędne. Przykładem tego może być sytuacja, gdy tworzy się intensywny ruch międzynarodowy do odległego kraju znajdującego się w stanie kryzysu. Stąd międzynarodowe i krajowe programy powinny być kompatybilne.

- pocztę elektroniczną (dokumentalną i głosową);
- szybką transmisję danych (np. transmisję danych pomiędzy sieciami LAN) umożliwiającą wymianę dużych plików;
- łatwy, a jednocześnie bezpieczny dostęp do baz danych;
- przesyłanie sygnałów wideo (o bardzo różnorodnych zastosowaniach i parametrach) oraz możliwość ich realizacji;
- inne usługi multimedialne, np. jednoczesna wymiana danych i obrazów;
- dystrybucja różnorodnych informacji (np.: rozpoznawczych, meteorologicznych itp.).

Z dokonanej analizy rozwoju sieci w ubiegłych latach można stwierdzić, że istniejąca infrastruktura telekomunikacyjna nie jest w stanie zapewnić wszystkich możliwych, przedstawionych na schemacie, usług telekomunikacyjnych oraz coraz bardziej wielorakich wymagań użytkowników. Jak wynika z podziału telekomunikacji dokonanego w poprzednim rozdziale infrastruktura telekomunikacyjna obejmuje zasadniczo dwie przenikające się struktury komunikacyjne:

- □ sieci telekomunikacyjne o warstwowej strukturze komutacji na wyższym poziomie transportowym PDH, SDH, ATM, DTM[114], z cyfrowymi systemami komutacji, ale także analogowymi centralami telefonicznymi i cyfrowymi centralami abonenckimi wraz z różnorodnymi sieciami telekomunikacyjnymi dostępu abonenckiego np.: linie telefoniczne, tory światłowodowe, kanały cyfrowe ISDN, kanały telewizji kablowej CATV[115] oraz z bezprzewodowymi sieciami radiowymi dostępu abonenckiego funkcjonującymi jako sieci teledacyjne, przywoławcze i komórkowe np.: NMT[116], GSM[117], jak też z systemami komunikacji i nawigacji globalnej np.: VSAT[118], GPS[119], i inne;

---

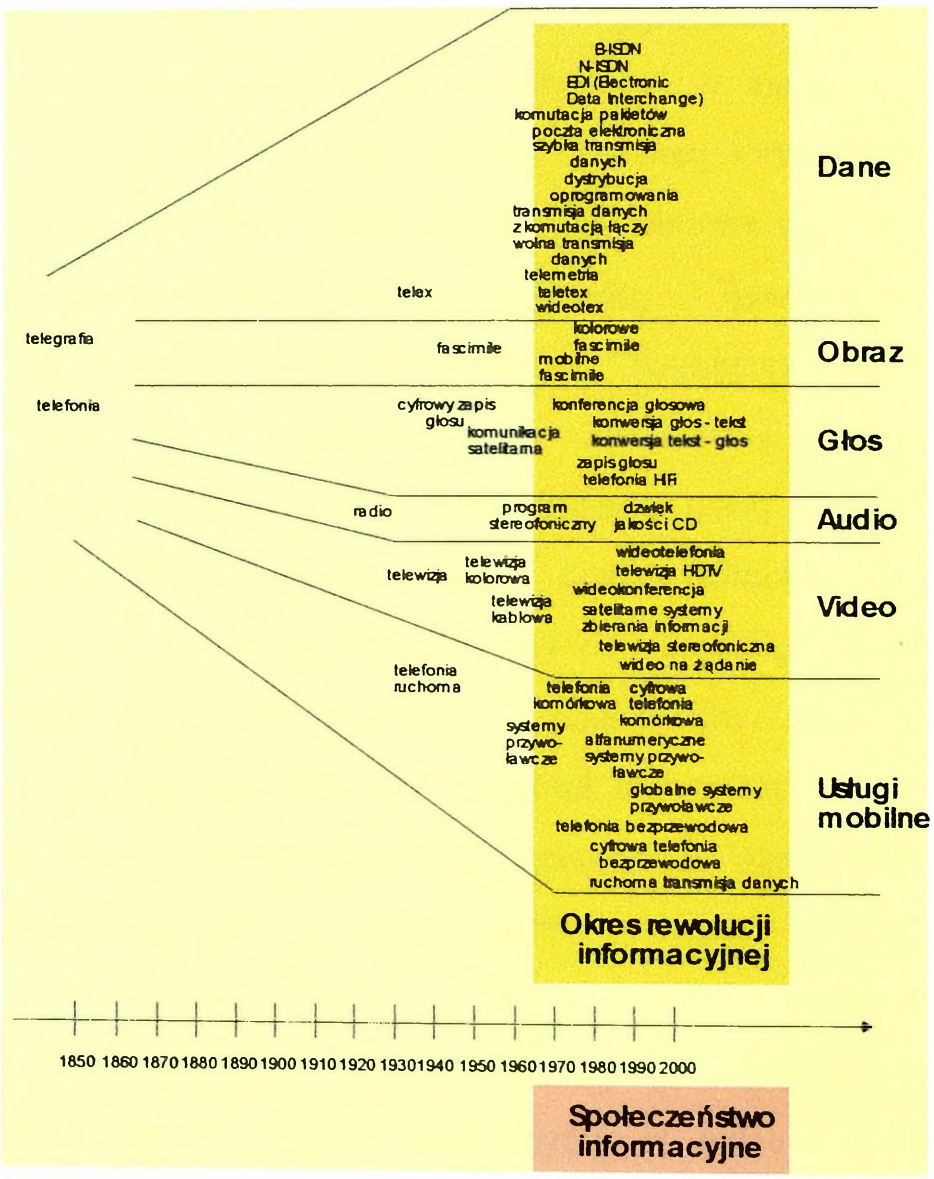
[114]DTM – ang. Dynamic Synchronous Transfer Mode – technologia dynamicznie i dyskretnie skalowanej transmisji o wysokiej przepływności od 512kb/s do 2,5 Gb/s, z przeznaczeniem do transportu przekazów cyfrowych działających w czasie rzeczywistym. Konkurencyjna technologia dla ATM.
[115]CATV - ang. Cable Television - telewizja kablowa.
[116]NMT – ang. Nordic Mobile Telephony - analogowa sieć telefonii komórkowej.
[117]GSM – ang. Global System for Mobile Communication - cyfrowa sieć telefonii komórkowej.
[118]VSAT – ang. Very Smsll Aperture Terminal – Małe stacje terminalowe z antenami parabolicznymi korzystające z kanałów satelitarnych w pasmie 11/12//14 GHz lub 4/6 GHz.
[119]GPS – ang. Global Positioning System – światowy system nawigacji satelitarnej.

dowolnego użytkownika poprzez pojedyncze urządzenie końcowe - terminal.

Realizacja tej idei stała się w dużej części możliwa po wdrożeniu w latach osiemdziesiątych w wielu państwach świata, zarówno w systemach publicznych, jak i w systemach specjalnych (wojskowych), sieci cyfrowych z możliwościami świadczenia szerokiego spektrum usług (Schemat 2.1.).

Schemat 2.1.

Rozwój usług telekomunikacyjnych



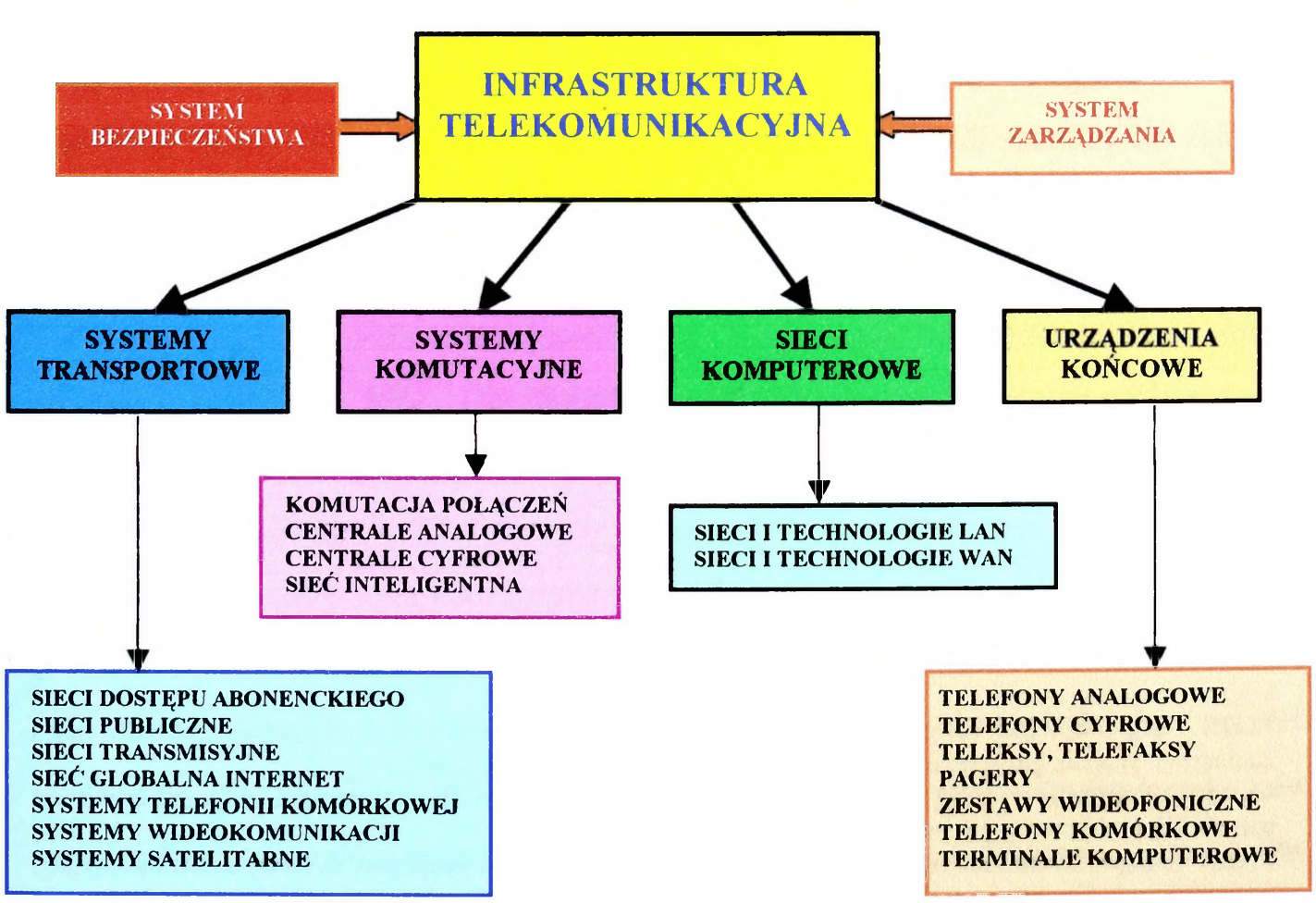
Źródło: Opracowanie własne na podstawie: *Koncepcja wykorzystania technicznych środków łączności najnowszej generacji w systemie łączności na potrzeby sytuacji kryzysowych.* Praca naukowo-badawcza pod kier. nauk. M. Krauze, AON, Warszawa 2000.

Budowa społeczeństwa informacyjnego spowodowała powszechną komputeryzację urzędów administracji państwa, placówek oświaty i szkolnictwa, różnych instytucji publicznych i wojskowych, firm, przedsiębiorstw i innych, przez co nastąpił gwałtowny wzrost zapotrzebowania na nowe usługi telekomunikacyjne umożliwiające między innymi:

3. **Sieci komputerowe:**
   a) sieci LAN;
   b) sieci WAN;
   c) technologie sieci lokalnych;
   d) technologie sieci rozległych.
4. **Urządzenia końcowe:**
   a) telefony analogowe i cyfrowe;
   b) teleksy;
   c) telefaksy;
   d) pagery;
   e) zestawy wideofoniczne;
   f) telefony komórkowe;
   g) terminale.

Schemat 2.2.

Infrastruktura telekomunikacyjna kraju



Źródło: Opracowanie własne na podstawie: *Net World Vademecum teleinformatyka cz. 1, 2, 3*, International Data Group Poland S.A., Warszawa 2004.

- cyfrowe sieci komputerowe oparte na strukturach sieciowych typu LAN, MAN, WAN, tworząc sieci komunikacyjne, które są łączone za pomocą węzłów: mosty[120], huby[121], gateway[122], routery[123], multipleksery[124] i umożliwiają konfigurowanie sieci szkieletowych jak też transportowych magistrali telekomunikacyjnych (PDH, SDH, ATM) z wykorzystaniem uniwersalnych interfejsów[125].

Aktualnie coraz to nowsze rozwiązania technologiczne dostępu abonenta do usług sieci telekomunikacyjnej umożliwiają zwiększenie szerokości pasma i łatwiejszy dostęp przez wszystkie znane media transmisyjne. W celu realizacji problemów badawczych pracy, dokonano analizy i usystematyzowania rodzajów infrastruktury telekomunikacji (Schemat 2.2.) według wybranych przekrojów:

1. **Systemy transportowe:**
   a) sieci dostępu abonenckiego;
   b) sieci publiczne;
   c) sieci transmisyjne;
   d) sieć globalna Internet;
   e) systemy telefonii komórkowe;
   f) systemy wideokomunikacji;
   g) systemy satelitarne.
2. **Systemy komutacji:**
   a) komutacja połączeń;
   b) centrale analogowe;
   c) centrale cyfrowe;
   d) sieć inteligentna.

---

[120]Most – Urządzenie komunikacyjne funkcjonujące w warstwie łącza i pełniące funkcję łącznika między sieciami lub segmentami sieci LAN (przesyła lub zatrzymuje pakiety).
[121]Hub - Elementarny węzeł komunikacyjny do łączenia, rozgałęzienia lub koncentracji strumieni przepływu danych w sieciach komputerowych LAN. Posiada wiele rozwiązań zastępuje: most, router, przełącznik itp.
[122]Gateway (brama) – pojęciowy albo fizyczny węzeł sieci komunikacyjnej stanowiący bramkę, stosowaną w sieciach lokalnych do obsługi niekompatybilnych dwóch sieci albo urządzeń.
[123]Router - Urządzenie komunikacyjne wraz z oprogramowaniem do sprzęgania sieci cyfrowych, funkcjonujące w warstwach: fizycznej, łącza danych i sieciowej modelu ISO/OSI (przełącza, przesyła i wybiera trasy).
[124]Multiplekser – sprzętowo programowe urządzenie mające zdolność multipleksowania kanałów.
[125]Styk, czyli miejsce lub punkt, w którym są zlokalizowane fizyczne połączenie komunikacyjne pomiędzy dwoma urządzeniami lub połączenie logiczne między użytkownikiem a programem czy też systemem operacyjnym.

- komunikację w podczerwieni;
- telefonię bezprzewodową;
- telefonię komputerową;
- radiofonię analogową i cyfrową;
- systemy radiowe, WLL (RLL), DECT;
- systemy przywoławcze np. ERMES;
- systemy trankingowe np. TETRA[132];
- analogowy dostęp komórkowy: NMT, AMPS;
- cyfrowy dostęp komórkowy: GSM, DCS, PCN;
- dostęp globalny i satelitarny: VSAT, UMTS[133], IMT2000, GPS;
- dostęp przez duże systemy satelitarne.

Analogowy dostęp abonencki. Przesłanie sygnału głosu ludzkiego wymaga kanału zdolnego do przeniesienia określonego pasma częstotliwości. Głos ludzki zawiera wiele częstotliwości podstawowych i harmonicznych, których zestaw nadaje ton i barwę charakterystyczną dla każdego rozmówcy. Widmo mowy obejmuje częstotliwości od 100 Hz do ponad 8 kHz, przy czym największa gęstość widmowa (energia) przypada w okolicy 500 Hz i sukcesywnie maleje ze wzrostem częstotliwości. Ucho ludzkie odbiera sygnały w znacznie szerszym zakresie częstotliwości, a graniczne wyróżnianie sygnałów zależy od cech osobniczych człowieka. Typowy zakres sygnałów rejestrowanych przez ucho ludzkie obejmuje częstotliwości od 20 Hz do 15 kHz (niekiedy 20 kHz), a największa czułość mieści się od 1 kHz do 3 kHz. Dla dobrego zrozumienia mowy i rozpoznania osoby mówiącej wystarczy pasmo, w którym jest zawarta główna cześć energii, to znaczy w zakresie od 360 Hz do 3400 Hz.

Ze względów ekonomicznych zdecydowano transmitować w urządzeniach telefonicznych pasmo o szerokości 3,1 kHz {niekiedy 3,3 kHz w zakresie od 200 do 3500 Hz), zapewniające właściwe zrozumienie mowy. Uwzględniając bariery ochronne po obydwu stronach pasma, niezbędne przy multipieksowaniu i wydzielaniu sygnałów mowy na wyższych częstotliwościach pracy, rzeczywista

---

[132]TETRA – ang. Trans-European Trunked Radio – europejski standard zbiorowej łączności typu dyspozytorskiego (trunkingowego), przystosowany do cyfrowej mowy i danych pakietowych.

[133]UMTS – ang – Universal Mobile Telecomunication System – europejski standard systemu komórkowego trzeciej generacji wywodzący się z systemu GSM.

Ad. 1. Systemy transportowe

Ad. a) sieci dostępu abonenckiego

Sieci funkcjonujące na najniższym poziomie warstwowym infrastruktury telekomunikacyjnej[126] stają się wyodrębnioną częścią sieci publicznej, zwaną siecią dostępu abonenckiego. Dostęp abonencki zapewnia znajdująca się najniżej hierarchicznie infrastruktura telekomunikacyjna, obejmująca medium transmisyjne i sposób dostępu abonenta do sieci (analogowej lub cyfrowej) - z uwzględnieniem różnorakich potrzeb abonenta. W zależności od wielkości zapotrzebowania na pasmo wymagane przez abonenta wyróżnia się usługi: głosowe POTS[127], teledacyjne (komputerowe), obrazowe obejmujące obrazy wideo, TV oraz telewizji interaktywnej[128].

To wszystko spowodowało, że obecnie podziału infrastruktury telekomunikacyjnej i świadczonych usług można dokonywać na wiele sposobów. Jednym z takiego kryterium jest zastosowane medium transmisyjne, według, którego zostały zdefiniowane rodzaje dostępu do usług telekomunikacyjnych, a najbardziej wykorzystywanymi i znanymi są:

- analogowy dostęp przewodowy przez: telefony analogowe, centrale abonenckie PABX[129] i publiczne systemy komutacji;
- cyfrowy dostęp przewodowy przez: telefony cyfrowe, wideofony, centrale PABX, terminale ISDN, urządzenia DSL, systemy komutacyjne, sieci pakietowe, terminale klasy PC i sieci komputerowej;
- dostęp optyczny: sieci FITL[130], sieci PON[131];
- dostęp hybrydowy: sieci HFC, sieci telewizji kablowej - CATV;
- dostęp bezprzewodowy obejmujący:

---

[126]Zob. Rozdział 1., Schemat 1.11. Uproszczony warstwowy schemat infrastruktury telekomunikacyjnej kraju.

[127]POTS – ang. Plain Old Telephone Services – najstarsza, podstawowa usługa telefoniczna, umożliwiająca analogowy przekaz głosu przez trwałe lub komutowane łącza telefoniczne.

[128]Usługa ineraktywna to taka, w której użytkownik ma większą możliwość wyboru programów i czasu trwania ich emisji oraz uczestniczenia w nich.

[129]PABX – ang. Private Automatic Branch Exchange – lokalny, automatyczny, cyfrowy system komutacji przeznaczony dla biur i przedsiębiorstw do realizacji połączeń wewnętrznych, także połączeń do zewnętrznej sieci publicznej

[130]FITL – ang. Fiber in the Loop - abonencki optyczny system dostępowy, realizowane mogą być usługi cyfrowe ISDN oraz szerkopasmowe o przepływności powyżej 2 Mb/s.

[131]PON – ang. Passive Optical Network – rozwiązanie abonenckiego dostępu kablowego przy użyciu sieci optycznej.

(telefony, telefaksy), jak i urządzenia cyfrowe (terminale ISDN, sieci cyfrowe) bez stosowania zewnętrznych modemów komunikacyjnych.

Cyfrowy dostęp abonencki. Transmisja cyfrowa w najprostszym wydaniu oznacza, że przesyłany jest ciąg impulsów dwustanowych typu TAK/NIE, podobnie jak w komputerach. Sygnały te, zwane są bitami, mogą być transmitowane przy współczesnych technologiach w szerokim zakresie szybkości, nawet powyżej kilkuset Gb/s (np. 400 Gb/s w jednym włóknie optycznym systemu WaveStar OLS 400G Lucenta). Istnieje wiele parametrów charakteryzujących przydatność łączy telekomunikacyjnych do transmisji danych.

Cyfrowy dostęp abonencki ISDN (ang. Integrated Services Digital Network) to otwarty, całkowicie cyfrowy system telekomunikacyjny z integracją usług gwarantuje realizację usług oferowanych dotychczas w sieciach analogowych, jak też zapewnia wprowadzenie nie oferowanych dotąd przekazów cyfrowych, opartych na technice cyfrowego przetwarzania informacji, komutacji kanałów i komutacji pakietów (Schemat 2.3.).

Potencjalne możliwości sieci ISDN, przekraczają aktualne potrzeby użytkowników, umożliwiają tworzenie lokalnych podsieci telekomunikacyjnych, zastępując w ten sposób niewielkie centralki domowe (do ośmiu urządzeń), dyspozytorskie czy zakładowe dla większej liczby abonentów. W systemie ISDN użytkownik posiada do dyspozycji dwa rodzaje dostępu do kanału telekomunikacyjnego:

- dostęp wąskopasmowy BRA (ang. Basic Rate Access) w kanale podstawowym o strukturze 2B + D16;
- dostęp szerokopasmowy PRA (ang. Primary Rate Access) w kanale pierwotno-grupowym o strukturze 30B + D64.

Korzystając z kanału podstawowego BRA abonent ma możliwość dostępu do dwóch jednakowych, dwukierunkowych i wzajemnie niezależnych kanałów informacyjnych B, każdy o maksymalnej przepływności binarnej 64 kb/s, oraz do jednego kanału D16 o szybkości podkładowej 16 kb/s. Kanał D jest przeznaczony do przesyłania sygnalizacji lub transportu danych telemetrycznych. Przekaz sygnalizacji w kanale D16 dokonuje się na zasadzie komutacji pakietów i jest niezależny od sposobu wykorzystania kanałów informacyjnych typu B.

szerokość pasma transmitowanego przez urządzenia telefoniczne i kanały transmisyjne wynosi 4 kHz, Do transmisji dźwięku {również tego o wysokiej jakości) przyjmuje się pasmo w zakresie częstotliwości naturalnych od 20 Hz do 16 kHz.. Istnieją dwa odmienne sposoby przesyłania dowolnej informacji przez łącza telekomunikacyjne: transmisja analogowa i transmisja cyfrowa.

Transmisja analogowa oznacza, że są przesyłane sygnały o ciągłym widmie częstotliwości, takim jak głos, dźwięk lub światło. Większość istniejących łączy telekomunikacyjnych, po których są przesyłane dane na najniższym poziomie infrastruktury, jest przeznaczona do transmisji analogowej, a nie cyfrowej. Również łącza telefoniczne, doprowadzone bezpośrednio do mieszkań abonentów, są głównie łączami analogowymi zdolnymi do przesyłania sygnałów w ograniczonym zakresie częstotliwości.

W systemach kablowej telefonii przewodowej zakres częstotliwości nośnych zależy od natury medium i wymagań aplikacyjnych. Na przykład typowa skrętka dwuprzewodowa przenosi częstotliwości w zakresie od 10 Hz do 1000 kHz, a w wykonaniach specjalnych nawet powyżej 1 MHz. Kable współosiowe (koncentryczne) są przystosowane do przekazów w zakresie częstotliwości od 1 do 100 MHz. Dla częstotliwości radiowych, aż do promieniowania widzialnego, zdefiniowano wiele pasm o różnych szerokościach i zastosowaniu.

Wzajemne łączenie dwóch abonentów, posiadających najprostsze aparaty telefoniczne bez tarczy numerowej, było nie lada problemem, który istniał od wynalezienia telefonu (1876 r.). W tym sposobie łączenia każdy aparat telefoniczny był wyposażony w induktor z korbką - sukcesywnie zastępowany lokalną baterią (akumulatorem), a przyjmowanie zgłoszeń, także krosowanie, trasowanie i likwidacja połączeń były załatwiane ręcznie przez telefonistkę na stanowisku łącznicy lokalnej, miejskiej lub międzymiastowej.

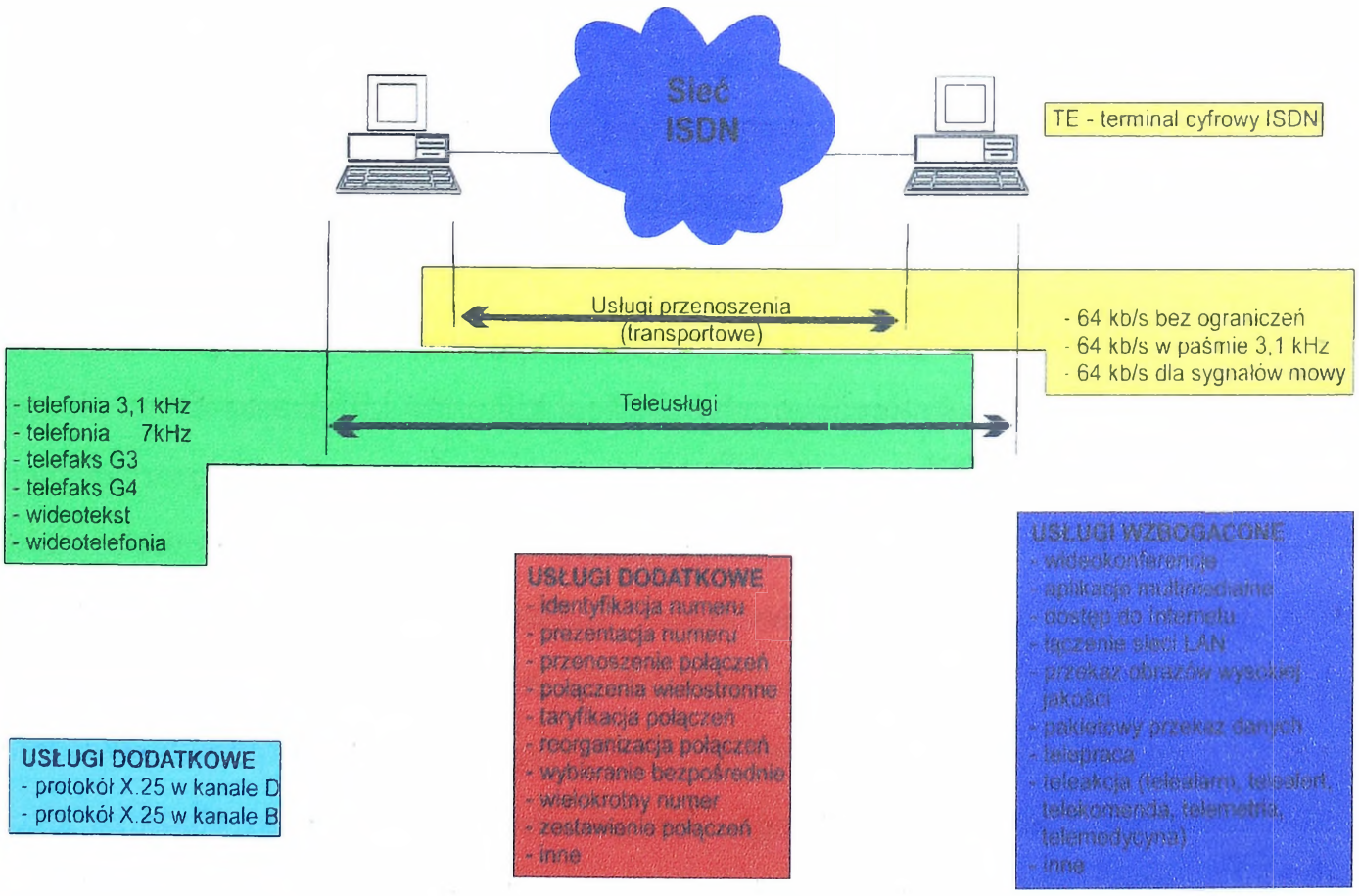
Współczesna centrala abonencka PABX (ang. Private Automated Branch Exchange) jest lokalnym, telefonicznym systemem komutacji przeznaczonym dla wydzielonych biur lub przedsiębiorstw i umożliwiającym połączenia wzajemne, także zestaw połączeń do zewnętrznej publicznej sieci telefonicznej PSTN. Automatyczne centrale abonenckie, oznaczone równoważnymi terminami PBX, PABX, EPABX, mogą obsługiwać zarówno klasyczne urządzenia analogowe

krotność (El) w transmisji synchronicznej SDH. Usługi w zintegrowanej usługowo sieci cyfrowej ISDN (Schemat 2.4.) można podzielić na:

- usługi przenoszenia, czyli usługi transportowe dotyczące sposobu transmisji sygnałów cyfrowych między terminalami użytkowników, definiowane na styku terminal-sieć. Usługi te określają możliwości sieci ISDN w zakresie trybu transmisji, wielkości przepływności i stosowanych protokołów transmisyjnych. Nie jest istotne, jakiego rodzaju dane są przesyłane ani do czego służą, ponieważ sieć nie zajmuje się obróbką informacji;
- teleusługi zawierające, oprócz odpowiednich usług przenoszenia, sposoby sterowania urządzeniami końcowymi. Sterowanie to, realizowane przez standardowe procedury siedmiowarstwowego modelu odniesienia ISO, zapewnia kompatybilność terminali pracujących w sieci.

Schemat 2.4.

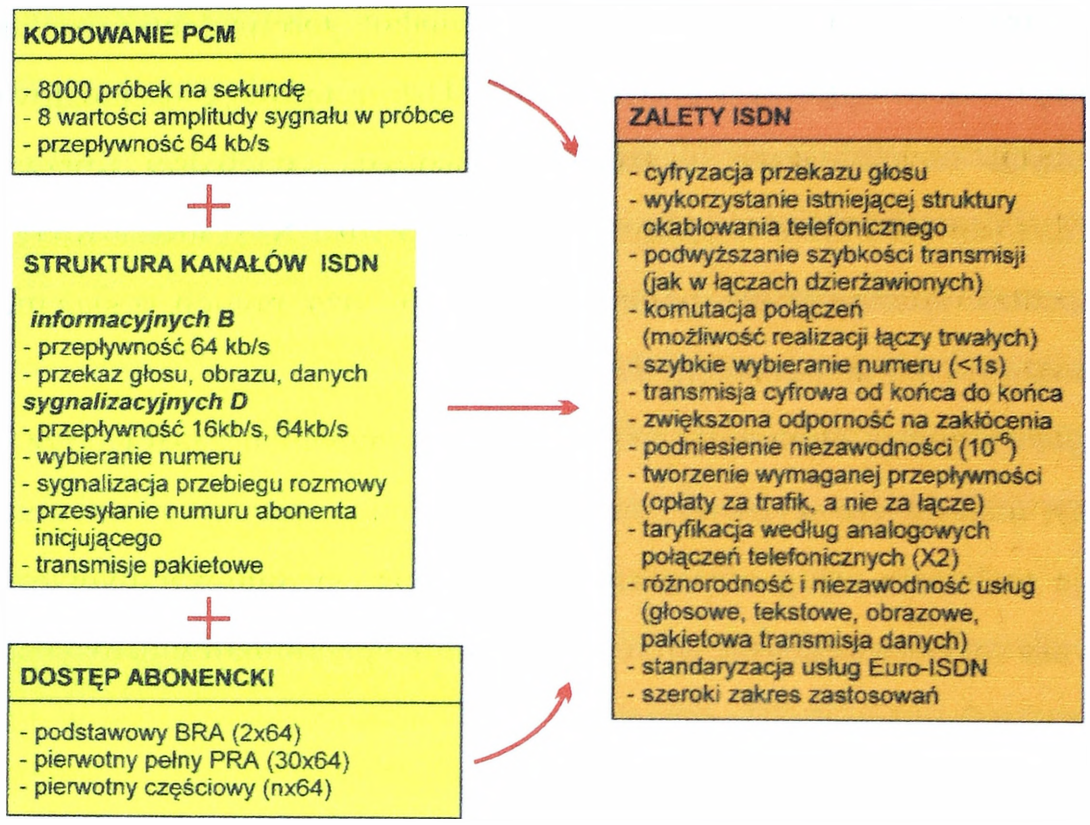
Podział usług sieci ISDN



Źródło: *Net World Vademecum teleinformatyka cz. 1*, International Data Group Poland S.A., Warszawa 2004, s. 85.

Schemat 2.3.

Zalety zintegrowanej sieci cyfrowej ISDN.



Źródło: *Net World Vademecum teleinformatyka cz. 1*, International Data Group Poland S.A., Warszawa 2004, s. 84.

Przepływność użytkowa kanału podstawowego BRA wynosi 2x64 kb/s+16 kb/s=144 kb/s, a po uzupełnieniu o kanał utrzymaniowy M (4 kb/s) oraz sygnały ramkowania (12 kb/s) - łączna wymagana przepływność kanału wynosi 160 kb/s. Nowa adaptacyjna technika jednoczesnego transportu informacji cyfrowych w obydwu kierunkach na tej samej linii dwuprzewodowej zajmuje dodatkowo 32 kb/s, co powiększa całkowitą przepływność linii fizycznej do 192 kb/s.

Wykorzystując kanał pierwotno-grupowy PRA, przeznaczony głównie do przyłączania koncentratorów i central abonenckich PABX, mamy możliwość dostępu do 30 dwukierunkowych kanałów informacyjnych B oraz jednego kanału sygnalizacyjnego D64 o szybkości podkładowej 64 kb/s. Całkowita przepływność kanału pierwotno-grupowego (nazywanego również pierwotnym) wynosi 30x64 kb/s+64 kb/s=1984 kb/s, a po uwzględnieniu dodatkowych sygnałów synchronizacji i nadzoru kanał ma łączną przepływność 2048 kb/s, przyjętą jako podstawową

- transmisja danych, przeznaczona do realizacji połączeń pomiędzy komputerami dwóch abonentów lub dostępu do wybranej sieci komputerowej. Transmisja może być realizowana w trybie komutacji kanałów lub pakietów. W jednym kanale B dostępu podstawowego BRA o szybkości podkładowej 64 kb/s można prowadzić równocześnie do 8 niezależnych transmisji danych o różnych przepływnościach (600 b/s, 1200 b/s itd.), przy czym maksymalna przepływność kanału nie może przekroczyć 57,6 kb/s.

Usługi teleakcji w ISDN stanowią odrębną grupą nowych usług sieci ISDN, dla których wspólną cechą jest przekazywanie krótkich komunikatów, zwykle wymagających małych szybkości transmisji (do 9600 b/s). Usługi te są realizowane wyłącznie w trybie transmisji pakietowej przez kanał sygnalizacyjny D16. Do tej pory zdefiniowane usługi teleakcji obejmują:

- telealarm - zapewniający przekazywanie komunikatów o alarmie z czujników zainstalowanych u abonenta do odpowiednich centrów dyżurnych sieci;
- telealert - zapewniający przesyłanie komunikatów rozsiewczych w przeciwnym kierunku niż telealarm, tzn. z centrum nadzorującego do poszczególnych lub wybranych terminali użytkownika. Usługa ta umożliwia też selektywne informowanie mieszkańców zagrożonego regionu o stanie pogody, poziomie zagrożeń wodnych czy sejsmicznych, stężeniu zanieczyszczeń atmosferycznych itp.;
- telekomenda - umożliwiająca zdalne sterowanie urządzeniami abonenta wg uzgodnionego algorytmu lub diagramu czasowego przez odpowiednie systemy zarządzające. Usługa ta jest stosowana przy uaktywnianiu wielu prostych, automatycznych czynności polegających na: załączaniu i wyłączaniu źródeł energii, regulacji centralnego ogrzewania, oświetleniu obiektów, ulic, również nawadnianiu terenów, zmianie reklam i zdalnej rejestracji przekazów telewizyjnych;
- telemetria - zapewniająca zdalny odczyt parametrów urządzeń pomiarowych zainstalowanych u abonenta sieci ISDN i przekazywanie

Teleusługi ISDN to konkretne funkcje usługowe dostarczane za pomocą cyfrowej sieci ISDN. Do najważniejszych udostępnianych teleusług w sieci ISDN należą:

- telefonia cyfrowa, zapewniająca zestawianie połączeń fonicznych wyłącznie za pomocą przekazu cyfrowego z jednoczesnym uaktywnieniem sygnalizacji abonenckiej typu DSS nr 1 przez kanał sygnalizacyjny D16. Usługa ta w sieci ISDN zapewnia standardowe pasmo przenoszenia (4 kHz), pasmo poszerzone (7 kHz), sygnały stereofoniczne (dla wideokonferencji), połączenia trójstronne lub konferencyjne;
- teleteks, umożliwiający transmisję tekstów o znacznie rozszerzonym zbiorze znaków alfanumerycznych, również dokumentów formatu A4 przy pełnym zachowaniu ich formy i treści;
- telefaks, polegający na przekazywaniu zarówno tekstu, jak i grafiki dzięki analizie pikslowej oryginału wraz z rozróżnianiem kolorów;
- wideoteks, prezentujący na ekranie monitora obrazy i informacje w trybie tekstowym, semigraficznym lub graficznym, wybierane interaktywnie za pomocą klawiatury. Wideoteks wprowadzono głównie w celu umożliwienia abonentowi korzystania z oddalonych baz danych. Usługa ta akceptuje przesyłanie obrazów w postaci skompresowanej, zgodnie z zaleceniami kompresji H.261;
- wideofonia, zapewniająca równoczesną transmisję sygnału mowy i obrazu wolnozmiennego z szybkością kilku lub kilkunastu zmian ekranu na sekundę. Usługa wideofonii jest szczególnie przydatna do organizacji wymiany danych w ramach grupy użytkowników o umiarkowanej liczebności, zainteresowanych realizacją usług multimedialnych o charakterze rozgłoszeniowym lub grupowym;
- poczta elektroniczna, umożliwiająca przekazywanie i przechowywanie wiadomości dla wybranego abonenta w wyodrębnionym obszarze sieci ISDN. Wiadomość może mieć formę pisma, mowy lub ilustracji, w zależności od rodzaju „skrzynki elektronicznej", i zostać odebrana przez abonenta w dowolnym, dogodnym dla niego terminie;

wykorzystujące technikę ATM zapewniają możliwość współpracy z innymi systemami, w tym z:

- systemami analogowymi (systemami starego parku – na poziomie kanałów analogowych;
- systemami cyfrowymi ISDN w sposób bezpośredni poprzez dostęp szerokopasmowy 155 Mb/s oraz PRI (2048 kb/s);
- systemami resortowymi w sposób pośredni przy wykorzystaniu interfejsów DSTG[134].

Systemy BISDN mogą zapewnić równorzędny, w stosunku do systemów ISDN lub wyższy poziom bezpieczeństwa łączności (Tabela 2.1.). W przypadku przekształcania sieci ISDN w sieci B-ISDN zostaje zachowana możliwość współpracy z użytkownikami publicznych sieci transmisji TD (w Polsce może to być np. POLPAK - T), z abonentami cyfrowych sieci komórkowych GSM oraz perspektywicznej sieci radiotelefonicznej IMT-2000, z abonentami analogowych sieci komórkowych (w przypadku Polski – CENTERTEL) itp.

Tabela 2.1. Zasadnicze różnice systemów N-ISDN i B-ISDN

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

Źródło: *Net World, Vademecum teleinformatyka cz. 1*, International Data Group Poland S.A., Warszawa 2004, s. 90 i 113.

Systemy B-ISDN wykorzystujące technikę ATM mogą być wprowadzane w sposób ewolucyjny, w ograniczonym zakresie oraz na dowolnym obszarze. Przewiduje się, że systemy B-ISDN z uwagi na swoje zalety będą w niedalekiej

---

[134]DSTG - ang. Digital Strategic – Tactical Gateway - Interfejs PCM/Delta – Porozumienie Standaryzacyjnym NATO Stanag 4578 - *The NATO Multi-Channel Digital Strategic – Tactical Gateway.*

ich do właściwego centrum rozliczeniowego (automatyczny odczyt liczników wody, gazu, energii elektrycznej, temperatury, itp.).

Szerokopasmowy dostęp abonencki BISDN. Sieć szerokopasmowa BISDN (ang. Broadband Integrated Sewices Digital Network) stanowi rozszerzenie wąskopasmowej sieci cyfrowej NISDN (Narrow ISDN). Zgodnie z zaleceniami ITU-T (CCITT) jest możliwe przesyłanie przez sieć BISDN informacji w różnych postaciach: dane cyfrowe, głos, dźwięk jakości CD, zeskanowane obrazy, obrazy wideo, filmy, sygnały telewizyjne zwykłe i wysokiej rozdzielczości HDTV. Kanały podstawowe PRA ISDN o szybkości nominalnej 2 Mb/s są łączone przez zwielokrotnienie w trakty szerokopasmowe o przepływnościach 155 Mb/s, 622 Mb/s, 2,5 Gb/s oraz 10 Gb/s, zgodnie z przyjętą hierarchią transmisji. Fizyczny transport danych w łączach szerokopasmowych opiera się na synchronicznej technologii światłowodowej SDH (amerykański SONET) lub technologii przekazu asynchronicznego ATM. W sieciach synchronicznych SDH transport informacji może odbywać się w ustalonych standardach: BISDN, FDDI i SMDS.

W technologii ATM jest możliwe bardziej efektywne wykorzystanie maksymalnej szybkości łączy szerokopasmowych przez elastyczne dopasowanie się sieci do przekazów o zmiennej wydajności źródeł. Technologia ATM, przystosowana do przekazów multimedialnych, jest w stanie obsługiwać transmisję danych dowolnego typu, w tym przekazy telewizyjne o zmiennej długości oraz spiętrzenia napływające równocześnie z wielu sieci lokalnych. Systemy szerokopasmowe rozwijane przy wykorzystaniu techniki ATM, dzięki wyposażeniu urządzeń sieciowych (węzłów komutacyjnych, stacji teletransmisyjnych) w odpowiedni – wymagany zestaw kart interfejsowych pozwalają współpracować z dowolnymi innymi sieciami i systemami telekomunikacyjnymi. Z uwagi na bardzo duże nakłady finansowe ponoszone przez wiodące światowe firmy telekomunikacyjne na rozwój techniki ATM – aktualnie jest już dostępny odpowiedni sprzęt umożliwiający budowę zarówno stacjonarnych jak i mobilnych sieci łączności na potrzeby systemu bezpieczeństwa państwa.

Szybki rozwój technologii ATM powoduje, że koszty wprowadzania tych systemów będą się sukcesywnie zmniejszać. Systemy szerokopasmowe B-ISDN

w obydwu kierunkach za pomocą pojedynczej skrętki miedzianej, jest stopniowo wypierana przez szybsze łącza HDSL, oferujące przepływność 2 Mb/s za pośrednictwem jednej lub dwóch par (skrętek) linii telefonicznej.

Asymetryczny dostęp abonencki ADSL (ang. Asymmetric Digital Subscriber Line) zapewnia przesyłanie sygnałów cyfrowych za pośrednictwem tradycyjnego kabla miedzianego z różnymi przepływnościami, zależnie od kierunku transmisji: większą w stronę abonenta, mniejszą w kierunku odwrotnym. Dostępna szybkość transmisji zależy od wielu czynników, między innymi od długości kabla, jego właściwości oraz zakłóceń pochodzących od urządzeń telekomunikacyjnych.

Przepływność kanału od abonenta w kierunku stacji centralnej - wynosząca początkowo 16 kb/s, następnie 64 kb/s, a docelowo 640 kb/s -umożliwia reakcję abonenta na ofertę przesyłanych przez dostawcę usług w szybkim kanale docelowym. Łącze ADSL jest wyposażone dodatkowo w dwukierunkowy kanał analogowy w naturalnym paśmie przenoszenia 4 kHz dla podstawowej usługi telefonicznej POTS.

Projekt ADSL, opracowany przez ANSI (pierwsze próby w 1993 r. w Bell Atlantic), jest przeznaczony do tworzenia usług multimedialnych i nowoczesnych usług interakcyjnych (VOD, IVOD) obejmujących, przekaz do abonenta wybranych filmów i obrazów telewizyjnych, szybki dostęp do Internetu, a także pracę biurową w domu, teleinformację, teleedukację, telezakupy, teleserwis itp.

Zaletą systemu jest wykorzystanie istniejących zasobów telekomunikacyjnych opartych na sieci abonenckiej i rozdzielczej, zbudowanych w całości z miedzianych linii telefonicznych - doposażonych w zespoły cyfrowych modemów DSL po obydwu stronach łącza.

Zasadniczą wadą systemów ADSL jest wielokrotnie mniejsza szybkość transmisji w porównaniu z systemami opartymi na szerokopasmowych światłowodowych łączach abonenckich, przy wysokim koszcie urządzeń wspomagających. Z tego powodu system ADSL jest nadal często traktowany jako przejściowy- przed powszechnym zastosowaniem torów światłowodowych doprowadzonych bezpośrednio do mieszkania abonenta.

Światłowodowy dostęp abonencki. Nowoczesny dostęp abonencki FITL (ang. Fiber in the Loop) jest oparty na penetracji światłowodu bezpośrednio do

przyszłości rozwijane i eksploatowane w wielu krajach świata. Systemy B-ISDN są systemami przyszłości i będą w stanie spełnić wymagania dowolnych użytkowników (publicznych, specjalnych) realizując nawet takie usługi, które na dziś dzień nie zostały przez tych użytkowników sformułowane. Są to systemy wyjątkowo podatne na dalszy rozwój.

Dostęp szerokopasmowy xDSL to nowoczesna technologia cyfrowego dostępu abonenckiego DSL (ang. Digital Subscriber Line) jest w Europie jedną z bardziej dynamicznie rozwijających się technologii dostępu szerokopasmowego na najniższym poziomie sieci telekomunikacyjnych.

Dwukierunkowe i zwykle asymetryczne końcowe urządzenia komunikacyjne - nazywane coraz częściej modemami DSL - umożliwiają transmisje w szerokim zakresie szybkości (od 640 kb/s do kilkudziesięciu Mb/s) w kierunku abonenta, przez jedną parę przewodów miedzianych łączących użytkownika z najbliższym węzłem telekomutacyjnym.

Abonenckie łącze cyfrowe HDSL (ang. High Digital Subscriber Line) o wysokiej przepływności jest realizowane na zwykłej miedzianej skrętce telefonicznej. Normalna szybkość transmisji wynosi 784 kb/s w obu kierunkach przenoszenia lub jednokierunkowo 1544 kb/s dla linii Tl (2048 kb/s dla linii El). Połączenie pełnodupleksowe o przepływności 2048 kb/s wymaga podwójnej skrętki miedzianej, przy ograniczonym zasięgu, bez stosowania regeneratorów sygnału. Zasięg łącza jest silnie uzależniony od przekroju przewodów miedzianych i wynosi od 4 km (przy przekroju kabli 0,4 mm) do 10 km (przy przekrojach 0,8 mm). Przepływność 2 Mb/s uzyskuje się najczęściej za pomocą efektywnej modulacji z kodowaniem 2B1Q o skuteczności widmowej 2 b/s/Hz. System, wyposażony w multipleksery z podziałem czasu po obydwu stronach łącza między współpracującymi węzłami, zapewnia zwykle przesyłanie strumienia danych (2 Mb/s) lub 30 kanałów telefonicznych, każdy o przepływności 64 kb/s. W Polsce znany jako system Watson (oferowany w kilku wersjach przez BPS również do transmisji multimedialnych). Inne rozwiązania, takie jak ASLMX (Digiloop, ECI TELECOM), umożliwiają zwiększenie zasięgu przez wprowadzenie regeneratorów.

Najstarsza i najprostsza wersja symetrycznego łącza nazwana SDSL (ang. Symmethc Digital Subscriber Line), zapewniająca przepływność 384 kb/s

Wybór odpowiedniej architektury szerokopasmowej sieci abonenckiej HFC, uzależniony od wielu czynników, powinien zapewnić kilka podstawowych wymagań abonenta:

- dostęp do dystrybucji telewizji programowej (nie mniej niż 50 kanałów w standardzie PAL) przy najmniejszych kosztach instalacyjnych;
- dostęp do realizacji usług interaktywnych[135] klasy VOD (ang. Video on Demand) wymagających dodatkowo kanału zwrotnego (w kierunku od abonenta do stacji czołowej);
- dostęp do usług IP[136] oferowanych przez sieć Internetu z pełną szybkością
- dosyłową hybrydowej infrastruktury;
- realizację klasycznych usług telefonicznych POTS oraz usług rozszerzonych, określanych jako multimedialne.

Rozróżnia się dwa rodzaje architektury sieci HFC stosowanej w sieciach kablowych CATV:

- architektura nakładkowa charakteryzująca się jeszcze rozdzieleniem kanałów i kierunków transportu informacji do węzła abonenckiego, zwykle dwoma włóknami w kierunku abonenta i jednym włóknem w stronę stacji czołowej;
- architektura integracyjna, w której transmisja przebiega dwukierunkowo jednym kablem koncentrycznym CATV między abonentem a węzłem dostępu sieciowego.

Pasmo w kanale zwrotnym przeznaczone do interakcji, usług teledacyjnych oraz podstawowych i rozszerzonych usług telefonicznych może przybierać trzy podzakresy (znane są też inne podziały pasma):

- 5÷30 MHz (lub 10÷55 MHz) przy podziale w dolnej części dostępnego pasma medium transmisyjnego;
- 5÷112 MHz przy podziale w środkowej części pasma;

---

[135]Usługa ineraktywna to taka, w której uzytkownik ma większą możliwość wyboru programów i czasu trwania ich emisji oraz uczestniczenia w nich.

[136]IP – ang. Internet Protocol – otwarty, stale rozwijany protokół komunikacyjny przeznaczony do realizacji usług połączeniowych za pomocą klasycznego protokołu transportowego czwartej warstwy modelu ISO/OSI ogólnego przeznaczenia, oferujący niezawodną, połączeniowo zorientowaną transmisję danych w sieciach o różnych sposobach transmisji: LAN, MAN lub WAN. Najczęściej kojarzony z funkcjonowaniem sieci Internet zawiera kilkadziesiąt protokołów wspomagających.

mieszkania abonenta. Zastępuje tradycyjną organizację analogowego dostępu telekomunikacyjnego wykorzystującego kable miedziane przez doprowadzenie szerokopasmowego kanału cyfrowego wykonanego w technice światłowodowej o przepływności od 2 Mb/s do 6/8 Mb/s w kierunku abonenta oraz od 64 kb/s do 640 kb/s w kierunku powrotnym.

Sieć optyczna FITL, oprócz tradycyjnych usług POTS i ISDN, realizuje transmisję danych oraz nowe usługi szerokopasmowe (min. 2 Mb/s) obejmujące: dostęp do Internetu, usługi multimedialne, programy TV i interaktywną telewizję IVOD.

Niezależnie od przyjętego rozwiązania światłowodowego trakt rozdzielczy między węzłem dostępu sieciowego OLT (ang. Optical Line Terminator), mieszczącym się w systemie komutacji lub w sieci transportowej, a węzłem abonenckim ONU (ang. Optical Network Unit) może przyjmować różne topologie sieciowe: punkt-punkt, strukturę gwiazdy lub strukturę drzewiastą. Światłowodowy tor dosyłowy o długości zwykle nie przekraczającej 20 km może mieć charakter pasywny PON (ang. Passive Optical Network) - łącznie z zainstalowanymi węzłami pośredniczącymi lub charakter aktywny AON (ang. Active Optical Network) – z zastosowaniem dwukierunkowych wzmacniaczy optycznych (regeneratory sygnału) umożliwiających reakcję abonenta. Spotykane są jeszcze mniej ekonomiczne rozwiązania, w których dwa jednokierunkowe tory optyczne prowadzą komunikację dwustronną między abonentami a centrum komutacji.

Hybrydowy dostęp abonencki HFC. Wprowadzenie techniki światłowodowej i modernizacja sieci telekomunikacyjnej w warstwie transportowej (PDH, SDH, ATM) pozwalają na tworzenie szerokopasmowego dostępu abonenckiego przez rozbudowę istniejącej, lokalnej sieci telewizji kablowej CATV (ang. Cable TV) z zastosowaniem modemów kablowych.

Coraz bardziej powszechnym rozwiązaniem jest instalacja sieci hybrydowych (ang. Hybrid Fiber Coax), w których część toru przesyłowego między abonentem a lokalnym systemem komutacyjnym wykorzystuje istniejące miedziane tory kablowe dwuparowe lub tory koncentryczne znajdujące się wewnątrz budynków.

o cechach zbliżonych do promieniowania widzialnego - ogranicza się do pomieszczeń, w których znajduje się nadajnik sygnału i umożliwia powtórne używanie tych samych częstotliwości w sąsiednich pomieszczeniach bez ryzyka wzajemnej interferencji sygnałów.

Telefonia bezprzewodowa dostępu abonenckiego. Ze względu na różne zasady działania systemów radiowych i stosowanie odmiennych technologii, a także osiągane zasięgi komunikacji wyróżnia się następujące klasy systemów radiowego dostępu abonenckiego:

- systemy krótkiego zasięgu - do 5 km (przy średnim zakresie ok. 3 km), przeznaczone dla obszarów o dużej gęstości abonentów, realizowane w standardach CT2 (zakres częstotliwości 864÷868 MHz) i DECT (zakres 1880÷1900 MHz);
- systemy dużego zasięgu - do 50 km - dla łączności typu punkt-wiele punktów klasy PMP (ang. Point to Multipoint) z szerokością pasma 2 lub 4 MHz, przeznaczone do obsługi stosunkowo małych skupisk abonentów oddalonych od istniejącej infrastruktury telekomunikacyjnej i systemów komutacji;
- wąskopasmowe systemy komórkowe - do 35 km, oparte na systemach analogowym NMT i cyfrowym GSM, z dostępem typu TDMA/FDMA (ang. Time/Frequency DMsion Multiple Access) i przeznaczone zwykle dla obszarów o dużej gęstości abonentów;
- szerokopasmowe systemy komórkowe - z wykorzystaniem dostępu radiowego typu TDMA/CDMA (ang. Time/Code DMsion Multiple Access), o różnorodnych zastosowaniach wymagających dużej odporności na zakłócenia zewnętrzne.

Do najbardziej rozpowszechnionych należą: abonenckie systemy bezsznurowe CT (ang. Cordless Telephony) klasy CT1 i CT2 oraz sieć abonencka w europejskim standardzie DECT - uważana za prekursora tej technologii, zwłaszcza dla obszarów wiejskich.

Najnowocześniejszy europejski standard cyfrowej telefonii bezprzewodowej *DECT* (pierwotnie: ang. Digital European Cordless Telecommunications; obecnie: ang. Digital Enhanced Cordless Telecommunications) działa w paśmie 1880-1900

- 5÷175 MHz przy podziale w górnej części pasma.

Do tej pory najbardziej popularny jest kanał zwrotny CATV w paśmie 5÷30 MHz, coraz częściej rozszerzany do 10÷55 MHz. Dla krajów europejskich pasmo dostępowe mieści się w zakresie od 87MHz do 860 MHz, obejmując nie tylko naturalne częstotliwości radiowe UKF/FM i kanały telewizji programowej (do 450 MHz), ale także drugi skojarzony komplet kanałów telewizyjnych i teledacyjnych do świadczenia szerokopasmowych usług teledacyjnych.

Bezprzewodowy dostęp abonencki w podczerwieni. Sieci bezprzewodowe oparte na promieniowaniu mikrofalowym RF (ang. Radio Frequency) lub podczerwonym IR (ang. InfraRed) coraz częściej zastępują klasyczne abonenckie sieci lokalne.

Atrakcyjność komunikacji bezprzewodowej, także lokalnych sieci bezprzewodowych, polega na elastyczności w konfigurowaniu sieci dostępu zgodnie z potrzebą chwili oraz prostocie ich instalacji w pomieszczeniach, gdzie jest utrudnione okablowanie (np. hale fabryczne) lub na terenie otwartym, w którym całkowicie brak infrastruktury kablowej (bezdroża, mokradła, tereny wiejskie).

Do cech charakterystycznych łączności na falach z zakresu podczerwieni należą:

- dostępność szerokiego zakresu widma częstotliwości (200 THz);
- wysoka tłumienność jednostkowa przyjmująca wartości z zakresu 1÷10 dB/km;
- duże współczynniki pochłaniania promieniowania w pomieszczeniach biurowych (ścian, sufitu, mebli), co w konsekwencji prowadzi do zaników związanych z wielodrogowością sygnału (brak sygnałów odbitych);
- stosunkowo wysokie współczynniki odbicia promieniowania od odbijających przeszkód (40÷90%), umożliwiające korzystanie z łączności typu dyfuzyjnego (promieniowanie odbite).

Szerokość dostępnego pasma w zakresie fal podczerwonych jest największą zaletą transmisji na tych długościach fal. Słabo wykorzystywane widmo fal elektromagnetycznych z zakresu 700-1500 nm dostarcza pasma użytecznego o niezwykłej szerokości, około 200 THz, które ponadto może być wielokrotnie wykorzystywane w budynkach. Praktyczne rozchodzenie się fal podczerwonych –

Telefonia komputerowa jest określeniem używanym w odniesieniu do przemysłu i usług koncentrującego się na wykorzystaniu inteligencji komputerowej w urządzeniach telekomunikacyjnych, zwłaszcza w centralach i telefonach. Określenie to obejmuje wiele zastosowań, w tym integrację komputera i telefonu CTI przez sieć lokalną LAN, interakcyjne przetwarzanie głosu, pocztę głosową, bezobsługową recepcję, rozpoznawanie głosu, przejście z tekstu drukowanego na mowę, faksowanie, równoczesne korzystanie z danych i głosu, przetwarzanie sygnałów, wideokonferencje, predykcyjne wybieranie numeru, audioteks, odczytywanie danych, centra telefoniczne, punkty pomocy, a także tradycyjne przełączanie rozmów telefonicznych i sterowanie tymi połączeniami.

Integracja systemów telefonicznych i komputerowych w jeden system telefonii komputerowej jest najnowszą technologią telekomunikacyjną umożliwiającą, oprócz realizacji dotychczasowych funkcji telefonii komputerowej, koordynację działań między systemami telefonicznymi i komputerowymi. Integracja obejmuje wspólne wykorzystanie dedykowanych serwerów aplikacyjnych znajdujących się w połączonych zasobach sieci telefonicznych i komputerowych.

Radiowy dostęp abonencki. Rozwój techniki telekomunikacyjnej stworzył możliwość zastąpienia kablowych sieci abonenckich wykonanych z przewodów miedzianych lub światłowodowych przekazem bezprzewodowym, czyli transmisją radiową. Systemy radiowego dostępu abonenckiego SRDA (ang. RLL - Radio in the Local Loop), określane także jako WLL (ang. Wireless Local Loop), są realizowane za pomocą różnych technologii i systemów dostępu wielokrotnego.

Wspólną ich cechą jest wykorzystywanie tego samego medium - transmisji radiowej, a istotną zaletą - krótki czas instalacji i łatwość rekonfigu racji infrastruktury. Technika dostępu radiowego SRDA jest wykorzystywana zarówno do komunikacji głosowej, jak i abonenckiej transmisji danych.

Systemy przywoławcze dostępu abonenckiego obejmują jednokierunkową łączność radiową umożliwiającą abonentowi wyposażonemu w niewielki i tani odbiornik kieszonkowy (ang. pager) otrzymywanie krótkich indywidualnych komunikatów przywoławczych. Standaryzacja wielu niespójnych systemów doprowadziła do określenia międzynarodowego standardu POCSAG, definiującego zasady sygnalizacji i kodowania w systemach przywoławczych, a w Unii

MHz. Znormalizowany i rekomendowany przez ETSI do stosowania we Wspólnocie Europejskiej jako podstawowy system bezprzewodowych central abonenckich WPABX (ang. Wireless PABX), zapewnia użytkownikom takie same usługi jak abonentom systemów przewodowych PABX.

W standardzie DECT stosuje się 10 częstotliwości nośnych, na których dokonuje się transmisji z dostępem TDMA za pomocą 24 okienek (szczelin) czasowych w trybie dupleksowym TDD, polegającym na kolejnym przesyłaniu w obie strony ramek na pojedynczej częstotliwości nośnej. Dwanaście szczelin służy do transmisji ze stacji bazowej do terminalu ruchomego, pozostałe dwanaście szczelin - w kierunku odwrotnym.

Podstawowe zastosowanie systemu obejmuje: centralki domowe, automaty telefoniczne (system TELEPOINT), centrale zakładowe o dużym ruchu abonenckim, transmisję danych, faks do 4,8 kb/s, współpracę z sieciami cyfrowymi ISDN. Standard DECT jest wciąż rozwijany. Opracowano nowe profile dostępu umożliwiające świadczenie usług ISDN i szybka transmisję danych. Na rynku pojawiają się również systemy wykorzystujące te nowe profile, np. SWING 2.

Telefonia komputerowa. Pod określeniem telefonia komputerowa funkcjonują trzy pojęcia: integracja telefonu z komputerem CTI (ang. Computer Telephony Integration) stanowiąca najprostszą formę telefonii komputerowej, właściwa telefonia komputerowa oraz integracja telefonii komputerowej z siecią komputerową w jeden system telekomunikacyjny.

Istotą integracji telefonu z komputerem CTI jest proces łączenia zewnętrznych, już istniejących systemów komputerowych (zwykle do tej pory niezależnych i nie połączonych z siecią) z siecią telefoniczną i węzłem komutacyjnym. Węzłem komutacyjnym jest urządzenie albo sieć urządzeń używanych do łączenia i kierowania użytkowników telefonu w publicznej sieci telefonicznej PSTN, za pomocą centrali miejskiej CM lub centrali abonenckiej PABX wykorzystywanych w prywatnych sieciach telefonicznych. Łącze między systemem telefonii komputerowej (komputer wyposażony w sprzęt i oprogramowanie telefonii komputerowej) a lokalną centralą abonencką PABX jest określane jako połączenie CTI.

przywoławczego adresata oraz treści komunikatu. Zakodowana wiadomość jest następnie kierowana do odpowiedniego nadajnika radiowego i dociera do abonenta drogą radiową już w kilkadziesiąt sekund później. Podstawową wadą współczesnych systemów przywoławczych jest brak możliwości potwierdzenia odebranego komunikatu (z wyjątkiem systemów przywoławczych serii ReFLEX Motoroli).

Opracowany w ramach ETSI (w latach 1987-1992) nowoczesny, o europejskim zasięgu standard przywoławczy ERMES (ang Eufopean Radio Message System) znacznie przewyższa eksploatowane do tej pory sieci prywatnych operatorów o charakterze lokalnym.

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

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

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

Europejskiej przygotowano standard cyfrowego systemu przywoławczego ERMES (ang. European Radio Message System) o europejskim zasięgu. Większość prywatnych systemów przywoławczych stosowanych w Europie stosuje kod POCSAG, uznany przez CCIR za międzynarodowy kod przywoławczy RPC1.

Ze względu na zasięg rozróżnia się systemy przywoławcze:

- lokalne, dla prywatnych sieci, stosowane zwykle w obrębie jednego przedsiębiorstwa i mające jeden lub kilka zsynchronizowanych nadajników małej mocy;
- dużym zasięgu, obejmujące obszar miasta, regionu lub kraju, nadzorowane przez operatorów publicznych. W tym przypadku instaluje się bądź specjalne stacje bazowe do nadawania wyłącznie sygnałów przywołania (Telepage, Easy Call, Elite, MetroBip), bądź korzysta się z emisji sygnałów przywoławczych przez dodatkowe kanały nadajników radiofonicznych UKF-FM (Polpager, RDS).

Ze względu na rodzaj przesyłanej informacji i związanej z tym konstrukcji terminali odbiorczych rozróżnia się następujące usługi realizowane przez systemy przywoławcze:

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

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

Najbardziej rozpowszechnioną metodą jest korzystanie z usług telefonistki specjalnej centrali przywoławczej, przez głosowe przekazanie jej numeru

z dostępu do sieci również poza zasięgiem nadajników swojego narodowego operatora.

Technikę systemu TETRA można porównywać z analogowymi systemami trankingowymi, systemami telefonii komórkowej, a także innymi cyfrowymi systemami radiokomunikacji ruchomej. Systemy cyfrowe mają wiele cech i oferują wiele funkcji niedostępnych w systemach analogowych. Dotyczy to np. równoczesnego przekazywania głosu i danych oraz możliwości korzystania z sieci przez wielu użytkowników w zamkniętych ramach poszczególnych organizacji.

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

Kraje Unii Europejskiej na spotkaniu w Schengen w 1995 roku doszły do porozumienia, że w krajach członkowskich powinien zostać wprowadzony wspólny, otwarty standard radiokomunikacji ruchomej dla organizacji bezpieczeństwa publicznego. Propozycja stworzenia takiego systemu wraz ze szczegółowo określonymi wymogami odnośnie jego funkcjonowania została przekazana do ETSI, a ETSI w oficjalnej odpowiedzi stwierdziła, że opracowywany właśnie standard TETRA spełnia oczekiwania Unii. W 1997 roku TETRA uznana została za standard dla organizacji bezpieczeństwa publicznego, który będzie wprowadzony w krajach UE. Do tej pory w Europie wydano już wiele licencji dla operatorów systemu TETRA. Powszechnie przyjętą jest praktyka wydawania licencji ogólnokrajowych, preferująca tworzenie zintegrowanych systemów rozległych. Takie podejście zapewnia przede wszystkim minimalizację kosztów inwestycyjnych i operacyjnych, a ponadto gwarantuje użytkownikom ten sam poziom usług niezależnie od ich lokalizacji (np. realizacja połączeń grupowych na obszarze całego kraju).

TETRA poza odpornością na zakłócenia i stabilnością działania zapewnia wiele funkcji użytecznych w codziennej pracy zarówno służb bezpieczeństwa publicznego jak i organizacji i przedsiębiorstw komercyjnych – jak np.

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

W Polsce pracuje wiele prywatnych i publicznych sieci trankingowych, spełniających funkcje teledacyjne. Nadzieją na standaryzację na poziomie europejskim jest TETRA (ang. Trans European Trunked Radio), będąca w zakresie systemów teledacyjnych odpowiednikiem standardu GSM.

Wysokie oczekiwania odbiorców profesjonalnych w zakresie jakości komunikowania się, szybkości i bezpieczeństwa przesyłania danych oraz szybki rozwój myśli technologicznej końca XX wieku, a szczególnie w zakresie telekomunikacji, przyczyniły się do stworzenia nowej generacji cyfrowego systemu radiokomunikacji ruchomej a nazwie TETRA. TETRA, czyli Terrestial Trunked Radio, to nazwa całego zespołu otwartych standardów – interfejsów i usług – opracowanych przez ETSI[137]. TETRA to pierwszy w pełni otwarty, międzynarodowy standard cyfrowej radiokomunikacji ruchomej do zastosowań profesjonalnych.

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

ETSI zarezerwowało dla standardu TETRA dwa pasma częstotliwości: 380 ÷400 MHz dla służb bezpieczeństwa i porządku publicznego oraz pasmo 410÷430 MHz dla organizacji komercyjnych. Oznacza to, że instytucje i służby oraz prywatni użytkownicy systemu TETRA z różnych państw mogą korzystać

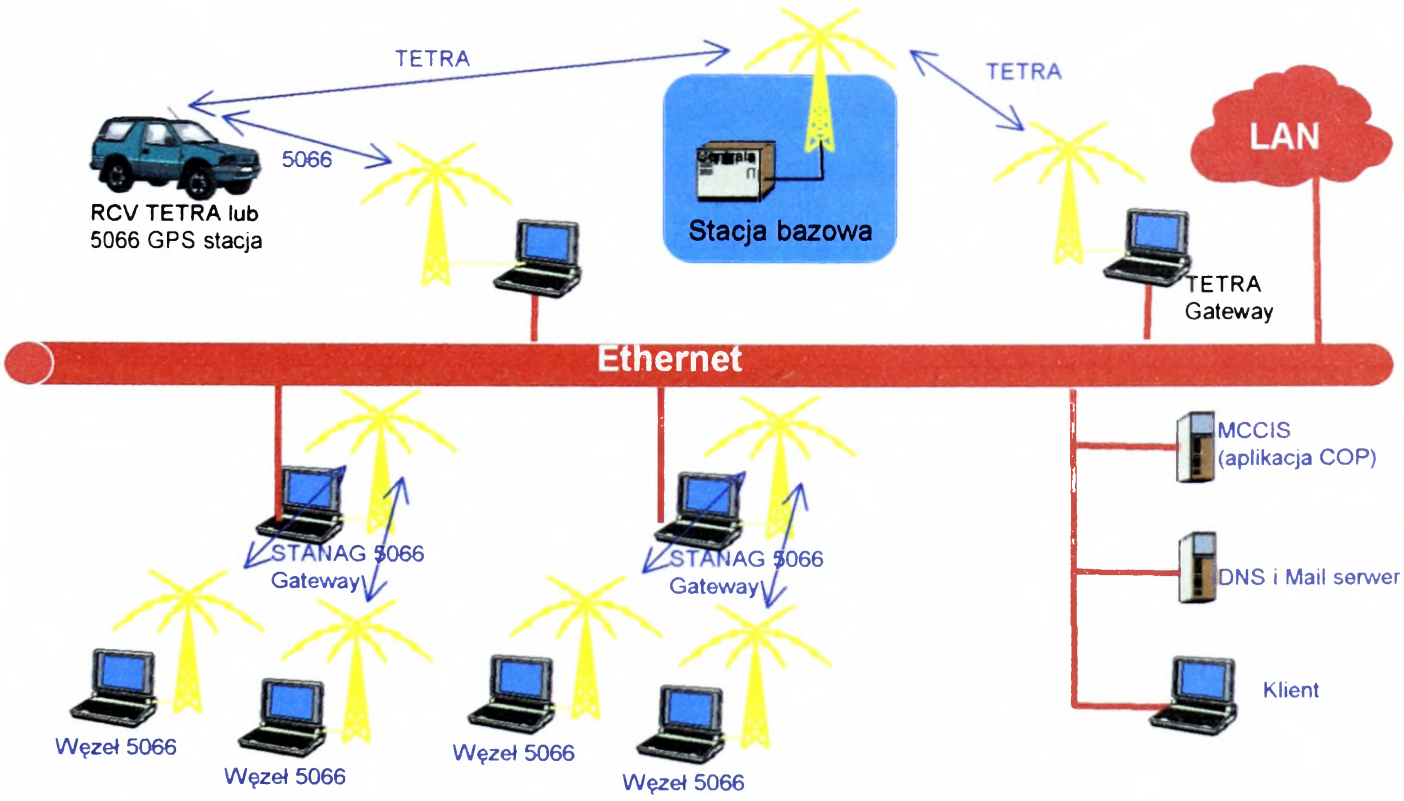
---

[137]ETSI – ang. European Telecommunication Standards Institute – Europejski Instytut Norm Telekomunikacji, utworzony z inicjatywy EWG, w celu standaryzacji rynku telekomunikacyjnego w zakresie sprzętu, sieci i usług komunikacyjnych.

opracowywana pod kątem spełnienia bardzo ostrych wymagań stawianych przez organizacje bezpieczeństwa publicznego. Natychmiastowe zestawianie połączeń, połączenia grupowe wraz z możliwością dynamicznego tworzenia grup (obejmujących w zależności od potrzeb przedstawicieli różnych służb), rozbudowane funkcje dyspozytorskie – są to przykładowe funkcje, które nie są realizowane w publicznych systemach telekomunikacyjnych. Umożliwia również integrację systemu informatycznego z systemem radiotelefonicznym standardu TETRA (realizacja zaleceń - STANAG 5066) na poziomie informatycznym (Schemat 2.5). W przypadku zniszczenia lub uszkodzenia stacjonarnej infrastruktury teletransmisyjnej umożliwia on budowę rozległych sieci komputerowych (WAN). Zastosowanie specjalizowanego adaptera telefonicznego umożliwia również wymianę informacji fonicznej jako radiowego punktu dostępowego.

Schemat 2.5.

Współpraca systemu
trankingowego TETRA z systemem łączności radiowej



Źródło: *System kierowania obronnością państwa w stanach nadzwyczajnych w kontekście wykorzystania w nim środków i systemów łączności najnowszej generacji*, Praca naukowa pod kier. M. Krauze, AON, Warszawa 2003, s. 197.

błyskawiczne zestawienie połączeń indywidualnych i grupowych, połączenia alarmowe, praca w trybie bezpośrednim, możliwość ustalania różnych priorytetów dla połączeń oraz dynamiczne tworzenie grup.

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

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

TETRA jest szczególnie przydatna w zastosowaniach na rzecz policji, straży pożarnej, pogotowia ratunkowego i wielu innych służb oraz organizacji mających na celu zapewnienie bezpieczeństwa i porządku publicznego. Rozwiązania oparte na publicznych środkach łączności nie spełniają w wystarczającym zakresie wymagań stawianych przed systemami profesjonalnymi. Tetra, jako system z założenia przeznaczona do zastosowań profesjonalnych, od początku była

w promieniu 30-300 m od punktów dostępu; dwupunktowe laserowe łącza bezprzewodowe P-P o przepływności 2÷155 Mb/s mogą operować w zasięgu kilku km (FDDI, ATM); naziemne łącza mikrofalowe o przepływności 2÷34 Mb/s działają natomiast na odległość do 90 km. Coraz większego znaczenia nabiera transmisja satelitarna, łącząca sieci szkieletowe (kręgosłupowe) MAN z sieciami globalnymi, jak też sieć VSAT służąca do bezpośredniej obsługi użytkowników w miejscach trudno dostępnych z przepływnością od 4 kb/s do 2 Mb/s.

Systemy dostępu wielokrotnego są podstawową metodą unikania konfliktów powstających podczas korzystania wielu użytkowników ze wspólnego kanału komunikacyjnego (w tym radiowego) przez stosowanie odpowiedniego protokołu dostępu wielokrotnego. Najbardziej ogólny podział radiowych protokołów bezkonfliktowych obejmuje: najstarsze protokoły ze stałym podziałem określonych zasobów transmisyjnych według wcześniej uzgodnionego planu (zwykle dla abonentów generujących ruch ciągły) oraz efektywne protokoły z dynamicznym przydziałem zasobów na żądanie i zestawianym wyłącznie na czas trwania połączenia. W łączności radiowej, także satelitarnej stosuje się dwa rodzaje protokołów dostępu: rywalizacyjne (losowe - np. szczelinowa Aloha) i rezerwacyjne (np. DAMA – ang. Demand Assigment Multiple Access).

Dynamicznego przydziału zasobów transmisyjnych można dokonywać zarówno w dziedzinach częstotliwości FDMA i czasu TDMA, jak też w dziedzinie kodów CDMA przez:

- dostęp wielokrotny z podziałem częstotliwości FDMA (ang. Frequency Division Multiple Access), polegający na podziale pasma przepustowego medium transmisyjnego na pewną liczbę rozłącznych przedziałów, tworzących kanały częstotliwościowe. Przesyłane przez medium sygnały pochodzące od różnych użytkowników są przemieszane w dziedzinie czasu, jednak widma tych sygnałów zajmują różne pasma w dziedzinie częstotliwości i dzięki temu mogą być rozdzielone za pomocą odpowiednich filtrów. Mimo więc że sygnały są przemieszane w czasie (mogą się nakładać czasowo), można je rozróżnić dzięki identyfikacji w dziedzinie częstotliwości;

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

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

Bezprzewodowa transmisja danych. Bezprzewodowa transmisja danych to dwukierunkowa sieć bezprzewodowa stosowana do transmisji danych obejmuje: bezprzewodowe sieci lokalne WLAN (Wireless LAN), dwupunktowe łącza bezprzewodowe typu P-P (ang. Point to Point) - 2÷622 Mb/s, bezprzewodowe systemy trankingowe typu TETRA, telefonię bezsznurową, systemy komunikacji osobistej PCS oraz satelitarne systemy telekomunikacyjne. Radiowe systemy komórkowe klasy GSM i DCS udostępniają zbyt małą przepływność (nie więcej niż 9,6 kb/s) na potrzeby transmisji, aby traktować je jako bezprzewodowe sieci transmisji danych.

Pierwsze rozwiązania w technologiach o podwyższonej szybkości transmisji przez sieci komórkowe zostały realizowane w technice HSCDS (ang. High Speed Circuit Switched Data) oraz technice przekazów pakietowych GPRS (ang. General Packet Radio Services) i umożliwiają zwiększenie transmisji danych (GSM) powyżej 100 kb/s (maks. 170 kb/s). Następnym krokiem przemian w kierunku trzeciej generacji systemów komórkowych stała się implementacja nowej metody modulacji i kompresji EDGE (Enhanced Data GSM Evolution) zapewniającej przekazy multimedialne z szybkością 384 kb/s (głos, dźwięk, obraz). Pierwsze aplikacje tego typu zademonstrowała (1999 r.) firma Ericsson.

Tradycyjne bezprzewodowe sieci Ethernet, wykonane w technologii podczerwieni, zapewniają przepływność w zakresie od 500 kb/s do 20 Mb/s

Małe stacje terminalowe VSAT (ang. Mery Smali Aperture Terminal) z antenami parabolicznymi i korzystające z kanałów satelitarnych w paśmie Ku 11/12/14 GHz lub paśmie C 4/6 GHz są przeznaczone do zastosowań rozsiewczych (tylko stacje odbiorcze) lub porozumiewawczych (stacje nadawczo-odbiorcze). Wyposażone w anteny paraboliczne o średnicy do 2,4 m dla pasma Ku (w paśmie C mogą być większe), pracują w trybie bezobsługowym bezpośrednio u użytkownika, zwykle na trudno dostępnym terenie lub pozbawionym wystarczającej infrastruktury telekomunikacyjnej. Maksymalna przepływność transmisji nie przekracza 2 Mb/s, najczęściej stosowana wynosi tylko 64,128 lub 256 kb/s.

Systemy VSAT odróżniają się od innych systemów satelitarnych następującymi cechami:

- pracują zwykle w zamkniętych sieciach dla określonych zastosowań;
- anteny paraboliczne VSAT są instalowane bezpośrednio u użytkownika, a ich gęstość występowania może być bardzo duża;
- są zwykle elementami sieci o topologii gwiazdy (star), składającej się ze względnie dużej stacji centralnej, zwanej stacją hub i wielu naziemnych stacji VSAT. Znane są jednak sieci o konfiguracji kraty (mesh) bez stacji centralnej ze sterowaniem rozproszonym;
- pracują w trybie bezobsługowym, zazwyczaj z monitorowaniem przez centralny ośrodek. Mogą również być wykorzystane lokalne ośrodki monitorowania i sterowania;
- wykorzystują transmisję cyfrową z szybkością nie większą niż 2 Mb/s;
- są wyposażone w nadajniki radiowe o małej mocy, a moc promieniowania musi być ograniczana, jeśli wymagają tego względy bezpieczeństwa;
- wymagają uzyskania licencji na ich stosowanie, jednak wiele administracji wprowadziło uproszczone procedury licencyjne dla użytkowników terminali VSAT.

Sieci VSAT w zależności od przeznaczenia są budowane w trzech podstawowych konfiguracjach: gwiazdy, kraty i punkt-punkt.

- 140dostęp wielokrotny z podziałem czasu TDMA (ang. Time Division Multiple Access), polegający na ustaleniu przedziałów czasowych (ramek niekoniecznie jednakowych), zwanych szczelinami, w których są umieszczane dane od różnych użytkowników. Przesyłane przez medium sygnały mają przemieszane widma, można je jednak zidentyfikować i określić ich położenie w dziedzinie czasu;
- dostęp wielokrotny z kodowym rozdziałem sygnałów CDMA (ang. Code Division Multiple Access), zapewniający każdemu użytkownikowi przez cały czas sesji pełne pasmo medium transmisyjnego, a sygnały są przemieszane zarówno w dziedzinie czasu, jak i w dziedzinie częstotliwości. W celu umożliwienia rozróżnienia poszczególnych sygnałów każdemu użytkownikowi przydziela się (na stałe lub na żądanie) odpowiedni kod pseudolosowy PNC (ang. Pseudo Noise Code), o parametrach statystycznych zbliżonych do parametrów statystycznych szumu białego. Za pomocą tego kodu sygnał ulega rozproszeniu w dziedzinie częstotliwości, upodabniając przesyłane informacje do szumu występującego w torze telekomunikacyjnym.

Dostęp satelitarny. Dostęp satelitarny VSAT jako komunikacja satelitarna należy do grupy systemów łączności globalnej użytkujących łącza satelitarne i łącza naziemne oparte na:

- naziemnych satelitarnych stacjach odbiorczych telewizji TVRO, pracujących w zakresie 11/12 GHz;
- terminalach VSAT pracujących w paśmie Ku 11/12/14 GHz lub w paśmie C 4/6 GHz;
- ruchomych naziemnych satelitarnych stacjach umożliwiających transmisję danych z niewielkimi szybkościami, pracujących w zakresie 11/12/14 GHz;
- naziemnych liniach radiowych do transmisji sygnałów cyfrowych, pracujących w zakresach 11, 14, 23, 38, 50GHz. Stacje te pracują w zakresach częstotliwości, które są przyznane wyłącznie dla specyficznych rodzajów służby lub wykorzystywane wspólnie przez wiele służb naziemnych.

łączy, naliczaniem opłat itp. W systemach o architekturze kraty terminale są wyposażone w relatywnie większe anteny i przenoszą mniejszy trafik.

W systemach typu punkt-punkt nie jest wymagana stacja centralna hubów, gdyż nie występują problemy związane z zestawieniem połączenia. Dwupunktowe łącze jest zestawiane w sposób trwały, a funkcje zarządzania i monitorowania systemu są realizowane zazwyczaj poza nim.

Dane szacunkowe wskazują, że liczba obecnie zainstalowanych na terenie kraju stacji VSAT nie przekracza 1000 terminali – przez zaledwie kilku operatorów sieci. Krajowe zapotrzebowanie na systemy VSAT ocenia się łącznie na około 8000 tysięcy terminali.

Ad. b) sieci publiczne

Publiczna sieć telefoniczna PSTN. Najstarsza, nadal jeszcze funkcjonująca infrastruktura telekomunikacyjna o charakterze publicznym PSTN (ang. Public Switched Telephone Network) jest oparta na komutacji łączy (linii telefonicznych). Podstawowa oferta usług w sieci PSTN, a obejmująca tylko automatyczną komutację kanałów rozmownych, jest stopniowo powiększana o usługi rozszerzone i dodatkowe - związane z wprowadzeniem bardziej inteligentnych cyfrowych systemów komutacji. Należą do nich:

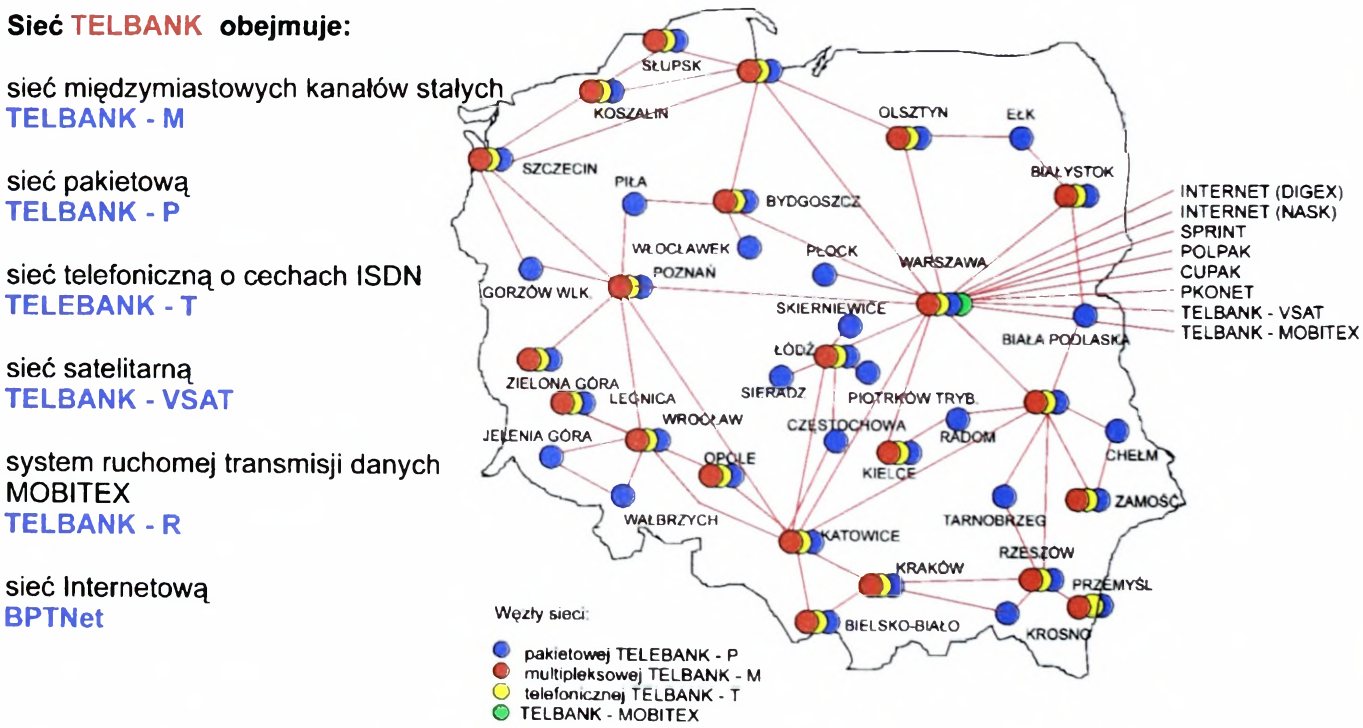
- usługi podstawowe (zestawianie połączeń za pomocą aparatów z tarczą numerową lub tonową DTMF, restrykcje zestawień, taryfikacja);
- usługi rozszerzone (rozmowy trójstronne, telekonferencje, przekierowanie rozmów, audioteks, gorąca linia, in.);
- usługi dodatkowe (poczta głosowa, poczta elektroniczna, usługa Centrex, usługi ISDN oraz usługi sieci inteligentnej IN).

Usługi podstawowe związane z transmisją głosu, funkcjonujące od czasu udostępnienia sieci publicznej głównie w centralach analogowych, nazwano usługami POTS (ang. Plain Old Telephone Srvices). Transmisje danych uparte na komutacji pakietów przeprowadza się w publicznych sieciach pakietowych PSDN.

W telekomunikacji taryfikacją określa się usługi i zdarzenia podlegające rozliczeniu, a także jednostki pomiarowe do realizacji usług i przypisane im odpowiednie wskaźniki opłat. Z taryfikacją usług są związane dwa (często mylnie identyfikowane) pojęcia: rozliczanie jako podstawowa funkcja zarządzania TMN

W systemach VSAT o architekturze gwiazdy informacja przesyłana między terminalami przechodzi przez stację centralną, tzw. hub lub stację hubów. Stacja ta jest zazwyczaj wyposażona w dużą antenę, przez co poprawia się bilans energetyczny łącza, a terminale VSAT mogą być wtedy wyposażone w mniejsze anteny i transmitować większe strumienie danych. W tego typu rozwiązaniach łatwiej jest również nadzorować pracę całego systemu oraz organizować dostęp do publicznych naziemnych systemów łączności przez stację centralną. Klasycznym przykładem wykorzystania VSAT do świadczenia szerokiego wachlarza najwyższej jakości usług telekomunikacyjnych jest Bankowe Przedsiębiorstwo Telekomunikacyjne „Telbank S.A."(Mapa 2.1.).

Mapa 2.1. Połączenia teleinformatyczne
sieci „Telbank S.A." w sieci satelitarnej VSAT (Wariant)



Źródło: Opracowanie własne: na podstawie materiałów prezentacji TPS.A.

W systemach VSAT o architekturze kraty informacja jest przesyłana bezpośrednio między terminalami (bez pośrednictwa innych stacji). W zależności od wybranego sposobu organizacji systemu jedna ze stacji (dowolnie wybrana) może pełnić funkcje stacji centralnej, ale tylko w zakresie zarządzania systemem. Zajmuje się ona zestawianiem oraz zwalnianiem łączy, monitorowaniem jakości

i poprawność odebranego pakietu przed jego dalsza ekspedycją. Ścieżki, po których są trasowane pakiety, mogą być traktowane jako:

- stałe połączenia wirtualne, utrzymujące połączenia między dwoma węzłami końcowymi, co gwarantuje odbiór pakietów w sekwencji ich nadawania;
- tymczasowe połączenia wirtualne i dostępne na żądanie, zestawiane na czas trwania sesji i likwidowane po jej zakończeniu.

Protokół Frame Relay. Urządzenia dostępu i sieć pakietowa Frame Relay, FRAD (ang. Frame Relay Access Devices) są stosowane w szybkich cyfrowych sieciach lokalnych i łączach telekomunikacyjnych. Pakietowa sieć transmisyjna z przełączaniem ramek FR dobrze funkcjonuje na łączach cyfrowych wysokiej jakości, zwykle światłowodowych, o niskiej stopie błędów i zmiennej przepływności w zakresie od 56 kb/s do 45 Mb/s.

Podstawowe kierunki zastosowań protokołu Frame Relay obejmują:

- łączenie różnego typu odległych sieci lokalnych LAN;
- przesyłanie dużych plików danych między stacjami roboczymi wysokiej rozdzielczości CAD/CAM a komputerową bazą danych przez sieci WAN;
- pracę interaktywną między terminalami o niewielkim ruchu a zasobami komputerów mainframe, zwykle z agregacją ruchu przez multipleksery statystyczne;
- komunikację interaktywną dla krótkich komunikatów z małymi opóźnieniami.

Gwałtowny rozwój technologii transmisji w ostatnim czasie spowodował, że sieć i przetaczaniem ramek FR nadaje się do przesyłania głosu (po jego uprzedniej konwersji do postaci pakietowej) w czasie rzeczywistym, czyli z niewielkimi opóźnieniami, jednak głównym zastosowaniem sieci Frame Relay jest transport pakietów danych.

W strukturze połączeń sieci FR wyróżnia się wiele fizycznych i logicznych alternatywnych dróg połączeniowych, umożliwiających tworzenie przez sieć połączeń wirtualnych, występujących w trzech postaciach:

- stałe połączenia wirtualne PVC (Permanent Virtual Circuit) przydzielane przed komunikacją na dłuższy okres (tygodnie, lata);

siecią telekomunikacyjną, które obciąża abonentów za zrealizowane usługi, oraz billing umożliwiający wystawianie rachunku dla każdego abonenta.

Rozliczanie jest podobne dla wszystkich rodzajów sieci publicznej PSTN i pakietowej PDPN i obejmuje trzy współpracujące funkcje:

- pomiar wykorzystania systemu;
- zaliczanie impulsów;
- właściwe generowanie rachunków (billing).

Niektóre numery telefonów (z grupy 900 w Polsce) nie podlegają taryfikacji w publicznych sieciach telefonicznych, inne usługi (grupa 700, grupa 800) są taryfikowane na specyficznych zasadach.

Publiczna sieć pakietowa PDN. Przekaz danych przez publiczne sieci pakietowe PDN (ang. Packet Data Network) dokonuje się w trybie pakietowym. Początkowa oferta w tych sieciach obejmowała transmisje danych z przepływnością 64 kb/s, obecnie dostęp do odpowiedniej przepływności w zakresie od 64 kb/s do 2 Mb/sjest negocjowany między abonentem a usługodawcą (telekomy).

W publicznych sieciach PDN dane w formie pakietów mogą być transmitowane przez wielu uczestników jednocześnie (każdy z każdym), zazwyczaj zapewniają one usługi bezpołączeniowe - nie zestawiające kanału komunikacyjnego przed transmisją. Sieć PDN jest tworzona z central komutacyjnych (exchange) interpretujących adresy pakietów, które przez wydzielone kanały są przesyłane do miejsca przeznaczenia. Możliwe jest tworzenie łącza logicznego - mającego w większości podobne cechy jak sieć z komutacją łączy PSTN - lecz droga przez sieć jest predefiniowana. Popularnym protokołem pakietowym jest X.25, coraz częściej zastępowany przez Frame Relay.

Protokół X.25. Standard protokołu X.25 definiuje połączenia terminali i komputerów w najprostszych sieciach pakietowych. Stosowany tradycyjnie w sieciach z komutacją pakietów o szybkości do 64 kb/s, został rozszerzony przez CCITT (1992 r.) do przepływności 2 Mb/s. W sieciach z protokołem X.25 przekaz danych następuje w trybie połączeniowym (poszczególne pakiety nie muszą zawierać adresu nadawcy i odbiorcy), a każdy węzeł sieci, dzięki rozbudowanym funkcjom kontrolnym i sterowania przepływem, sprawdza kompletność

transportowych PDN. Zastępowanie transmisji długodystansowych z protokołem X.25 przekazem pakietowym FR w kablowych sieciach miedzianych musi być poprzedzone sprawdzeniem jakości dotychczasowych łączy kablowych. Niska jakość infrastruktury kablowej może spowodować nie tylko niższą efektywność działania sieci FR w porównaniu do X.25, lecz nawet całkowicie uniemożliwić jej funkcjonowanie.

Najstarsza, działająca w Polsce od 1992 r., publiczna sieć pakietowa POLPAK (2 Mb/s) została zmodernizowana i rozszerzona pod nazwą POLPAK-T i pracuje według protokołu Frame Relay z realizacją transmisji w paśmie od 64 kb/s do 2 Mb/s na łączu abonenckim oraz 2-34 Mb/s w połączeniach międzywęzłowych.

Wirtualna sieć prywatna VPN. Koncepcja wirtualnej sieć prywatnej (VPN - ang. Virtual Private Network) - polega na wykorzystaniu zasobów sieci publicznej do zapewnienia własności funkcjonalnych sieci wydzielonej. Sieć wydzieloną można traktować jako zamkniętą grupę użytkowników zrealizowaną w sieci publicznej. Najważniejszą właściwością VPN jest rozpoznawanie prywatnego planu numeracji i jego translacja na rzeczywiste numery sieciowe.

Sieci VPN zapewniają udogodnienia sieci wydzielonych, takie jak:

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

Usługa wirtualnej sieci prywatnej może być przydatna dla potrzeb służb specjalnych i na okres stanów nadzwyczajnych ze względu na swoje unikalne właściwości. Usługa sieci prywatnych (VPN) wychodzi naprzeciw nowym potrzebom telekomunikacyjnym użytkowników współczesnych sieci telekomunikacyjnych. Rozwijane sieci prywatne charakteryzują się zwykle większymi nakładami inwestycyjnymi niż sieci publiczne oraz większymi

- komutowane połączenia wirtualne SVC (Switched Virtual Circuit);
- zestawiane na żądanie abonenta, typu punkt-punkt, analogicznie jak w sieciach telekomunikacyjnych;
- grupowe połączenia wirtualne (ang. multicast) zezwalające na równoczesny dostęp wielu użytkowników do tych samych zasobów.

Procedury komunikacyjne sieci FR uwzględniają negocjowanie wymaganej szerokości pasma przez tory światłowodowe za pomocą wskaźnika i przydziału pasma CIR (ang. Committed Information Rate), oddzielnie dla każdego połączenia wirtualnego. Sieć automatycznie kontroluje sumaryczną wartość negocjowanych wskaźników w poszczególnych łączach i węzłach sieci, wprowadzając dopuszczalne korekty (drogi alternatywne, obniżenie wskaźnika CIR, odrzucenie zgłoszenia, okresowe zawieszenie połączenia). Z uwagi na duże zdolności adaptacyjne sieć pakietowa FR jest przydatna zarówno do transmisji długich pakietów (do 4096 bajtów), jak też współpracy z najnowszą technologią ATM przez segmentację ramek, aż do wielkości pojedynczej komórki (53 bajty) standardu ATM. Funkcje kontrolne poprawności przekazu i potwierdzenia są scedowane na stacje końcowe lub węzły brzegowe sieci FR.

W porównaniu z Frame Relay połączenia w standardzie X.25 cechują się niską wydajnością sieci (dobrze spełniają swoje funkcje tylko przy niewielkim ruchu). Każdy węzeł X.25, pośredniczący w łańcuchu połączeń, przeprowadza pełną kontrolę błędów całego pakietu przed jego wysłaniem w dalszą drogę - powodując duże opóźnienia przesyłek. Protokół X.25 dobrze sprawuje się zwłaszcza w sieciach o niskiej jakości łączy.

W sieciach Frame Relay węzły identyfikują tylko adres nagłówka pakietu bez sprawdzania poprawności przesyłanych danych, nie potrzebują więc tablic stanu do sterowania przepływem przez węzły, a identyfikacją, kompletnością i retransmisją zajmują się stacje lub węzły końcowe. Dzięki temu transmisja przebiega sprawniej niż w sieciach X.25, lecz wymaga medium transmisyjnego o wysokiej jakości, zwykle światłowodowego. Szybsze sieci z transmisją pakietową FR zastępują z powodzeniem sieci pakietowe z protokołem X.25 o znacznie niższych przepływnościach, oferując, oprócz wyższej szybkości (do 45 Mb/s), większą niezawodność i elastyczne wykorzystanie istniejących zasobów

(ang. CNM – Customer Network Management) zapewnia użytkownikowi podgląd elementów bezpośrednio wpływających na działanie i wydajność sieci VPN, jak również w pewnym zakresie (przypisanym mu przez operatora sieci publicznej) sterować tymi elementami. Użytkownik VPN może stosować własne zabezpieczenia sprzętowe, lub programowe dla zapewnienia bezpieczeństwa przesyłanych danych. Bezpieczeństwo danych w sieciach VPN jest z reguły większe niż w fizycznych sieciach prywatnych. Powodem tego jest to, że znacznie trudniej jest pozyskać (podsłuchać, przechwycić) dane przesyłane w strumieniach o bardzo dużej szybkości, jak również to, że na łączach międzywęzłowych dane są kodowane (szyfrowane) przez użytkownika VPN według własnych protokołów.

Ogólnie rzecz biorąc do podstawowych zalet sieci VPN należą:

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

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

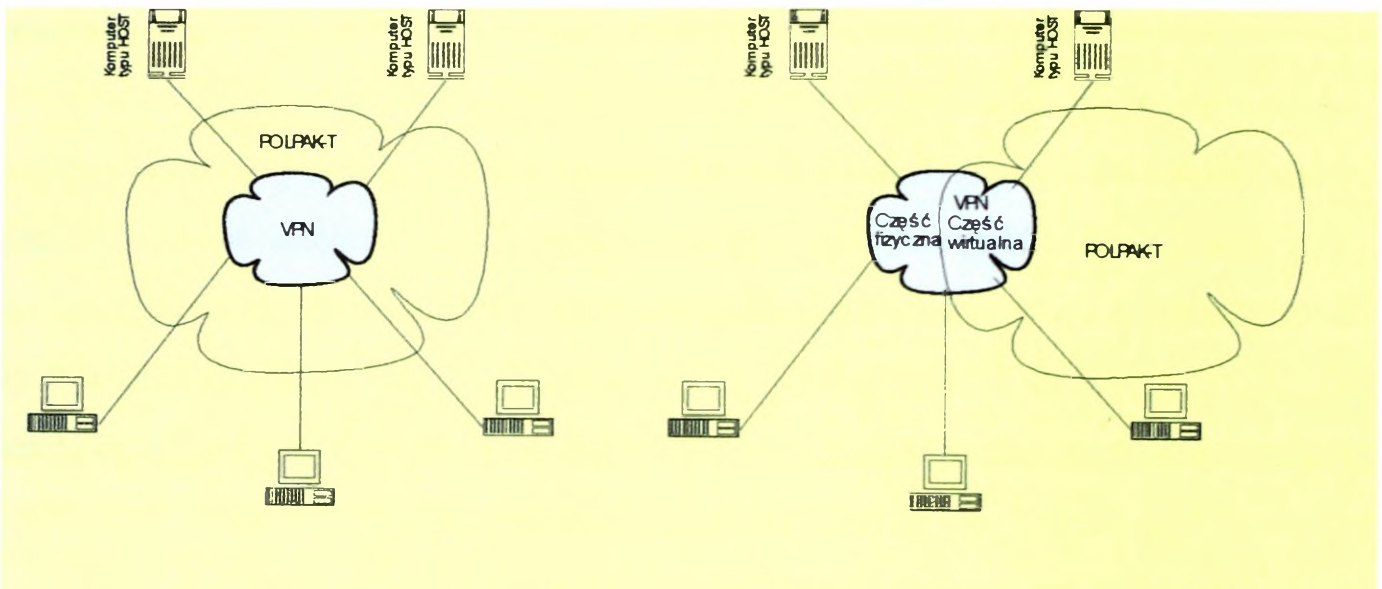
Ad. c) sieci transmisyjne

Sieci plezjochronlczne PDH. Plezjochroniczny system zwielokrotnienia (PDH - ang. Plesiochronous Digital Hierarchy) i transportu sygnałów cyfrowych, opartych na modulacji kodowo-impulsowej PCM, jest do tej pory powszechnie stosowany w telekomunikacji. Hierarchia plezjochroniczna PDH - zwana również prawie synchroniczna - określa sposób tworzenia strumienia zbiorczego 2048 kb/s z sygnałów elementarnych o podstawowej przepływności 64 kb/s oraz sposób zwielokrotnienia tych strumieni (2 Mb/s lub większych) na kolejnych poziomach multipieksacji. Ponieważ zwielokrotnione strumienie są generowane przez różne urządzenia i różnią się nieznacznie miedzy sobą przepływnością, przyjęta technika multipleksowania uzupełnia informację w przeplecie bitowym o dodatkowe pozycje zwane bitami uzupełnienia. Bity te są usuwane z sygnału w procesie demultipleksacji.

wymaganiami ich użytkowników do jakości świadczonych usług (głównie w zakresie TD) (Schemat 2.6). Z drugiej strony rozwijane nieustannie sieci publiczne cechuje z reguły większy zasięg terytorialny (np. łączność międzymiastowa, międzynarodowa) oraz używanie łączy dalekosiężnych o dużo większej szybkości transmisji. Ten fakt powoduje, że operatorzy sieci publicznych coraz częściej oferują operatorom sieci prywatnych usługi VPN.

Schemat 2.6.

Realizacja sieci VPN dla potrzeb sieci POLPAK-T (Wariant)



a/ Sieć VPN całkowicie wydzielona z zasobów sieci publicznej

a/ Sieć VPN złożona z fizycznej sieci prywatnej oraz zasobów sieci publ

Źródło: *Koncepcja wykorzystania technicznych środków łączności najnowszej generacji w systemie łączności na potrzeby sytuacji kryzysowych*, Praca naukowo-badawcza pod kier. M. Krauze, AON, Warszawa 2000, s. 55.

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

VPN pozwala w sposób logiczny powiązać linie dostępowe i terminale należące do danego użytkownika sieci. Opłaty za usługę VPN zależą przede wszystkim od stopnia wykorzystania ilości i rodzajów zasobów sieci publicznej (zwykle nie zależą od ilości przesyłanych informacji). Własny ośrodek zarządzania

Sieci synchroniczne SDH. Historycznie pierwszą synchroniczną siecią transmisyjną opartą na technice światłowodowej - przyjętą przez pocztę i działającą na terenie amerykańskim – był system SONET (ang. Synchronous Optical NETwork), określany również jako standard komunikacyjny sieci synchronicznych. Specyfikacja SONET, zaproponowana w połowie lat osiemdziesiątych przez BellCore i objęta standardem ANSI, definiuje metody transmisji danych synchronicznych i izochronicznych (wrażliwych na opóźnienia, sekwencje wideo), zapewniając współpracę na poziomie fizycznym ze światłowodowym sprzętem telekomunikacyjnym pochodzącym z różnych firm.

System SONET określa parametry kabli światłowodowych, sposób generacji światła, ramek transmisyjnych i ich multipleksacje, a przede wszystkim hierarchię różnych szybkości sygnałów optycznych, spójną w skali ogólnoświatowej. Zwielokrotnienia sygnałów optycznych w standardzie SONET uwzględniają metodykę włączania sygnałów przesyłanych z mniejszymi szybkościami (T1/E1, T3/E3) do transmisji synchronicznych SDH stosowanych w Europie. Korelacje między stykami optycznymi OC (ang. Optical Carrier), stykami elektrycznymi STS (ang. Synchronous Transport Signal) i hierarchią synchroniczną SDH zostały adaptowane do międzynarodowych standardów transportowych.

W synchronicznej hierarchii cyfrowej SDH zdefiniowano pięć poziomów zwielokrotnienia, przy czym tylko trzy najniższe mają certyfikat CCITT (ITU-T). Jako podstawową - na najniższym poziomie - przyjęto przepływność binarną 155 Mb/s (dokładnie 155 520 kb/s) dla modułu transportowego STM-1, umożliwiającą łatwą współpracę z siecią plezjochroniczną PDH o przepływności 140 Mb/s. Przepływności wyższych poziomów są wielokrotnościami poziomu podstawowego uzupełnionymi o nagłówki: STM-4 (622 Mb/s), STM-16 (2,5 Gb/s), STM-32 (5 Gb/s) i STM-64 (10 Gb/s). Przepływności oraz nazwy sygnałów (modułów) SDH odpowiadają określone oznaczenia (Tabela 2.2.).

System synchroniczny SDH (ang. Synchronous Digital Hierarchy), zastępujący stopniowo plezjochroniczne sieci transportowe PDH, umożliwia niemal nieograniczony wzrost przepływności (powyżej 10 Gb/s) w sieciach telekomunikacyjnych z zastosowaniem światłowodów. Podstawową cechą SDH jest synchroniczność przekazu, oparta na stałej ramce transmisyjnej o czasie trwania

Różne zasady zwielokrotnienia sygnałów doprowadziły do powstania wielu standardów transmisyjnych PDH, z których powszechnie stosowanymi są: japoński, amerykański i europejski. Różnią się one nie tylko przepływnością i zwielokrotnieniem na różnych poziomach, ale także organizacją przesyłanej informacji. Brak jest mechanizmów niwelujących te różnice, co utrudnia współdziałanie i podnosi koszt translacji przekazów działających w różnych standardach.

Wysokie koszty wydzielenia i wprowadzania strumieni niższego poziomu z/do wyższego stanowią kolejne ograniczenie stosowania PDH. Brak bezpośredniego dostępu do pojedynczych kanałów (64 kb/s), transmitowanych w strumieniu o dużej przepływności, wymaga praktycznie demultipleksacji wszystkich strumieni składowych oraz ich ponownego zwielokrotnienie w każdym wydzielającym węźle. Procedura taka, oprócz tego, że kosztowna, obniża niezawodność całego systemu transmisyjnego.

Inną niedogodnością systemu jest zbyt mała przepływność kanału sygnalizacyjnego, wynikająca z przyjętej struktury ramki transmitującej sygnały przez medium (30+2 szczeliny). W konsekwencji niemożliwe jest przystosowanie systemów plezjochronicznych do skutecznego i scentralizowanego zarządzania siecią, a także sprawowanie nad nią odpowiedniej kontroli. Niewielka przepływność kanału sygnalizacyjnego objawia się również ograniczeniem zdalnej rekonfiguracji sieci, prowadząc w praktyce do ręcznego krosowania torów w przełącznicach cyfrowych przy zmianie połączeń między nimi.

Istotnym ograniczeniem systemów plezjochronicznych jest też brak standaryzacji styku optycznego. Utrudnia to lub wręcz uniemożliwia powszechne stosowanie torów światłowodowych pochodzących od różnych producentów, a połączenie ze sobą dwóch systemów optycznych wymaga dokonania podwójnej konwersji optyczno-elektrycznej i realizacji połączenia na poziomie sygnału elektrycznego. Ograniczenia systemów teletransmisyjnych opartych na plezjochronicznej hierarchii cyfrowej spowodowały, że od 1996 r. nowe PDH nie są już i praktycznie instalowane. Równocześnie następuje szybki wzrost najnowszej cyfrowej transmisji synchronicznej objętej międzynarodowym standardem SDH, bez wad i ograniczeń występujących w PDH.

kontenerów VC wyższego rzędu. W drugim zachodzi łączenie kontenerów wirtualnych VC z nagłówkiem sekcji SOH (Section Overhead) w celu utworzenia modułów transportowych STM (Synchronous Transport Module) o wymaganej przepływności dla strumienia zbiorczego. Inaczej niż w systemach PDH - bezpośrednio zwielokrotniających z przeplotem bitowym -w technologii SDH przesyłana informacja ulega przetworzeniu (uzupełnieniu o nagłówki ramek), a następnie zwielokrotnieniu z przeplotem bajtowym sygnałów składowych. Wielkość przepływności sygnałów składowych jest w tym przypadku nieistotna, a wydzielenie strumienia o dowolnej przepływności możliwe w każdym węźle transportowym.

Sieci asynchroniczne ATM. Asynchroniczna i szerokopasmowa technologia komunikacyjna ATM (ang. Asynchronous Transfer Modę) jest przeznaczona do przesyłania usług multimedialnych (głosu, dźwięku, obrazu, danych) i przyjęta jako technika transmisji w szerokopasmowych sieciach transportowych BISDN. Technika ATM łączy zalety transmisji synchronicznej STM (ang. Synchronous Transfer Mode) i transmisji pakietowej PTM (ang. Packet Transfer Mode), eliminując większość wad każdego z tych systemów.

Uniwersalność tej technologii polega na możliwościach:

- przesyłania stałych porcji informacji o pojemności 53 bajty (w tym 48 bajtów informacji użytecznej), co ułatwia proces ich obróbki w węzłach sieci ATM;
- ustalania indywidualnych połączeń o dowolnej szybkości w obrębie przyjętych lub istniejących standardów (25 Mb/s, 100 Mb/s, 155 Mb/s, 622 Mb/s, 2500 Mb/s), dzięki przyporządkowaniu dowolnej liczby komórek do konkretnego połączenia użytkownika;
- obsługi transmisji izochronicznych (głos, obraz, HDTV) z opóźnieniem nie większym niż 10 ms, przez zastosowanie przełączników ATM z szybkim sprzętowym przełączaniem komórek i połączeń;
- skalowania przepływności ścieżek i węzłów ATM, dzięki czemu wykorzystuje się w pełni maksymalną przepływność dowolnego medium transportowego, w tym wysoką przepływność torów światłowodowych w sieciach LAN i WAN;

Tabela 2.2. Przepływności oraz nazwy sygnałów (modułów) SDH

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

* - standardy są w przygotowaniu

Źródło: *Kierowanie obronnością państwa w stanach nadzwyczajnych*, Praca naukowa pod kier. M. Krauze, AON, Warszawa 2000, s. 147.

125 :s, która jest generowana współbieżnie z głównym zegarem systemu, tzw. pierwotnym zegarem odniesienia PRC (ang. Primary Reference Clock).Ograniczona stabilność taktujących zegarów kwarcowych (stałość 10^{-11}) oraz zmienne własności nośników optycznych mogą wprowadzać niewielkie, stałe lub zmienne nie kontrolowane przesunięcia fazowe w węźle odbiorczym (w stosunku do źródła sygnału). Kompensacja tych poślizgów dokonuje się automatycznie przez wprowadzenie metody wyrównywania fazy odbieranego sygnału za pomocą znaczników AU przyporządkowanych do kontenera wirtualnego VC - wskazujących nie tylko położenie ramki w przestrzeni adresowej kontenera, ale także względne przesunięcie ramki (dodatnie, zerowe lub ujemne) w stosunku do znacznika. Przyjęta struktura ramek i zastosowanie mechanizmu wskaźnika AU znajdującego się w nagłówkach kolejnych kontenerów pozwalają na bezpośrednie wydzielenie lub łączenie w sygnał zbiorczy strumieni składowych na różnych poziomach zwielokrotnienia. Nie jest potrzebna w tym przypadku kosztowna demultipleksacja (lub multipleksacja) wszystkich pozostałych strumieni składowych do wydzielenia lub translacji pojedynczego strumienia danych.

Proces zwielokrotnienia przebiega dwuetapowo. W pierwszym etapie następuje multipleksacja kontenerów wirtualnych VC niższego rzędu do

retransmisji i powtórzeń, ale wykorzystując media o bardzo dobrej jakości, jest szybką i nowoczesną siecią transportową.

Sieci skalowalne DTM. Technologia dynamicznego skalowania przepływności sieci transportowej DTM (ang. Dynamic Synchronous Transfer Mode) jest najnowszą wersją szerokopasmowego i synchronicznego przekazu multimedialnego działającego w czasie rzeczywistym, zarówno w sieciach transportowych, jak i bezpośrednio w otoczeniu abonenta. Dzięki unikatowemu sposobowi przełączania o bardzo dużej i dynamicznie skalowanej przepływności, w zakresie od 512 kb/s do 2,5 Gb/s, technologia ta zastępuje nie tylko sieci telekomunikacyjne z komutacją kanałów (np. ISDN), ale i łącza komunikacyjne z transmisją pakietową.

Technologia DTM łączy w sobie - unikając wad - najlepsze cechy asynchronicznej technologii ATM opartej na przełączaniu komórek (stała długość komórek, wirtualizacja połączeń, dostępność pasma na żądanie, przekazy izochroniczne) z zaletami przełączania kanałów (gwarancja stałego poziomu usług przez alokację odpowiedniej liczby kanałów cyfrowych, prosta izolacja wielu usług), uzyskiwanych w takiej technologii jak sieć cyfrowa ISDN.

Technologia dynamicznego skalowania, zaprojektowana pierwotnie do efektywnego korzystania z infrastruktury sieci IP (ang. Internet Protocol), stała się przydatna do kreowania innych usług multimedialnych, ważnych z punktu widzenia pracy w czasie rzeczywistym (również dla IP), umożliwiając równoczesną pracę przez jeden kanał wielu użytkownikom sieci. W systemie DTM całkowita pojemność transmisyjna kanału światłowodowego jest podzielona na segmenty czasowe (slots), każdy o długości 125 μs, które dalej są dzielone na 64-bitowe ramki. Liczba tych ramek, przypadająca na konkretny segment (odcinek czasowy) światłowodu między kolejnymi węzłami sieci świadczy o szerokości dostępnego pasma między tymi węzłami (typowo 4800 ramek w kanale o przepustowości 2,5 Gb/s). Przyjęta długość pojedynczego segmentu (125 μs), także wielkość bitowa ramki (64 bity) umożliwiają stosunkowo prostą konwersję sygnałów operujących w odmiennych technologiach, takich jak SDH (SONET) czy ISDN.

- stosowania multipleksacji statystycznej poszczególnych kanałów, co pozwala na efektywne gospodarowanie pasmem łącza transmisyjnego;
- tworzenia przekazów głównie w trybie połączeniowym, co oznacza, że przed wysłaniem informacji właściwej występuje faza zestawienia łącza - według parametrów deklarowanych przez abonenta (typ usługi, przewidywana przepływność, deklarowany adres), a po zakończeniu przekazu -jego likwidację;
- tworzenia wirtualnych połączeń przez sieć zarówno dla pojedynczych kanałów, jak i definiowanych grup kanałów zwanych ścieżkami. Jest to możliwe dzięki istnieniu odpowiednich identyfikatorów VCI (ang. Virtual Channel Identifier) dla kanałów oraz identyfikatorów VPI (ang. Virtual Path Identifier) dla ścieżek wirtualnych. Pola tych identyfikatorów znajdują się w nagłówku każdej komórki ATM przesyłanej przez sieć;
- adaptacji strumienia komórek ATM do dowolnej przepływności medium transportowego, przez wprowadzanie komórek pustych, pomijanych w węźle docelowym;
- przypisania komórkom ATM (kanałowi, ścieżce, połączeniu między użytkownikami) konkretnej usługi, której parametry mogą być dynamicznie zmieniane zarówno w fazie nawiązywania łącza, jak i w trakcie działania usługi komunikacyjnej;
- zapewniania „przezroczystości" przenoszenia informacji przez sieć ATM, a więc dostosowanie pracy sieci z różnymi protokołami komunikacyjnymi i do realizacji różnych usług.

Duża szybkość multipleksowania portów i strumieni w rozbudowanych przełącznikach ATM klasy high-end, sięgająca 40 Gb/s (znane są już rozwiązania działające z szybkością 160 Gb/s), wynika ze sprzętowej realizacji procesu przełączania opartego na dynamicznie wymienianych tablicach routingu, przekazywanymi kanałami sygnalizacyjnymi ATM. Dla optymalizacji szybkości przekazu komórek przełączniki ATM nie mają warstwy sieciowej modelu odniesienia OSI, nie prowadzą kontroli błędów transmisyjnych, a stacja odbiorcza sama musi sprawdzić, czy odebrany przekaz jest kompletny i poprawny. Sieć ATM, inaczej niż sieć X.25, nie odpowiada za błędnie przesłane komórki, nie inicjuje

wyszukiwanie, język HTML, protokół HTTP), komunikację (poczta elektroniczna, MIME) i aplikacje (klient-serwer, CORBA, Java).

Telefonia internetowa IP. Telefonia IP stanowi nową technologię przekazów głosowych, polegającą na integracji telefonii CTI z Internetem, intranetem, ekstranetem bądź innymi sieciami za pomocą protokołu IP (Internet Protocol). W konsekwencji mamy do czynienia z telefonią IP (IP Telephony), nazywaną inaczej telefonią internetowa. Telefonia IP realizuje usługi telefoniczne przez sieci pracujące z protokołem IP, przy czym połączenia telefoniczne mogą odbywać się w relacji: komputer PC - komputer PC, komputer PC - telefon oraz telefon - telefon, ze znacznie niższymi opłatami taryfikacyjnymi niż w tradycyjnej telefonii długodystansowej.

Wyposażenie niezbędne do modernizacji urządzeń terminalowych (komputerów PC) określa norma H323 (najnowsza wersja z 1998 r.), natomiast sam komputer jest traktowany przez oprogramowanie jako oprogramowanie klienta. Specyfikacja H.323 definiuje cztery podzespoły architektury przekazu głosowego VoIP (Voice overIP) w sieciach wspieranych protokołem IP, a więc w sieciach internetowych, intranetowych i ekstranetowych, obejmujące:

- terminale, zwykle klasy PC, dysponujące oprogramowaniem typu klient zgodnym z normą H.323 (kodek audio, cyfryzacja, kodowanie, kompresja wejściowa i operacje w odwrotnym kierunku na wyjściu);
- bramki PSTN/IP, stosowane w sytuacjach, gdy użytkownicy komunikują się przez sieci inne niż pakietowe (komutowane bądź ISDN PRI/BRI);
- bramki Gatekeeper, spełniającej funkcję kontrolną nad połączeniami (translacja adresów, identyfikacja terminali w sieci, kontrolowanie szerokości pasma, kontrola dostępu przez odrzucanie wywołań z terminali nieupoważnionych);
- wielopunktowy serwer konferencyjny, wspierający połączenia głosowo-obrazowe w sesjach typu multicast lub unicast.

Połączenia głosowe oraz przesyłanie faksów dokonuje się w trybie czasu rzeczywistego lub technologii „zapamiętaj i prześlij". Przesyłanie danych przez łącza komutowane, także przez linie dzierżawione publicznej sieci telefonicznej PSTN i sieci z komutacją pakietów (Internet/intranet, LAN, X.25) wymaga

W razie niedoboru pasma protokoły komunikacyjne tej technologii, lokowane w węzłach sieci, potrafią jednak łączyć poszczególne kanały optyczne (Xn) systemu zwielokrotnienia DWDM, dostarczając w ten sposób jedno spójne pasmo transmisyjne o przepływności rzędu dziesiątków lub setek gigabitów w ciągu sekundy. Takie przepływności, jakie są potrzebne w sieciach transportowych.

Dzięki olbrzymiej elastyczności sieć telekomunikacyjną wykonaną w technologii DTM można traktować zarówno jako multimedialną sieć dostępową (np. sieć abonencką o klasycznej szybkości 50 Mb/s) do komunikacji między aplikacjami, jak też jako transportową (ang. carrier network) - o cechach zbliżonych do technologii sieciowych klasy ATM (2,5-10 Gb/s).

Ad. d) sieć globalna Internet

Internet **-** nazwa sieci globalnej operującej protokołem IP (ang. Internet Protocol), łączącej rozsiane po świecie lokalne komputery agencji i instytucji edukacyjnych, badawczych, rządowych, przemysłowych i prywatnych, a także serwery webowe; również usługi świadczone przez te sieci. Współczesny Internet stanowi konglomerat wzajemnie połączonych i komunikujących się podsieci, oraz niezliczonych serwerów webowych pajęczyny WWW (World Wide Web), wykorzystujących zestaw protokołów sieciowych określanych skrótem TCP/IP. Środowisko, szczegółowe funkcje i usługi dostępne w Internecie - bardziej zbliżone do systemów komputerowych niż telekomunikacyjnych.

Intranet. Współczesne rozwiązanie funkcji sieci Internetu, działające w zakresie sieci LAN i obejmujące swym zasięgiem ograniczony obszar (biuro, pojedynczy zakład, grupę przedsiębiorstw), nazwano intranetem. Elementy intranetu oparte głównie na protokole TCP/IP obejmują: sieć LAN (lub najwyżej MAN), prywatne serwery webowe i zakładowe, lokalne przeglądarki, a także współpracę z komputerem mainframe. Bezpieczne połączenie intranetu z Internetem wymaga stosowania zapory ogniowej (ang. firewall). Istotą intranetu są prywatne serwery webowe i lokalne przeglądarki (ang. browsers) współpracujące ze sobą za pośrednictwem protokołu komunikacyjnego TCP/IP w obrębie sieci lokalnej. Wśród wielu prowadzonych klasyfikacji intranetowych zwraca uwagę podział według zastosowań, obejmujący: publikacje (strony webowe,

sieciowy system plików NFS – ang. Network File System). Dotychczas najbardziej popularną usługą jest WWW (World Wide Web). Sieć Internet funkcjonuje w oparciu o pakiet protokołów TCP/IP (transmisja datagramowa – bezpołączeniowa). Filozofia TCP/IP jest antytezą filozofii ISO/OSI (Model referencyjny OSI), lecz ze względu na swoją popularność TCP/IP stanowi praktycznie podstawę wszystkich sieci działających w oparciu o system operacyjny UNIX. W TCP/IP protokoły są bardzo proste i gdy pojawia się konieczność rozbudowy sieci dodawane są nowe protokoły.

Najważniejsze protokoły TCP/IP obejmują:

- IP – ang. Internet Protocol;
- ICMP – ang. Internet Control Message Protocol;
- UDP – ang. User Datagram Protocol;
- TCP – ang. Transmission Control Protocol.

Inne protokoły poszerzające możliwości sieci to:

- SMTP – wersja poczty elektronicznej na bazie TCP/IP;
- Telnet – umożliwiający tworzenie wirtualnego terminala sieciowego;
- FTP (ang. File Transfer Protocol) – korzystanie z zasobów sieci.

Aktualnie wykorzystywany w Internet zestaw protokołów TCP/IP nie nadaje się do transportu strumieni danych multimedialnych. W standardowym protokole IP wyróżnia się dwa rodzaje pakietów: „unicast" (adresowanych do jednego ściśle określonego odbiorcy) i „broadcast" (docierające do wszystkich komputerów w obrębie jednej sieci lokalnej). Z chwilą, gdy pojawiło się zapotrzebowanie na usługi przesyłania dźwięku i obrazu w Internet pojawiła się również potrzeba przesyłania pakietów multicasingowych. O ile już w protokole IP stworzonym na początku lat 70-tych dopuszczano adresacje multicastową, to istniejące aplikacje, jak również stosowane routery pozwalały na jej stosowanie tylko w obrębie sieci lokalnych (lub wykorzystując pakowanie jej w zwykłe pakiety tworzenie w sieci rozległej „wysp multicastowych").

Sieć Internet jest ciągle rozwijana. Jej możliwości gwarantują wysoką pozycję wśród sieci dostępowych z integracją usług i powodują, że może stanowić poważną konkurencję dla innych rozwiązań. Można stwierdzić, że cechą, która będzie stanowić o dalszej popularności Internet w przyszłości, będzie dostępność

stosowania bramki telefonicznej (ang. phone gateway) umieszczanej przy sieciowym systemie komutacji, zwykle w/obok prywatnej centrali abonenckiej PABX. Zalety i wady telefonii IP są porównywalne. Do zalet można zliczyć:

- dziesięciokrotnie lepsze wykorzystanie pasma dla transmisji głosowych przeprowadzanych w trybie czasu rzeczywistego;
- oszczędność do 40 proc. kosztów przesyłania faksów;
- bezpośrednia łączność abonenta ze strony WWW z przedstawicielem handlowym - bez konieczności przerywania własnej sesji komputerowej.

Natomiast wady to:

- jakość głosu jest niższa niż w tradycyjnej telefonii przewodowej;
- możliwość pojawienia się problemów związanych z gubieniem pakietów;
- konieczność instalacji przez dostawców urządzeń zdolnych do przeprowadzania jednocześnie setek lub tysięcy rozmów;
- brak obowiązujących standardów dla współdziałania urządzeń pochodzących od różnych producentów.

Bramka PSTN/IP (ang. gateway) jest kluczowym elementem głosowej komunikacji internetowej, umożliwiającym właściwą konwergencję dwóch rodzajów sieci i odmiennych przekazów (głos, dane). Spełnia ona kilka istotnych funkcji:

- przeformatowanie transmitowanej informacji (np. ze stacji H.323 protokołu IP do analogowej stacji telefonicznej i odwrotnie);
- kompresję głosu (z PCM 64/G.711/ na format G.723 lub inny);
- translację procedur nawiązywania, utrzymania i rozłączania połączeń (obligatoryjna sygnalizacja H.225.0 od strony sieci lokalnej, oparta na Q.931, i sygnalizacja telefoniczna z drugiej strony).

Internet jest obecnie największą na świecie siecią transmisji danych (TD). Jej protoplastą była sieć Arpanet łącząca liczne ośrodki wojskowe, przemysłowe i uniwersyteckie w USA. Wkrótce sieć, z uwagi na jej zalety, rozszerzyła się na cały świat. Stworzono olbrzymią ilość, specjalnie dla niej stworzonego, oprogramowania, w tym aplikacje stosowane w sieciach rozległych, umożliwiające zdalną pracę na komputerach dużej mocy, dostęp do różnorodnych baz danych, transmitowania plików oraz aplikacje stosowane głównie w sieciach lokalnych (np.

w dalszych kierunkach rozwoju światowej telekomunikacji. Program umożliwia przesyłanie obrazów z maksymalną szybkością do 30 klatek/sekundę (przy wymaganej przepustowości rzędu 1,5 Mb/s). Program umożliwia również przesyłanie dowolnych okien X-Windows. Do transmisji Video używane są również inne programy np.: IVS (INRIA Videoconferencing System) – niekompatybilny z NV oraz VIC (obsługujący obydwa formaty NV i IVS).

Wyżej wymienione aplikacje z uwagi na to, że są rozwijane głównie dla różnych wersji systemu UNIX, nie zdobyły wielkiej popularności w środowisku użytkowników komercyjnych (korzystających z systemu MS-DOS. Dla tych użytkowników zostały opracowane aplikacje (nie pracujące jednak pod systemem UNIX):

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

Ad. e) systemy telefonii komórkowej

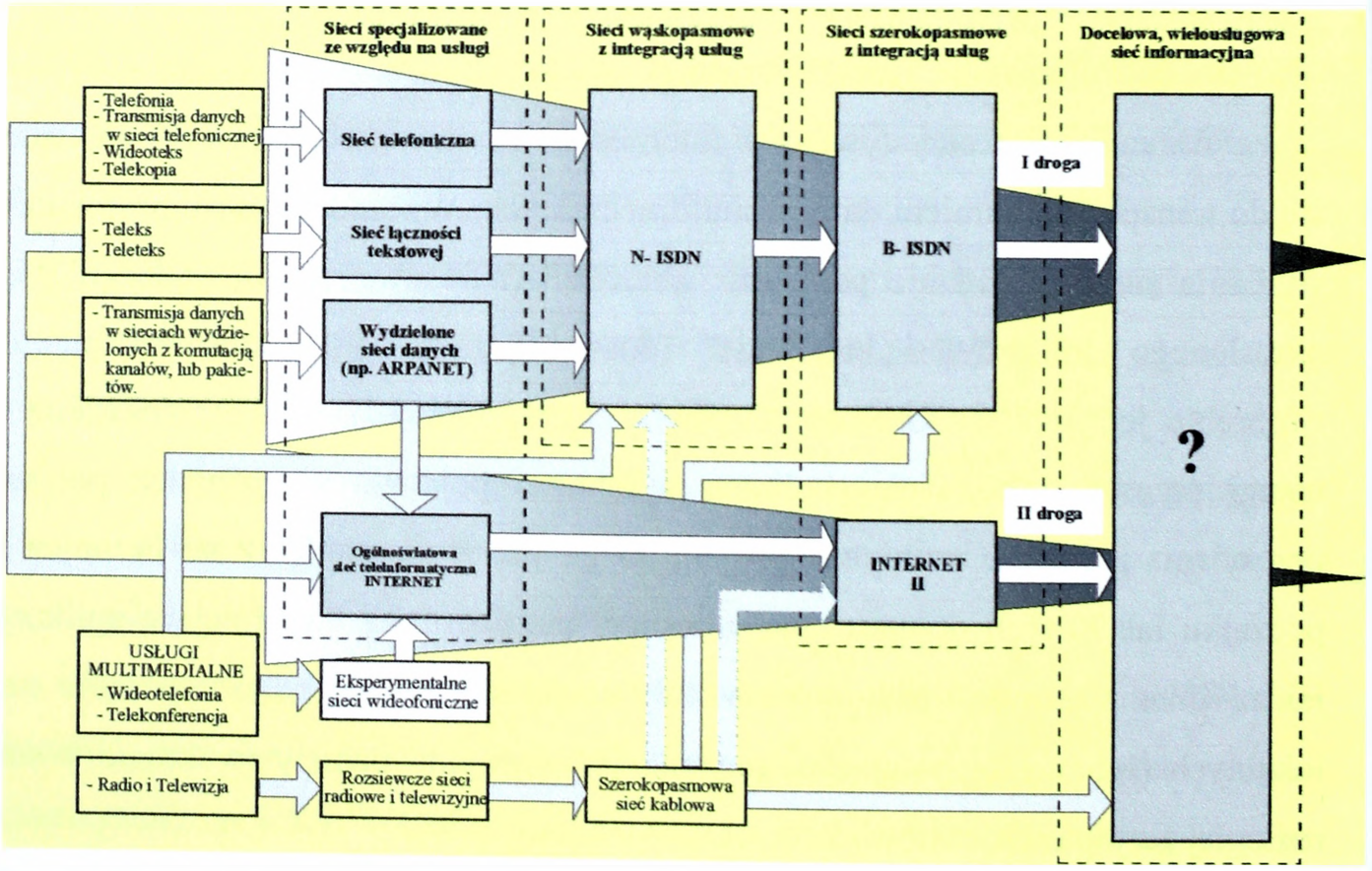
Rozwój radiokomunikacji ruchomej jest związany z łącznością typu komórkowego, przeznaczoną do obsługi abonentów ruchomych i stacjonarnych zarówno w systemach analogowych - opartych na emisji analogowych sygnałów radiowych, jak i bardziej nowoczesnych systemach cyfrowych (cyfrowy przekaz głosu i danych).

Wśród systemów komórkowych pierwszej generacji (analogowych) najbardziej znanymi są: amerykański system AMPS (ang. Advanced Mobile Phone System), jego europejska wersja TACS (ang. Total Access Communication System), skandynawski system NMT (ang. Nordic Mobile Telephony), francuski R2000 i niemiecki C-450. Systemy analogowe są zwykle wzajemnie niekompatybilne, nawet na obszarze tego samego kraju.

w niej usług multimedialnych (np. radio, telefon, telewizja rozsiewcza, wideokonferencja itp.). W Internet wykorzystywane są trzy grupy oprogramowania umożliwiające przekazywanie dźwięku oraz video: oprogramowanie telekonferencyjne umożliwiające przekazywanie dźwięku i obrazu równocześnie pomiędzy wieloma użytkownikami sieci. Aktualnie niepisany standard tworzą dźwięki zbliżone do jakości sygnałów radiowych zakresu fal AM (pasmo 4 kHz) oraz dwie aplikacje multicastingowe korzystające z protokołu RTP: VAT - Visual Audio Tool. Przesyłane sygnały podlegają procesom kompresji i dekompresji. Jakość przesyłanego NV - Network Video to typowa szybkość transmisji 128 kb/s umożliwia przesyłanie 3 do 5 klatek/sekundę obrazu zakodowanego w systemie PAL (384x240 pikseli), lub NTSC (320x240 pikseli). Obecnie rozwijana jest nowa wersja sieci Internet – tzw. Internet II, w którym wykorzystuje się łącza międzywęzłowe o bardzo dużych przepustowościach (rzędu 2 Gb/s) (Schemat 2.7.).

Schemat 2.7.

Rozwój sieci Internet w ogólnej ewolucji sieci telekomunikacyjnych



Źródło: Opracowanie własne na podstawie: *Net World, Vademecum teleinformatyka cz. 1, 2,3,* International Data Group Poland S.A., Warszawa 2004.

Zakłada się, że będzie on stanowił poważną konkurencję dla tradycyjnych zintegrowanych sieci szerokopasmowych i może spowodować rewolucję

odbioru sygnałów jest wielodrogowość informacji, wynikająca z załamań i odbić sygnałów od płaszczyzn i ścian budynków na terenie zurbanizowanym.

W zależności od potrzeb obszary o szczególnie wysokim trafiku są umownie dzielone na 2-3 poziomy obejmujące:

- makrokomórki - obszary o promieniu od 1 do 20 km obejmujące tereny leżące poza miastami, o niewielkich skupiskach ludności, a także szybko przemieszczających się abonentów (ulice, drogi, autostrady);
- mikrokomórki - obszary o promieniu od 100 m o 1 km obejmujące głównie tereny miejskie, osiedla i duże skupiska ludności, przeznaczone dla pieszych lub prawie stacjonarnych użytkowników systemu, zwykle znajdujących się w terenie otwartym (tereny rekreacyjne, stadiony);
- pikokomórki - o promieniu poniżej 100 m stosowane głównie wewnątrz obiektów (budynki, biura, domy towarowe, dworce i lotniska) o szczególnym zagęszczeniu terminali aktywnych na tym obszarze.

System komórkowy, wykorzystując wieloparametrowe procedury lokalizacyjne, automatycznie ocenia mobilność każdego aktywnego abonenta i przyporządkowuje go do właściwego, optymalnego obszaru komórkowego. W zaawansowanych systemach komórkowych (faza 2+) przewiduje się wielopoziomowe trasowanie połączeń z wykorzystaniem makrokomórek i mikrokomórek przyporządkowanych do różnych systemów.

W celu uzyskania optymalnego zasięgu poprawnego odbioru, w sieci komórkowej stosuje się wiele metod korekcyjnych, przeciwdziałających szkodliwym działaniom interferencyjnym i anizotropowej propagacji pola radiowego. Podstawowym kryterium jest właściwy dobór częstotliwości nośnych poszczególnych stacji bazowych w bezpośrednim sąsiedztwie każdego obszaru komórkowego, tak aby interferencje międzykanałowe były minimalne. Powszechnie jest stosowana metoda otaczania każdej komórki jednym pierścieniem komórek lub wieloma pierścieniami o nie powtarzających się częstotliwościach kanałowych.

Analogowa telefonia komórkowa. System NMT (ang. Nordic Mobile Telephony) to skandynawski standard analogowego systemu komórkowego, rozwijany w krajach europejskich od końca lat siedemdziesiątych. W pierwotnej wersji NMT 450 wykorzystano zakres częstotliwości 450 MHz, z liczbą kanałów

Wprowadzenie znormalizowanych systemów cyfrowych drugiej generacji (GSM/DCS) o zasięgu globalnym usuwa tę podstawową niedogodność dla abonenta, zmniejszając równocześnie zakres zajmowanego pasma częstotliwości. Systemy cyfrowe klasy GSM są oznaczone i normalizowane re-gionalnie: w Europie jako GSM 900 w paśmie 900 MHz oraz GSM 1800 (DCS 1800) w paśmie 1800 MHz, w Ameryce Północnej D-AMPS (ang. Digital AMPS) oraz nowszy PCS1900 (ang. Personal Communication System), w Japonii PDC (ang. Personal Digital Communication).

Dwie istotne cechy odróżniają systemy telefonii komórkowej od innych bezprzewodowych systemów łączności radiowej:

- komórkowa struktura sieci - składa się ona z komórek radiowych, każda jest obsługiwana przez swoja stację bazową. Komórki radiowe są różnej wielkości: małe komórki występują na obszarach o dużym skupieniu abonentów, a tam gdzie abonentów jest niewielu - komórki są duże. Wielkości komórek, ich rozmieszczenie, kształt i liczba na danym obszarze mogą ulegać zmianom.;
- ciągła aktualizacja (bieżąca i okresowa) stanu aktywnych aparatów komórkowych znajdujących się w zasięgu stacji bazowej, mająca na celu lokalizację przemieszczających się abonentów obsługiwanych przez sieć. Lokalizacja następuje automatycznie przy inicjowaniu każdego połączenia lub okresowo, a podczas przemieszczania się abonenta z jednej komórki dci drugiej (w tej samej sieci) zachodzi zdalne przestrajanie kanałów radiowych - bez utraty lub przerwania prowadzonej łączności.

Koncepcja komunikacji radiowej opiera się na podziale całego obszaru na komórki, o kształcie wieloboku heksagonalnego, w których jest centralnie umieszczona nieruchoma stacja bazowa do obsługi użytkowników ruchomych w obrębie komórki. W warunkach rzeczywistych heksagonalny kształt komórek jest daleki od idealnego, również rozkład pola w zasięgu stacji bazowych nie jest jednorodny i zależy od charakteru zabudowy, konfiguracji ulic, wysokości budynków i ukształtowania terenu. Dodatkowym czynnikiem pogarszającym jakość

wymaga zarówno lokalizacji położenia terminali, jak też identyfikacji abonenta i terminalu końcowego oraz właściwej taryfikacji za wykonywane usługi.

Utrzymanie nie zakłóconej transmisji przez najlepsze, aktualnie dostępne kanały radiowe w obrębie stacji bazowej BS, a także korzystanie z sąsiednich komórek radiowych tej samej sieci są możliwe dzięki procedurze przełączania handover, funkcjonującej w zasięgu konkretnej sieci komórkowej. Łączność między sieciami komórkowymi innych operatorów, także poza obszarem obsługiwanym przez macierzystą sieć komórkową (rozmowy międzynarodowe), wymaga korzystania z usługi roamingu - uzgodnionej między operatorami różnych sieci. Poufność przekazów (karta SIM, szyfrowanie, identyfikacja) jest w pełni zapewniona tylko w systemach cyfrowych o znacznie większych możliwościach obsługi, lepszej jakości połączeń i szerszym zakresie usług dodatkowych.

System GSM 900. Cyfrowy system ruchomej łączności komórkowej GSM (ang. Global System for Mobile Communication) został znormalizowany w swojej końcowej formie przez ETSI jako GSM 900 w paśmie częstotliwości 900 MHz. Systemy komunikacyjne oparte na standardzie GSM (także DCS) charakteryzują się lepszą jakością przekazu mowy niż systemy analogowe NMT, są przystosowane do transmisji danych, transmisji faksowej, przesyłania i rozgłaszania krótkich komunikatów SMS (ang. Short Message System), wywoływania indywidualnych abonentów oraz zapewniają współpracę z ruchomymi i stacjonarnymi sieciami wszystkich typów.

Do realizacji systemów zastosowano najnowocześniejsze osiągnięcia techniki cyfrowej: efektywne kodowanie mowy (6,5 kb/s, 13 kb/s), kombinowaną technikę zwielokrotnienia i dostępu FDMA/TDMA, emisję z rozproszonym widmem CDMA-FH, modulację GMSK oraz programowaną regulację mocy nadajników (zwykle tylko w terminalach ruchomych). Zmniejszanie mocy przy zbliżaniu się stacji ruchomej do stacji bazowej jest wskazane w celu ograniczenia poziomu interferencji w kanale radiowym i zmniejszenia wzajemnego oddziaływania na inne kanały rozmowne, natomiast zwiększanie mocy nadajników terminali ruchomych i stacji stacjonarnych jest niezbędne przy oddalaniu się abonentów - w celu utrzymania jak największego zasięgu sieci.

ok. 200, co przy dużej popularności systemu było przyczyną jego niewydolności na obszarach o większej gęstości abonentów. Kolejne modernizacje spowodowały powstanie wielu niekompatybilnych wersji; najnowsza ujednolicona wersja NMT 900 pracuje w zakresie 900 MHz, z obsługą do 1000 kanałów podstawowych i 999 kanałów połówkowych (12,5 kHz). Standard NMT 450 (zmodernizowany jako NMT 450i) stał się popularny w krajach europejskich, jest dopuszczony również do użytkowania w Polsce.

Telefonia analogowa w Polsce. Realizowana w Polsce od 1991 r. sieć komórkowa, nazwana Centertel i oparta na skandynawskim NMT 450, obejmuje prawie 95% powierzchni kraju. Z usług pierwszej krajowej telefonii komórkowej Centertel, realizowanych za pomocą 4 central MTX zlokalizowanych w Warszawie, Gdańsku, Katowicach i Poznaniu. Mała liczba kanałów (16) w jednej komórce, przy maksymalnie trzech komórkach w stacji bazowej z anteną trójsektorową, nie zapewnia, niestety, potrzebnej liczby kanałów radiowych na terenach zurbanizowanych, a tym samym jakość połączeń w sieci ulega ciągłej degradacji. Ponieważ systemy NMT 900 o zwiększonej pojemności nie mogą być stosowane w Polsce ze względu na zarezerwowanie pasma 900 MHz na potrzeby telefonii cyfrowej GSM, dalszy wzrost liczby abonentów obsługiwanych przez telefonię analogową w centralnych systemach miejskich jest niemożliwy. Na skutek szybkiej ekspansji telefonii cyfrowych GSM - o wyższych parametrach użytkowych sieć analogowa NMT 450i prawdopodobnie ulegnie w Polsce likwidacji w ciągu najbliższych kilku lat, mimo że jej możliwości techniczne jeszcze się nie wyczerpały.

Zmodernizowana w 1997 r. wersja w standardzie NMT 450i została uzupełniona o niektóre nowsze cechy systemu NMT 900 (identyfikacja abonenta, modyfikacja protokołów sygnalizacji, polepszenie jakości mowy i inne) i zajmuje nieco inne pisma częstotliwości (452,5-457 MHz i 4623-467 MHz) niż określa to standard NMT 450.

Cyfrowa telefonia komórkowa. Podstawowym kryterium wprowadzania telefonii cyfrowej było uzyskanie jednolitej łączności nie tylko na terenie jednego kraju objętego systemem komórkowym, ale użytkowania telefonu komórkowego na obszarach innych krajów objętych tym samym systemem. Realizacja tego celu

5. Dystrybucja mocy. W obydwu systemach jest zastosowany taki sam mechanizm sterowania mocą sygnału radiowego: na polecenie sterownika stacji bazowych terminale ruchome MS (ang. Mobile Station) i stacje bazowe BS zmniejszają lub zwiększają moc swoich nadajników od wartości maksymalnej dla danej klasy do poziomu minimalnego 13 dBm, krokami co 2 decybele i nie szybciej niż co 60 ms. Maksymalna moc stacji BS w systemie GSM 1800 wynosi 20 W (w MS - 1-0,25 W), natomiast w systemie GSM 900 - 320 W (w MS - 2-0,8 W). Automatyczna adaptacja mocy stacji bazowej leży w gestii operatora systemu.

System PCS. Cyfrowy system komórkowy PCS (ang. Personal Communication System), mający cechy komunikacji osobistej PCN, jest rozwijany na terenie amerykańskim. W PCS przewiduje się stosowanie 6 różnych technologii komunikacji, w tym również systemu komórkowego DCS 1900 klasy GSM. Dla PCS zarezerwowano kilka pasm częstotliwości (A, B, C, D, E), wszystkie w zakresie bliskim 1900 MHz (stacje ruchome 1850-1910 MHz, stacje bazowe 1930-1990 MHz). Operatorom sieci (wiele licencji) pozostawiono wybór liczby kanałów, przy ustalonym odstępie dupleksowym 80 MHz (w GSM jest 45 MHz) i zwielokrotnieniu FDMA/CDMA (w GSM – FBMA/TDMA).

Systemy cyfrowe w Polsce. System GSM 900, wprowadzany w Polsce od 1996 r. na zasadzie przetargu, jest rozwijany przez dwóch operatorów krajowych: konsorcjum PTC (Polska Telefonia Cyfrowa) w sieci Era GSM oraz konsorcjum Polkomtel SA jako sieć Plus GSM. Obydwu sieciom przyporządkowano krajowe kody operatora MNC (ang. Mobile Network Code): 01 dla sieci Plus GSM oraz 02 dla sieci Era GSM, świadczące o kolejności uzyskiwania licencji. Trzecim operatorem systemu GSM 900 został (1999 r.) Centertel, już posiadający dwie licencje komórkowe: sieć analogową (od 1992 r.), początkowo jako NMT 450 i zmodernizowaną według specyfikacji NMT 450i Plus oraz sieć cyfrową GSM 1800 o nazwie Idea, działającą - komercyjnie w Polsce od 1998 r. Od marca 2000 r. wszyscy trzej operatorzy (PTC, Polkomtel i Centertel) mogą nadawać w pasmach 900 i 1800 MHz przez sieci cyfrowe GSM. Sprzęt telekomunikacyjny dla systemu GSM instalują głównie: Ericsson, Nokia i Siemens.

Ewolucja standardów komórkowych. Uniwersalny system dla telekomunikacji ruchomej ***UMTS*** (ang. Universal Mobile Telecommunication

System zapewnia automatyczną ciągłość transmisji (ang. handover, roaming) dla abonentów ruchomych przez hierarchiczną budowę struktur komórkowych oraz indywidualną lokalizację i identyfikację użytkowników za pomocą kart identyfikacyjnych SIM (ang. Subscriber Identity Module), umożliwia także szyfrowanie mowy i danych.

System GSM 1800 (DCS 1800). Rozszerzeniem standardu GSM jest nowsza jego wersja - oznaczana pierwotnie jako DCS 1800 (ang. Digital Communication System), a obecnie GSM 1800 – o trzykrotnie zwiększonej pojemności komunikacyjnej, przystosowana do pracy w zakresie częstotliwości 1800 MHz. System cyfrowy GSM 1800, oprócz wielu podobieństw do GSM 900, różni się następującymi cechami:

1. Częstotliwość pracy. Obydwa systemy działają z podziałem częstotliwości radiowej w zależności od kierunku transmisji. W systemie GSM 900 zakres częstotliwości dla kierunku w dół wynosi 935÷960 MHz oraz dla kierunku w górę 890÷915 MHz. System DCS 1800 pracuje w zakresie częstotliwości 1805-1880 MHz dla kierunku w dół oraz w zakresie 1710÷1785 MHz dla kierunku w górę.

2. Szerokość pasma w systemie GSM wynosi 25 MHz, co teoretycznie pozwala na inicjowanie 125 kanałów radiowych o szerokości 200 kHz każdy. W rozszerzonej wersji tego systemu, znanej jako E-GSM, szerokość pasma jest o 10 MHz większa niż w zwykłym systemie GSM i wynosi 35 MHz (175 kanałów). W odróżnieniu od GSM 900 w systemie GSM 1800 szerokość pasma wynosi 75 MHz (375 kanałów o szerokości 200 kHz każdy).

3. Warunki propagacyjne to dwukrotny wzrost częstotliwości pracy powoduje wzrost tłumienia fal radiowych w wolnej przestrzeni, co skutkuje około trzykrotnym zmniejszeniem komórek w stosunku do systemu GSM. Do równomiernego pokrycia radiowego podobnych obszarów przywołań w systemie DCS potrzeba odpowiednio więcej stacji bazowych BS (ang. Base Station).

4. Sygnalizacja. Mniejsze komórki wymagają większej liczby przełączeń pomiędzy nimi, co pociąga za sobą wzrost liczby kanałów sygnalizacyjnych w porównaniu z systemem GSM. Powoduje to również obniżenie efektywności przekazu informacji przez te kanały i wpływa na podwyższenie kosztów sieci stałej.

umożliwiać transmisję wąskopasmową i szerokopasmową z dostępem lokalnym do 2 Mb/s i globalnym bez ograniczenia odległości (z przepływnością do 384 kb/s).

FPLMTS (ang. Future Public Land Mobile Telecommunication Systems) - publiczny, ogólnoświatowy system łączności radiowej przeznaczony dla abonentów znajdujących się w ruchu. Koncepcja opracowana w sektorze standardów telekomunikacyjnych ITU-R przewidywała stosowanie tego przyszłościowego systemu w paśmie 2000 MHz, przy szerokości pasma min. 230 MHz. Wzrastające zapotrzebowanie na ruchome usługi komórkowe, konieczność stosowania nowych technik i technologii oraz integracja z innymi systemami światowymi spowodowały modernizację koncepcji i zmianę nazwy systemu na IMT-2000 (stosowanej również zamiennie z FPLMTS).

IMT 2000 (ang. International Mobile Telecommunications 2000) - podstawowy składnik globalnego systemu przyszłościowej komunikacji osobistej UPT (ang. Universal Personal Telecommunication), zastępujący dotychczasową koncepcję ogólnoświatowej łączności ruchomej i stacjonarnej typu FPLMTS. Dla IMT 2000 przeznaczono dwa podzakresy częstotliwości obowiązujące na całym obszarze Ziemi:

- satelitarny 1980÷2010 MHz i 2170÷2200 MHz;
- naziemny (dostępny w pełni po 2005 r.) w pasmach 2010÷2025 MHz i 2160÷2170 MHz;
- przystosowanie terminali ruchomych do współpracy z różnymi typami sieci komórkowych;
- usprawnienia w zakresie identyfikacji terminali i użytkowników za pomocą kart identyfikacyjnych SIM (ang. Subscriber Identity Module) dla różnych środowisk abonenckich.

W sieci systemu IMT 2000 są przewidywane wszystkie typy usług (przesyłanie mowy, usługi taksowe i przywoławcze o zasięgu światowym, łączność typu dyspozytorskiego, dwukierunkowa transmisja danych i przepływnością do 384 kb/s, wideoteks, wideofon, przekaz obrazów wysokiej jakości HDTV, a także dostęp abonentów do usług audiowizualnych). Docelowa przepływność transmisji danych przez sieci globalne IMT-2000 nie będzie przekraczać 384 kb/s zarówno w dostępie lokalnym, jak i zdalnym. Jako urządzenia odbiorcze są to małe,

System) stanowi najlepiej zdefiniowany przez europejską grupę działającą w ramach projektu RACE (ang. Research and Development Program in Advanced Communication in Europe) system - nazywany również trzecią generacją systemu GSM. System UMTS należy do rodziny systemów IMT-2000. Do najbardziej istotnych cech systemu, należą:

- integracja różnych metod pokrycia radiowego w jeden spójny mechanizm łączenia globalnego;
- połączenie usług oferowanych w systemach wąskopasmowych i szerokopasmowych dostępnych z terminalu ruchomego;
- zharmonizowanie platform przenoszenia (roaming) łączności między różnymi systemami i operatorami;
- współpraca terminali z różnymi typami lądowych sieci inteligentnych IN (ang. Inteligent Network).

Europejską wersję tego systemu przedstawiła (1997 r.) organizacja normalizacyjna ETSI. Zawarto w niej większość propozycji systemu IMT-2000 w prawie nie zmienionej postaci, chociaż modyfikacje dotyczą nie tylko pasm częstotliwości. Projekt stanowi de facto konwergencję wielu dotychczas działających sieci, przez modernizację istniejących systemów naziemnych (dyspozytorskich, komórkowych, przywoławczych), z systemami satelitarnymi. W rezultacie tego indywidualny abonent ruchomy otrzymuje nową jakość usług multimedialnych o przepływności od 64 kb/s do 384 kb/s, rozszerzanych w środowisku lokalnym do 2 Mb/s.

Zgodnie ze światowymi tendencjami konwergencji teleinformatyki za pomocą systemu UMTS można będzie konsekwentnie ujednolicić globalną infrastrukturę telekomunikacyjną przez: integrację wielu sieci i usług, personalizację dostępu do sieci, rozszerzenie dostępu do usług szerokopasmowych i rozpowszechnianie technik dostępu bezprzewodowego.

System UMTS został zdefiniowany jako standard otwarty dla systemów mobilnych o dużej szybkości transmisji, zarówno dla systemów naziemnych, jak i satelitarnych. Ma on zapewnić międzynarodowy roaming sieciowy za pomocą uniwersalnego terminala osobistego 3G, dostęp do wszystkich istniejących usług internetowych wraz z ofertą nowych usług szerokopasmowych. System ma

Istniejące generacje systemów komórkowych różnią się od siebie w istotny sposób (Tabela 2.3.).

Tabela 2.3. Podstawowe cechy generacji systemów komórkowych

		GENERACJA III (3G): - cyfrowe globalne UMTS (IMT - 2000) - zintegrowane usługi wąsko- i szerokopasmowe - transmisja danych EDGE 384kb/s, WCDMA 2Mb/s - usługi internetowe i multimedialne	**4 G**
	GENERACJA II (2G): - cyfroweGSM900, DCS1800 - usługi wąskopasmowe: głos, dane, SMS, VMS, faks	- transmisja danych HSCDSD115kb/s, GPRS do 170kb/s – usługi dodatkowe – roaming międzynarodowy	
GENERACJA I (1G): - analogowe (AMPS, NMT, TACS) - transmisja, danych 9,6 kb/s - SMS do 160 znaków	- poczta głosowa VMS - połączenia alarmowe, brak roamingu międzynarodowego		
1981 r.	**1991 r.**	**2001 r.**	**...? r.**

Źródło: *Net World, Vademecum teleinformatyka cz. 1*, International Data Group Poland S.A., Warszawa 2004, s. 100.

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

Rosnąca liczba użytkowników oraz zwiększające się ich wymagania spowodowały konieczność rozpoczęcia pracy nad kolejnym etapem telekomunikacji przenośnej. Dlatego największe światowe organizacje takie jak Międzynarodowa Unia Telekomunikacyjna (ITU) a nawet Komisja Europejska, rozpoczęły prace nad

kieszonkowe, podręczne (naręczne) i wielofunkcyjne terminale komórkowe działające nawet przy zmianie położenia z szybkością 500 km/h. Zastosowanie funkcji roamingu w komunikacji osobistej systemu IMT 2000 między dowolnymi punktami na Ziemi pozwoli na wykorzystanie wielu typów łączy: satelitarnych, radiowych, stacjonarnych, optycznych, także lokalnych linii kablowych.

W latach osiemdziesiątych powstały pierwsze systemy telefonii komórkowej pierwszej generacji (1G) oparte na technice analogowej - AMPS, NMT, TACS. Dla telefonii 1G zostały określone podstawowe cechy komunikacji: transmisja danych - 9,6 kb/s, transmisja mowy - kodowanie z przepływnością 13 kb/s, dostęp do kanału radiowego ze zwielokrotnieniem czasowym i ramką TDMA współpracujący z siecią pakietową publiczną - protokół X.25, przesyłaniem SMS-ów (krótkich wiadomości tekstowych) oraz realizacja połączeń alarmowych. Najwięksi producenci urządzeń i telefonów komórkowych: Ericsson, Nokia, Motorola i Uniwired Planet podjęli inicjatywę opracowania jednolitej, uniwersalnej i ogólnie akceptowalnej w przyszłości aplikacji WAP (Wireless Application Protocol) przeznaczonej dla abonentów telefonii komórkowej. Uzgodniono wersję tego protokołu, która niewątpliwie uzyska z czasem rangę standardu współpracy prostych i najprostszych terminali bezprzewodowych z siecią Internetu. W specyfikacji zdefiniowano uniwersalne środowisko pracy WAE (Wireless Application Enviroment) dla istniejących i przyszłych aplikacji opartych na internetowym modelu typu klient-serwer, w postaci stron i skryptów udostępnianych przez serwery sieciowe WWW (WML) dla przeglądarek klienta. Istotnym elementem specyfikacji jest specjalny język opisu stron internetowych WML (Wireless Markup Language), wzorowany na dotychczasowych procedurach HTML i HTTP, a także protokole TCP/IP. Dzięki temu abonenci niespójnych systemów sieci komórkowych lub przywoławczych, używający dowolnego rodzaju terminali mobilnych (o niewielkich rozmiarach i różnorodnych ekranach), będą mieli dostęp do tych samych aplikacji i usług.

Pierwsze komercyjnie dostępne telefony komórkowe z protokołem WAP już były demonstrowane na wystawie w Cannes jako: OneTouch Pocket (Alcatel), Nokia 7110 (Nokia) i SGH-800 (Sagem). Chociaż mogą one działać z sieciami 2G (faza 2+), to korzystanie z dobrodziejstw wynikających z protokołu WAP będzie możliwe dopiero po wprowadzeniu szybszej pakietowej transmisji danych GPRS.

natomiast w Polsce system GSM 900 został wprowadzony w 1996 roku przez firmy PTC (Polska Telefonia Cyfrowa) w sieci Era GSM oraz Polkomtel S.A. w sieci GSM Plus. W 1998 roku koncesję na GSM 1800 dostał trzeci polski operator Centertel - sieć Idea. Telefonia 2G w 1995r. otrzymała usprawnienia obejmujące transmisję telefaksową, interfejs komputerowy, usługi telekonferencyjne oraz identyfikację abonenta za pomocą karty SIM. Następną fazą ewolucji systemów komórkowych jest faza 2,5G, będąca fazą przejściową pomiędzy drugą i trzecią generacją telefonii komórkowej. Telefonia 2,5G powstała w 1997 roku. Opiera się na dwóch szybszych technologiach transmisji: HSCSD (Hight Speed Circuit Swiched Data) do 115 kb/s i GPRS (General Packed Radio Service) do 170 kb/s. Transmisja danych HSCDSD umożliwia zwiększenie szybkości przekazu poprzez przydział kilku szczelin czasowych do jednego połączenia, każda o szybkości nominalnej 9,6 kb/s. Jedna transmisja może zajmować 7 szczelin (67,2 kb/s), a przy zastosowaniu kompresji przepływność zwiększa się do 115 kb/s.

Natomiast transmisja pakietowa GPRS polega na powiązaniu i wspólnym sterowaniu kilku kanałów transmisyjnych w jeden tor komunikacyjny. Możliwe jest przyporządkowanie 8 szczelin czasowych w jednym kanale radiowym (76,5 kb/s), a przy zastosowaniu kompresji przepływność zwiększa się do 170 kb/s. Ostatnim krokiem ku telefonii 3G po wprowadzeniu transmisji GPRS jest etap transmisji EDGE (ang. Enhansed Data GSM Evolution) umożliwiający transmisję z przepływnością 384 kb/s poprzez infrastrukturę GSM. Przez wiele lat systemy GSM będą funkcjonować równolegle z UMTS.

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

- interfejs radiowy według nowego standardu UTRA UMTS (Terrestial Radio Access), rekomendowany przez ETSI dla europejskich systemów UMTS;
- interfejs radiowy CDMA 2000, stanowiący rozwinięcie standardu dotychczasowego IS-95 według TIA (ang. Telecommunications Industry Association), z przeznaczeniem do stosowania w USA;

nowym, ogólnoświatowym standardem. Założenia przygotowywane w ITU nazwano IMT-2000 (od międzynarodowej telefonii ruchomej - international mobile telephony).

Prace, prowadzone od początku lat dziewięćdziesiątych przez ITU, nad standaryzacją przyszłego systemu komunikacji osobistej zakładały utworzenie jednolitego systemu lądowego (dla całego globu), nazywanego początkowo FPLMTS (Future Public Land Mobile Telecommunication System). Niezwykle szybki rozwój systemów satelitarnych spowodował rozszerzenie funkcji i zasięgu tego naziemnego systemu globalnego o segment satelitarny i rozwiązania techniczne łączące ziemskie systemy telefonii komórkowej z systemami satelitarnej łączności ruchomej. Wspólny wysiłek wielu służb normalizujących, z uwzględnieniem różnych zastosowań systemu, zaowocował opracowaniem światowego standardu radiokomunikacyjnego oznaczonego IMT-2000 (ang. International Mobile Telecommunications).

Zakończenie długiego procesu normalizacji i zatwierdzenie standardu IMT-2000 przez ITU przewiduje się w najbliższym czasie. Ze względu na zbyt duże różnice występujące między infrastrukturą sieci eksploatowanych w poszczególnych częściach świata i różne zajętości pasm radiowych postanowiono, że systemy globalne będą funkcjonowały w kilku odmianach regionalnych (Europa, USA, Japonia, Chiny, Korea i in.), przy zachowaniu możliwie wielu wspólnych cech i wymagań ogólnych systemu IMT-2000 o wysokiej przepustowości, także podstawowych zakresów częstotliwości ustalonych przez ITU. Największe odstępstwa od standardu i związane z tym kłopoty, wynikające z wcześniejszego zagospodarowania podstawowych zakresów częstotliwości na inne potrzeby, będą widoczne na terenie amerykańskim.

W Polsce był to system NMT 450 wprowadzony przez Centertel w 1991 roku, pracujący w częstotliwości 450 MHz z liczbą kanałów 200 pokrywający 95% powierzchni kraju. Systemy analogowe miały sporo wad - małą odporność na zakłócenia, łatwość podsłuchu rozmów, brak roamingu międzynarodowego i niedostateczną transmisję danych. Wymusiło to powstanie systemów komórkowych drugiej generacji (2G) popularnie zwanych GSM pracujących w technice cyfrowej. Pierwszy system GSM na świecie został oddany w 1991 roku,

usług szerokopasmowych 3G. Zakres nowych usług dostępnych w systemie UMTS jest duży, co jest związane z możliwością dostępu do szerokiego pasma głównie z ofertą usług multimedialnych (Tabela 2.4.).

Tabela 2.4. Przepływność dla poszczególnych usług (kb/s)

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

Źródło: Opracowanie własne na podstawie: *Kierowanie obronnością państwa w stanach nadzwyczajnych,* Praca naukowa pod kier. M. Krauze, AON, Warszawa 2000.

System UMTS jest bowiem optymalizowany nie pod kątem transmisji mowy, lecz globalnych i zróżnicowanych przekazów multimedialnych. Stanowi to zasadniczą różnicę w ofercie usług między systemami cyfrowymi dotychczasowej generacji (2G) i systemami trzeciej generacji 3G. Docelowo usługi 3G będą dostępne za pomocą jednego (fizycznie) wspólnego terminalu działającego w różnych środowiskach sieciowych, zarówno wewnątrz pomieszczeń (na wzór terminali systemu DECT), jak i na zewnątrz budynków, a także w pojazdach.
Terminale i telefony 3G nie są jednak standaryzowane, co oznacza, że można oczekiwać bardzo zróżnicowanych terminali wideofonicznych, nie tylko pod względem oferowanych funkcji, ale i ich ergonomii. Dalsza ich przyszłość wiąże się przede wszystkim z rozwojem kamer cyfrowych, modernizacją systemów rozpoznawania obrazów oraz ciągłej miniaturyzacji komunikatorów PDA, pozycjonerów GPS, laptopów i browserów internetowych.

Rozwiązaniem idealnym jest pełny zakres oferowanych usług, dostępny wszędzie i w każdej sytuacji. O szybkości dochodzenia do takiego stanu zadecydują głównie potrzeby, gdyż wydaje się, że poszczególne elementy technologii takiego

- interfejs radiowy UWCC-136, będący ewolucyjnym rozszerzeniem istniejącego standardu IS-136, rekomendowany przez UWCC (ang. Universal Wireless Communications Consortium) na terenie USA.

Interfejs UTRA. Większość przedstawionych propozycji interfejsu radiowego, włącznie z europejskim UMTS opiera się na technice WCDMA (ang. Wideband Code Division Multiple Access), a więc szerokopasmowym rozpraszaniu widma za pomocą ciągu kodowego. Oryginalną koncepcją interfejsu radiowego UTRA (UMTS Terrestial Radio Access) jest działanie w dwóch trybach pracy dupleksowej: FDD (ang. Frequency Division Duplex) i TDD (ang. Time Division Duplex). Te i inne przyjęte rozwiązania dają elastyczność w konfigurowaniu kanału transmisyjnego, możliwość równoległej transmisji o zmiennej szybkości w kilku kanałach, stosowanie efektywnej transmisji pakietowej, łatwe przenoszenie do innych systemów, ze szczególnym uwzględnieniem sieci GSM. Mają one również na celu: zaoferowanie optymalnego bilansu energetycznego dla obydwu kierunków transmisji (anteny adaptacyjne), lepsze wykorzystanie dostępnego widma i łatwe wdrażanie przekazów. Parametry interfejsu radiowego WCDMA i sieci szkieletowej pozwalają na wykorzystanie dotychczasowych zasobów sieci GSM, budowę terminali uniwersalnych GSM/UMTS oraz ewolucyjny rozwój systemów komunikacji osobistej UMTS.

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

Stosunkowo krótkie terminy realizacji poszczególnych regionalnych systemów szerokopasmowych wynikają z ich podobieństwa do technologii stosowanych w środowisku GSM i stanowią niejako ewolucję tych sieci w kierunku szerszego pasma transmisji 3G, a w ślad za tym budowę terminali i świadczenia

- Standard SECAM (ang. Systeme Electronique Couleur Avec Memorie) jest wersją rozwijaną we Francji i stosowaną w krajach Europy Środkowej. System telewizji kolorowej SECAM stosuje inny sposób kodowania chrominancji. W Polsce zrezygnowano z transmisji w standardzie SECAM na korzyść systemu PAL.

Telewizja kablowa CATV. Telewizja kablowa CATV (Cable Television, Community Antenna Television) spełnia funkcję dystrybucji sygnałów telewizyjnych wysokiej częstotliwości przez sieć abonencką zbudowaną z kabli współosiowych. W układzie klasycznym (stosowanym do tej pory) możliwa jest zarówno transmisja analogowa, jak też transmisja sygnałów cyfrowych metodami modulacji szerokopasmowej stosowanej w sieciach LAN/WAN.

Podstawową funkcją CATV w tym jednokierunkowym układzie jest rozprowadzenie wielokanałowego zbioru modulowanych sygnałów wizji i fonii ze stacji czołowej (lub retransmisyjnej) do tysięcy odbiorników abonenckich.W wersji rozszerzonej, z dodatkowym kanałem zwrotnym (od abonenta do stacji czołowej) o przepływności: małej - 16 kb/s, średniej - 144 kb/s lub dużej – 2 Mb/s, możliwa jest interakcja, niezbędna przy korzystaniu z usług teledacyjnych i multimedialnych usług szerokopasmowych. Po stronie abonenta są stosowane interaktywne kodeki i dekodery analogowo-cyfrowe w celu rozszerzenia oferty o płatne (kodowane) programy TV.

Pierwszym etapem wdrażania usług interaktywnych w sieciach CATV jest budowa sieci hybrydowych HFC (ang. Hybrid Fiber Coax), łączących współosiową infrastrukturę mieszkaniową z sieciami światłowodowymi (rozwijana przez Alcatel, Lucent Technologies, Siemens).

Telewizja cyfrowa DVB. Europejski projekt rozsiewczego systemu telewizji cyfrowej DVB (ang. Digital Video Broadcasting) działa (od 1993 r.) w sieciach naziemnych, kablowych i satelitarnych. W systemach naziemnych kanały częstotliwościowe telewizji cyfrowej są identyczne z przyjętymi dla telewizji analogowej, w Europie dla IV i V zakresu częstotliwościowego mają one szerokość 8 MHz. Wszystkie trzy sieci stosują ten sam system kodowania źródłowego sygnałów wizyjnych i fonicznych według standardu MPEG-2, podobną strukturę zwielokrotnienia MPEG-3 TS, jak również te same metody korekcji błędów

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

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

Ad. f) systemy wideokomunikacji

Telewizja analogowa. Pierwsze biało-czarne przekazy telewizyjne (1945 r.) zajmowały pasmo o szerokości 4,5 MHz. Przekazy kolorowe rozpowszechniły się kilka lat później (1954 r.) we wszystkich podstawowych standardach telewizji analogowej:

- Standard NTSC (ang. National Television Standards Commitee) został zaakceptowany (1953 r.) w amerykańskiej analogowej telewizji rozsiewczej stosującej 525 linii skanujących. W standardzie NTSC rozdzielczość wynosi 640 punktów w linii (z tego 485 przeznaczonych do odwzorowania obrazu) przy częstości 30 r/s i formacie 4:3;
- Standard PAL (ang. Phase Alternate Line), wprowadzony (1967 r.) w niektórych krajach europejskich, Australii i Afryce, działa stosując 625 linii, z częstością 25 r/s, rozdzielczością 640 punktów w linii i w formacie 4:3. W systemie PAL sygnał koloru jest odwracany o 180° w kolejnych liniach skanowania - z czym jest związana nazwa standardu;

Współczesne układy, stosujące kompresję według algorytmu MPEG-2, otwierają drogę do wideofonii wysokiej jakości HQ (High Quality), wymagającej przepływności tylko 384 kb/s w kanale komunikacyjnym, angażując do transmisji 6 kanałów typu B, czyli kanał HQ oferowany w sieciach cyfrowych ISDN.

Wideokonferencja. Współczesne systemy wideokonferencyjne przesyłają jednocześnie sygnał fonii i wizji w czasie rzeczywistym na dowolna odległość, z wykorzystywaniem sieci analogowych, cyfrowych (ISDN), lokalnych LAN, a nawet łączy naziemnych bądź satelitarnych. Są dwojakiego rodzaju.

Usługa wideokonferencyjna może być realizowana na dwa sposoby: za pomocą ulepszonych komputerów klasy PC lub specjalnych zestawów multimedialnych, zapewniając w ten sposób organizowanie spotkań lub telekonferencji wielu użytkownikom znajdującym się w odległych od siebie miejscach. Najprostsze stanowisko uczestnika wideokonferencji musi być wyposażone w: komputer z łączem telekomunikacyjnym o szybkości minimalnej 128 kb/s, kamerę wideo z kodekiem dokonującym kompresji i dekompresji sygnałów wizyjnych oraz głośno mówiący telefon (cyfrowy system komputerowy).

Najważniejszym parametrem systemu jest szybkość, z jaką są kodowane i przesyłane informacje - zgodnie z zaimplementowanym algorytmem i protokołem transmisji. Wpływają one bezpośrednio na jakość transmitowanego obrazu i dźwięku, sposób rejestracji danych z kamery i mikrofonów oraz działają pośrednio na maksymalną liczbę stanowisk (osób) uczestniczących w seansie wideokonferencji.

W celu zmniejszenia wymagań na pasmo transmisji do przekazów wideokonferencyjnych stosuje się różne ograniczenia „transmisji na żywo", obejmujące zgodnie ze standardem H.320:

- usuwanie ramek: 10 ramek/s (seria nieruchomych obrazów), 15 ramek/s (popularna obecnie forma wideokonferencji), powyżej 20 ramek/s (prawie płynny ruch obrazu);
- mały format obrazu CIF (ang. Common Intermediate Format) zawierający 288x352 (punkty), związany ze standardem kompresji H.261;
- zmniejszony format QCIF (ang. Quarter CIF) zawierający 144x 176 (punktów);

pierwszego stopnia (kod Reeda Solomona i przeplatanie danych). Metody kodowania kanałowego i modulacji są odmienne w poszczególnych systemach. Pierwszym krajem europejskim wprowadzającym telewizję cyfrową była Wielka Brytania (1995 r.), stając się poligonem doświadczalnym Europy w zakresie DVB. Proces normalizacji sieci cyfrowej, chociaż nie jest doprowadzony do końca, wyróżnia cztery rodzaje standardów:

- DVB-T (Terrestial) - dla kanałów o szerokości 7÷8 MHz w systemach naziemnych;
- DVB-S (Satellite) - w paśmie 11/12 GHz, kanał o szerokości 30÷40 MHz;
- DVB-C (Cable) - kompatybilny z DVB-S, kanały 8 MHz;
- DVB-CS (Common Satellite) - do anten zbiorowego odbioru satelitarnego.

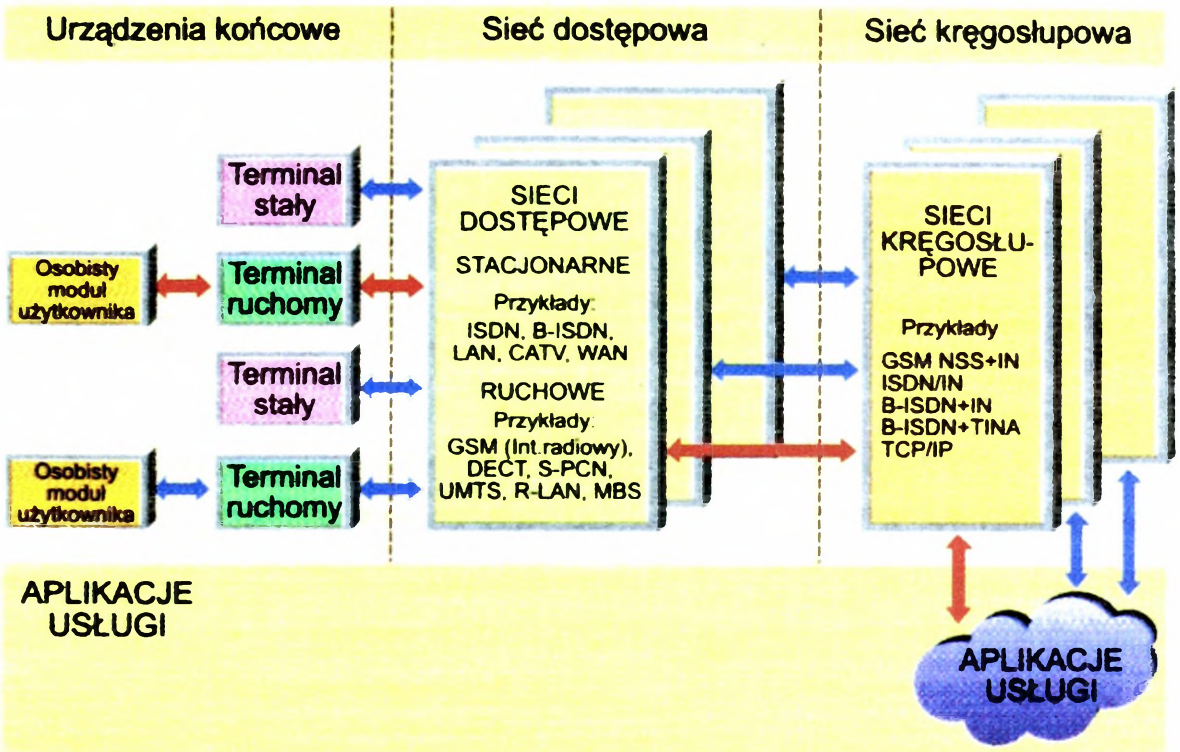
Telewizja wysokiej jakości HDTV. Standard HDTV (ang. High Definition TeleVision) umożliwia przekaz telewizyjny o dużej rozdzielczości obrazu, dwukrotnie wyższej od obecnie stosowanej. Do przesyłania obrazu wymaga skomprymowanej przepływności 20-30 Mb/s, przy rozdzielczości obrazu 1440x1152 lub 1920x1152 punkty i częstości ramek 60, 40 lub 24 ramki/s. Przepływność bez cyfrowej kompresji sygnału wizyjnego wynosi około 140 Mb/s.

Wideotelefonia. Historycznie pierwsza i najprostsza usługa telefonii obrazowej obejmuje dwustronną, symetryczną wideotelefonię i stanowi element obsługi telekonferencyjnej (bez przesyłania pełnego ruchu obrazu). Pierwsze usługi wideotelefoniczne (VideoPhone 2500, AT&T, 1992 r.), zestawiane na życzenie dwóch abonentów, wymagały łączy o przepływności 2 Mb/s do przesyłania skompresowanego sygnału audio-wideo. Najprostszą formą wideofonii jest wideotelefon stacjonarny (telefon, modem, kamera, kodek sygnałów audio, kodek sygnałów wideo, procesor do zarządzania i synchronizacji głosu z obrazem, ekran), umożliwiający realizację seansu łączności przez kanały publicznej, komutowanej sieci telefonicznej. Nowsze układy umożliwiają kompresję sygnału wizyjnego w formacie CIF (288x352 punkty) przy częstotliwości powtarzania 20 ramek/s lub QCIF (144x176 punkty) z powtarzaniem do 30 ramek/s i przesyłanie zakodowanego sygnału przez kanał komunikacyjny o przepływności zmieniającej się w zakresie już od 40 kb/s do maksymalnej 2 Mb/s.

gwałtowne zapotrzebowanie na usługi multimedialne pochodzi od użytkowników terminali ruchomych, dla których synonimem stał się telefon komórkowy sieci cyfrowej GSM (Schemat 2.8.).

Schemat 2.8.

Architektura ruchomej sieci multimedialnej



Źródło: *Net World, Vademecum teleinformatyka cz. 1*, International Data Group Poland S.A., Warszawa 2004, s. 112.

Wykorzystanie sieci komórkowej GSM jako sieci dostępowej do usług świadczonych przez sieci stacjonarne, stało się częścią ogólnej koncepcji globalnego ruchowego systemu dostępu do usług multimedialnych GMM (ang. Global Multimedia Mobility). Multimedialnego systemu ruchowego, który pomimo braku w pełni szerokopasmowego dostępu powinien:

- dostarczać różnorodne usługi komunikacyjne;
- świadczyć usługi oferowane przez wielu różnych operatorów (korporacji międzynarodowych, narodowych telekomów, operatorów sieci prywatnych i lokalnych;
- umożliwiać dostęp o podwyższonej szybkości transmisji do tych samych aplikacji za pomocą różnych rodzajów terminali;

- kompresję głosu i dźwięku o wysokiej jakości, z przepływnością kanałową tylko 16kb/s.

Systemy wideokonferencyjne - realizowane za pomocą analogowych linii telefonicznych (standard kompresji H.263), pozwalają obsłużyć strumień medialny z maksymalną szybkością do 15 klatek obrazowych na sekundę, bez stosowania kosztownych kart rozszerzających (efektywna kompresja i dekompresja obrazu). Jakość obrazu i dźwięku uzyskana dla tego typu połączeń pozostaje jednak jeszcze daleko od oczekiwań potencjalnych użytkowników systemu, a w celu uzyskania wysokiej jakości obrazów z dynamicznie rejestrowanym ruchem treści zaleca się korzystanie wyłącznie z sieci ISDN z przekazem cyfrowym.

Brak obowiązujących standardów wideokonferencji powoduje powstawanie wielu niekompatybilnych systemów, współpracujących tylko z własnymi protokołami, bez możliwości działania z innymi systemami. Najczęściej stosowanymi systemami wideo konferencyjnymi są: Proshare (Intel), MCU (Lucent Technologies), ShowMe 2.0 (Sun Microsystems), seria systemów: Vision 2000, Vision 770 (Tandberg ASA) i inne.

Multimedia. Współczesna technologia umożliwia równoczesne przekazywanie (także przesyłanie, komutowanie, rozgłaszanie i rejestrowanie do dalszej obróbki) kilku rodzajów usług telekomunikacyjnych za pomocą tych samych środków technicznych oddziałujących na zmysły człowieka. Technologia multimedialna operuje informacją skojarzoną - używając kombinacji mieszanej: głosu, dźwięku, tekstu, grafiki, obrazu ruchomego i animacji - z interakcyjnym wsparciem od strony użytkownika.

Do realizacji usług multimedialnych niezbędne są: sieci o przepływności od 2 Mb/s do 8 Mb/s (niekiedy 20÷30 Mb/s) doprowadzające sygnał bezpośrednio do stacjonarnego miejsca abonenta, kanał zwrotny przeznaczony do interakcji użytkownika (min. 64 kb/s), a także odpowiednie urządzenie abonenckie (dźwięk, grafika, ekran). Oprócz tego są potrzebne multimedialne programy aplikacyjne, implementowane zarówno po stronie abonenckiej, jak też w systemach komutacji i centrum obsługi obrazowej (TV, CATV).

Multimedialna przyszłość należy jednak do systemów ruchowych (ruchome są tylko terminale przenośne), a ich wdrażanie już się rozpoczyna. Coraz częściej

międzykontynentalnych za pomocą kanałów telewizyjnych, telefonicznych i transmisji danych.

INMARSAT (Inmarsat 2, Inmarsat 3) jest systemem z satelitami nad oceanami Atlantyckim, Indyjskim i Spokojnym, służy głównie do realizacji połączeń telefonicznych i transmisji danych z ruchomymi terminalami satelitarnymi znajdującymi się na morzu (na okrętach, statkach i łodziach), na lądzie (na wszelkiego typu pojazdach) oraz z przenośnymi, np. typu walizkowego.

W systemie wyróżnia się kilka standardów stacji:

- Inmarsat A - analogowa transmisja głosu, terminale stałe (ok. 100 kg);
- Inmarsat B - cyfrowa transmisja mowy, terminale przewoźne (18 kg);
- Inmarsat C - transmisja danych (600 b/s), terminale przewoźne;
- Inmarsat D - transmisja danych (20 kb/s), terminale przenośne (do 10 kg);
- Inmarsat M - cyfrowy przekaz mowy i danych (2,4 kb/s), terminale przenośne;
- Inmarsat P - pierwotna niskoorbitowa wersja systemu dla terminali kieszonkowych, zastąpiona obecnie systemem ICO (ang. Intermediate Circular Orbit).

ORION posiada satelity umieszczone nad Oceanem Atlantyckim i służy głównie do połączeń między Ameryką Północną a Europą. Realizuje również kanały transmisyjne w systemach VSAT oraz kanały przekazów telewizyjnych.

PANAMSAT posiada satelity znajdujące się nad Oceanem Indyjskim i zapewnia głównie komunikację w systemach VSAT, przekazy telewizyjne oraz łączność telefoniczną.

EUTELSAT wykorzystuje satelity obejmujące swym zasięgiem Europę. Służą one głównie do transmisji telewizyjnych, również transmisji danych w systemach VSAT. Ze względu na wysoki stopień dostępności jest najbardziej odpowiednim systemem satelitarnym do wykorzystywania w Polsce. Satelity tego systemu mają wiązki promieniowania radiowego skierowane w różne części Europy, dwie z nich obejmują zasięgiem Europę Centralną.

W kraju istnieje nowoczesny system łączności satelitarnej (na skalę europejską) w Psarach koło Kielc, będący systemem sieci stacjonarnej (Schemat 2.9.).

- oferować usługi w różnorodnych środowiskach w zależności od warunków lokalnych.

W architekturze multimedialnego systemu ruchowego GMM opartego na strukturze klient-mediator-serwer (W odróżnieniu od klasycznej struktury klient-serwer), wykorzystano łącza cyfrowe ruchomych stacji roboczych GSM MOWGLI (ang. Mobile Office Workstations using GSM Links).

Ad. g) systemy satelitarne

Stacjonarne systemy satelitarne. W stacjonarnych systemach satelitarnych komunikacja między abonentami dokonuje się za pomocą satelitów telekomunikacyjnych umieszczonych na orbitach geostacjonarnych. Każdy system obejmuje jeden lub kilka aktywnych satelitów i przynajmniej jednego rezerwowego, uaktywnianego w przypadku uszkodzenia lub utraty kontroli nad satelitą aktywnym.

Satelity wykorzystywane do celów telekomunikacyjnych są zwykle wyposażone w kilka (do kilkudziesięciu) transponderów, pracujących w różnych pasmach o częstotliwości od kilku do kilkudziesięciu GHz, wykorzystywanych w zależności od: zastosowań, rodzaju transmisji, sposobu rezerwacji pasma i wielkości przepływności binarnej przez kanały satelitarne. Typowymi zastosowaniami systemów satelitarnych są:

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

Niektóre pasma częstotliwości satelitarnych pokrywają się z naziemnymi liniami radiowymi do transmisji sygnałów cyfrowych działających w zakresach częstotliwości 11, 14, 23, 38, 50 GHz, które są przyznane wyłącznie dla specyficznych rodzajów służb lub wykorzystywane wspólnie służby publiczne.

Do największych światowych systemów satelitarnych należą: Intelsat, Inmarsat, Orion, Eutelsat i Panamsat. Optymalne położenie satelitów ze względu na dostęp z terytorium naszego kraju mają systemy: Intelsat, Inmarsat i Eutelsat.

INTELSAT posiada satelity rozmieszczone nad oceanami Atlantyckim, Indyjskim i Spokojnym, jest przeznaczony głównie do zapewnienia połączeń

Zależnie od położenia orbity względem Ziemi rozróżnia się satelity:

- synchroniczne - o okresie obrotu równym okresowi obrotu Ziemi względem osi;
- podsynchroniczne - o okresie obrotu mniejszym od obrotu Ziemi;
- stacjonarne (synchroniczne) - krążące po orbicie kołowej leżącej w płaszczyźnie równika ziemskiego i ruchem zgodnym z kierunkiem obrotu Ziemi i okresie równym okresowi obrotu ziemi.

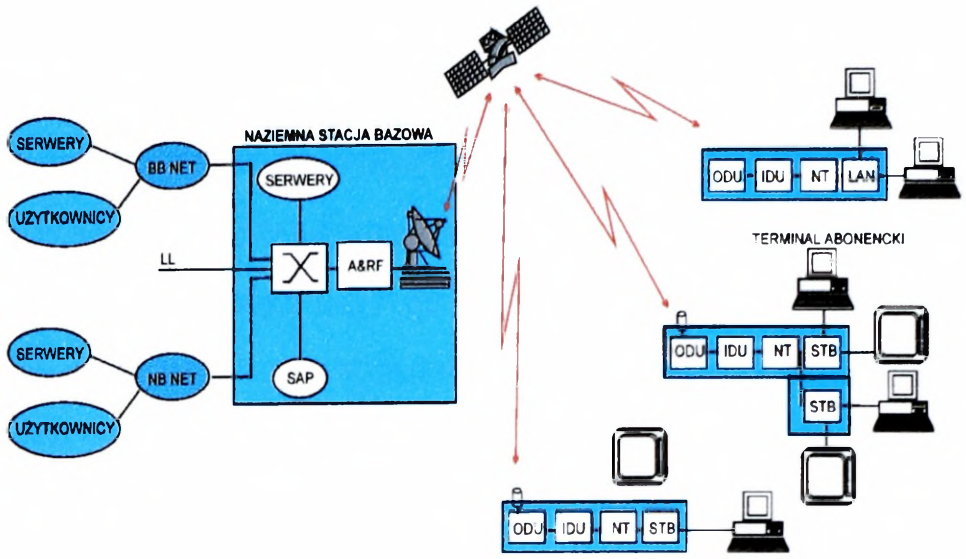
Umieszczony na orbicie okołoziemskiej satelita telekomunikacyjny stanowi bezobsługowy przekaźnik satelitarny (transponder) umożliwiający nawiązanie i utrzymanie łączności satelitarnej (telegraficznej, telefonicznej, radiotelefonicznej, telewizyjnej, przesyłania danych itp.) pomiędzy odległymi punktami na powierzchni Ziemi. Pod względem działania rozróżnia się satelity:

- □ bez przetwarzania sygnału na pokładzie satelity (transmisje przeczroczyste) oraz z przetwarzaniem sygnału na satelicie, pracujące w czasie rzeczywistym lub w trybie zapamiętaj i prześlij;
- □ przeznaczone do odbierania, wzmacniania i zapisywania sygnałów oraz ich retransmisji w odpowiednim czasie, zwykle w perygeum orbity, lub przy przelatywaniu nad określonym obszarem.

Przekaźnik satelity. Przekaźnik satelitarny stanowi wielokanałowe urządzenie komunikacyjne umieszczone na satelicie telekomunikacyjnym przeznaczone do retransmisji sygnałów nadawanych z Ziemi. Pasmo komunikacyjne każdego szerokopasmowego kanału transpondera jest rozdzielone częstotliwościowo na dwie części: łącze w górę do przesyłania sygnałów z Ziemi do przekaźnika i łącze w dół do przesyłania sygnałów z przekaźnika do stacji naziemnych. Nominalna szerokość pasma przenoszonego przez przekaźnik wynosi nie mniej niż 500 MHz i jest podzielona na kanały szerokopasmowe (10÷24 kanałów), które są konfigurowane zdalnie w zależności od zapotrzebowania na moc sygnałów radiowych RF (ang. Radio Frequency) nadawanych w kierunku Ziemi w paśmie dolnym. Liczba i moc poszczególnych kanałów wyjściowych są ograniczone maksymalną wydajnością zasilania; w zależności od typu przekaźnika zmienia się ona od 10W do 100W w całym paśmie łącza dolnego. Przemiennik pasmowy satelity dokonuje przesunięcia grupowego częstotliwości nośnych we

Schemat 2.9.

Schemat sieci satelitarnej (Wariant)



Oznaczenia:

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

Źródło: Opracowanie własne na podstawie materiałów Instytutu Łączności w Miedzeszynie.

Orbity satelitarne. Spośród orbit okołoziemskich, po których krążą satelity komunikacyjne, ze względu na ich kształt oraz oddalenie od Ziemi wyróżnia się:

- HEO (ang. Highly Eliptical Orbit) - orbita eliptyczna używana głównie dla satelitów badawczych, mająca typowo: apogeum w odległości 25÷45 tys. km oraz perygeum w odległości 3÷5 tys. km od powierzchni Ziemi, czas obiegu satelitów ok. 3 godz., wiele płaszczyzn orbitowania;
- LEO (ang. Low Earth Orbit) - orbita kołowa dla satelitów niskoorbitowych, odległość 200÷1200 km od powierzchni Ziemi, czas obiegu satelitów ok. 100 minut (Iridium, Globalstar, Orbcomm);
- MEO (ang. Medium Earth Orbit), ICO (Intermediate Circular Orbit) - orbity kołowe, wysokość ok. 10 tys. km, czas obiegu od 6 do kilkunastu godzin (Concordia, ICO Communication);
- GEO (ang. Geostationary Earth Orbit) - orbita geostacjonarna w odległości 36 tys. km od powierzchni Ziemi, z przeznaczeniem dla stacjonarnych systemów satelitarnych (Inmarsat, Intelsat, Eutelsat, Panamsat, Orion).

Wprowadzenie na rynek przenośnych i poręcznych odbiorników sygnałów GPS o różnej dokładności wywołało olbrzymie zainteresowanie tym systemem nawigacji i lokalizacji (również do precyzyjnego pomiaru czasu bezwzględnego GMT) w dziedzinach: nawigacji, geodezji, kartografii, lokalizacji pojazdów znajdujących się w ruchu oraz synchronizacji transmisyjnych systemów telekomunikacyjnych.

Inne systemy satelitarne. Satelitarne systemy komunikacji osobistej przeznaczone są do komunikacji osobistej i opierają się na satelitach krążących po orbitach niestacjonarnych, znajdujących się znacznie niżej niż 36 000km.

System Globalstar. Składa się z 56 satelitów rozlokowanych na ośmiu orbitach przebiegających na wysokości 1414 km, o inklinacji 52°, przy czym 8 satelitów pełni funkcje rezerwowych. W systemie wykorzystano technikę dostępu kodowego CDMA. Sygnały z terminali abonentów są przekazywane przez satelitę do pracujących w granicach wiązki satelitarnej stacji naziemnych, eksploatowanych przez operatorów. Do połączeń między stacjami naziemnymi jest wykorzystywana sieć naziemnych łączy międzynarodowych. Uruchomiony został w 1999 r.

System Iridium. Jest jednym z czołowych systemów satelitarnej łączności ruchomej. Aktualnie obejmuje 66 satelitów roboczych z urządzeniami nadawczo-odbiorczymi pracującymi w paśmie L oraz 6 zapasowych obiegających Ziemię po nisko położonych orbitach (wysokość 780 km) i rozdzielonych równomiernie na sześć płaszczyzn orbitalnych. Transmisja dwukierunkową w zakresie 1616÷1626,5 MHz, wykorzystuje technikę dostępu TDMA/FDMA. Podobnie, jak w naziemnych systemach radiotelefonii komórkowej, utworzono na powierzchni Ziemi 48 „komórek", każda o średnicy około 600 km, dzięki czemu można było zagwarantować łączność ruchomą, obejmującą całą powierzchnię kuli ziemskiej. Uruchomiony w 1998 roku. Oprócz łączności telefonicznej weszły usługi przywoławcze i transmisji danych. Usługi te są dostępne dla abonentów użytkujących terminale przenośne niewielkich rozmiarów umożliwiają działanie w dwóch trybach pracy DM (ang. Dual Modme), z siecią komórkową GSM.

System ICO (ang. Intermediate Circular Orbit) - (Inmarsat-P). Jest systemem globalnej łączności ruchomej z wykorzystaniem terminali o rozmiarach współczesnego telefonu komórkowego. Oparty na niestacjonarnych satelitach

wszystkich retransmitowanych kanałach przez kwarcowy, wysoko stabilny generator podnośnej znajdujący się w transponderze. Rozdzielenie częstotliwości nośnych do odbioru i nadawania sygnałów, a także odpowiednia zmiana polaryzacji sygnałów umożliwiają wykorzystanie jednej kierunkowej anteny nadawczo-odbiorczej, dla łącza zarówno dolnego, jak i górnego.

Lokalizacja GPS. Światowy system radionawigacji satelitarnej GPS (ang. Global Positioning System), wprowadzony (1978 r.) na potrzeby wojskowe przez amerykański Departament Obrony, został udostępniony w ograniczonym zakresie do publicznego użytkowania w 1994 r. System precyzyjnej lokalizacji GPS jest oparty na 24 satelitach NAVSTAR (w tym 3 rezerwowych) krążących wokół Ziemi po 6 równomiernie oddalonych od siebie orbitach, po 4 satelity na każdej orbicie. Zastosowana wysokosprawna modulacja kodowa zezwala na transmisję informacji nawigacyjnych na dwóch poziomach:

- z większą dokładnością - do zastosowań militarnych (niedostępnych publicznie) o największej precyzji pozycjonowania PPS (Precision Positioning Senvice), w zakresie od 1 m do 10 m;
- ze zredukowaną dokładnością - dostępną standardowo w zastosowaniach cywilnych SPS (Standard Positioning Senvice), w zakresie do 100 m, a dla uprzywilejowanych użytkowników nawet do 10 m.

W systemie GPS dwie częstotliwości nośne, L1 i L2, są modulowane kodowo sygnałem z rozproszonym widmem SS (ang. Spread Spectrum): kodem C/A (ang. Coarse Acquisition Coce) z szybkością 1 MHz, dostępnym do zastosowań cywilnych, oraz kodem precyzyjnym P (ang. Precision Code) z szybkością do 10 MHz w zastosowaniach militarnych.

Największą precyzję lokalizacji, dostępną dla uprzywilejowanych użytkowników systemu, uzyskuje się przez stosowanie dodatkowej stacji referencyjnej o znanej, bardzo dokładnie ustalonej pozycji. Stacja referencyjna za pomocą systemu różnicowego DGPS (ang. Differential GPS) oblicza i emituje dodatkowe parametry korekcyjne, niwelujące znaczną część błędów spowodowanych celowym przekłamywaniem informacji nawigacyjnych S/A (ang. Selective Availability) oraz wynikających z różnic w propagacji sygnałów przez przyległe ścieżki jonosfery.

przez sieć do systemu użytkownika docelowego. Zawiera co najmniej trzy elementy: fazę ustanowienia połączenia, fazę transferu właściwego i fazę rozłączenia. Odmianą tej komutacji jest wielostrumieniowa komutacja kanałów;

- komutację pakietów i wiadomości (w tym również głosu w postaci pakietowej), uważaną za najbardziej elastyczną technikę komutacji, przydatną dla użytkowników nawiązujących wielokrotne połączenia z wieloma klientami, zwłaszcza o zmiennej ilości danych. Informacja dzielona na pakiety stałej długości (nagłówek plus dane) jest przesyłana przez sieć jedną z dwóch metod: bezpołączeniową (datagramy informacji - bez potwierdzania odbioru) i połączeniową - wymagającą zestawienia kanału logicznego przez sieć przed przesłaniem pakietów. Wirtualne połączenia logiczne mogą mieć charakter tymczasowy SVC (ang. Switched Virtual Circuit) bądź trwały PVC (ang. Permanent Virtual Circuit). Odmianą komutacji pakietowej tworzonej w łączach o dobrej jakości jest technika komutacji ramek, w której z uwagi na małe prawdopodobieństwo przekłamań zredukowano zakres kontroli przepływu i korekcji błędów w poszczególnych węzłach tranzytowych sieci, a ramki błędne bądź niekompletne są po prostu usuwane;
- komutację komórek, stanowiącą odmianę szybkiej komutacji pakietowej liczonej w Gb/s (np. ATM), z przeznaczeniem do przekazów przez łącza o bardzo wysokiej jakości, czyli światłowodowe. Dane pierwotne są porcjowane na komórki o małej długości (53 bajty), a transmisja dokonuje się zwykle w trybie połączeniowym, co umożliwia efektywny przekaz informacji w czasie rzeczywistym. Obsługą problemów związanych z pakietami zagubionymi, uszkodzonymi bądź przesłanymi w niewłaściwej kolejności zajmują się systemy użytkowników końcowych, a nie sieć transmisyjna (z komutacją komórek).

Komutacja kanałów (KK) polega na tworzeniu, na żądanie, pomiędzy dwiema lub więcej stacjami końcowymi drogi połączeniowej do ich wyłącznego użytku aż do chwili rozłączenia. Charakteryzują ją: dużo istotnych wad jak i niewielka ilość zalet (Tabela 2.5.).

krążących po kołowych orbitach pośrednich, rozmieszczonych na dwóch orbitach o inklinacji 45°. Wykorzystuje 10 lub 12 satelitów krążących w odległości 10 355 km od powierzchni Ziemi. Współpracę systemu ICO z systemami radiokomunikacji ruchomej lądowej publiczną siecią telefoniczna uzyskuje się za pomocą 12 węzłów dostępu do platformy kosmicznej SAN (ang. Satellite Access Node). Podręczne telefony systemu ICO mają dwa tryby pracy typu DM. Jeżeli abonent znajdzie się w zasięgu działania naziemnego systemu komórkowego (np. GSM), to telefon automatycznie będzie się kontaktował z tym systemem.

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

Ad. 2. Systemy komutacji

Ad. a) komutacja połączeń

Tradycyjna telekomunikacja oparta na komunikacji porozumiewawczej - obejmującej usługi telefoniczne, telegramowe i teleksowe - wymaga kanałów o niewielkiej przepływności, wykorzystujących prawie wyłącznie analogowe linie telefoniczne z podstawowym pasmem przenoszenia w zakresie 300-3400 Hz. Istotne zmiany w telekomunikacji stały się możliwe po opanowaniu cyfrowej techniki kodowania mowy, wprowadzeniu techniki zwielokrotnienia kanałów oraz światłowodów dla rozszerzenia pasma transmisji, a przede wszystkim włączeniu do sieci telekomunikacyjnej elementów komutacji (przełączania) pochodzących z technologii sieci komputerowych.

Wśród kilku popularnych technik telekomutacyjnych zawiadujących przesyłaniem informacji przez sieć należy wyróżnić następujące sposoby komutacji:

- komutację kanałów (połączeń, układów, linii) wymagającą przed przesłaniem informacji zestawienia dedykowanej trasy od źródła przekazu

odtwarzane (zestawiane) w stacji końcowej. Pakiety mają ściśle określoną strukturę obejmującą: nagłówek zawierający adres i informacje sterujące, część wiadomości oraz informacje zabezpieczające przed błędami. W bilansie wad i zalet przeważają zalety (Tabela 2.6.).

Tabela 2.6. Zalety i wady komutacji pakietów

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

Źródło: *Kierowanie obronnością państwa w stanach nadzwyczajnych*, Praca naukowa pod kier. M. Krauze, AON, Warszawa 2000, s. 126.

Systemy komutacji pakietów są sprawdzonym rozwiązaniem w zastosowaniu do teleinformatyki i na jej bazie budowane są współczesne publiczne sieci pakietowe (np. krajowa sieć POLPAK), sieci dedykowane tj. przeznaczone dla potrzeb określonych grup użytkowników (np. sieci krajowe TELBANK, KOLPAK, NASK itp.) oraz wojskowe (np. planowana do rozwinięcia w ubiegłym dziesięcioleciu sieć powiadamiania i alarmowania WP- FUNKIA), sieci dla potrzeb rodzajów wojsk i służb (dla potrzeb logistyki) jak i sieci kierowania systemami i środkami walki. Konsekwencją natłoku w sieci z komutacją pakietów jest wydłużenie kolejek pakietów czekających na obsługę i wynikające stąd opóźnienia w dostarczaniu pakietów do odbiorcy. Do współpracy sieci pakietowych z sieciami o innych technikach komutacji na styku „węzeł-węzeł" stosowane są urządzenia pośredniczące - konwertery międzysieciowe, których funkcja polega na wzajemnym dopasowywaniu różnych kodów, szybkości transmisji oraz protokołów komunikacyjnych.

Komutacja wiadomości (KW), jako odmiana komutacji pakietów, polega na tym, że informacje (o różnych długościach) są przesyłane pomiędzy stacjami końcowymi w postaci wiadomości zawierających adres stacji docelowej (mogą być magazynowane w węzłach sieci). Komutacja wiadomości jest najbardziej typowym

Tabela 2.5. Wady i zalety komutacji kanałów

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

Źródło: *Kierowanie obronnością państwa w stanach nadzwyczajnych,* Praca naukowa pod kier. M. Krauze, AON, Warszawa 2000, s. 124.

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

Komutacja pakietów (KP) jest również przykładem metody „zapamiętaj i prześlij". W odróżnieniu od komutacji wiadomości, w systemach z komutacją pakietów informacja jest wymieniana pomiędzy stacjami końcowymi w postaci grup elementów binarnych o ograniczonej długości zwanych pakietami. Długie wiadomości są przed przesłaniem ich w sieci dzielone na pakiety, a następnie

przenoszenia lub poprzez kosztowne międzycentralowe urządzenia zwielokrotnienia częstotliwościowego o niewielkiej krotności kanałów rozmownych. Jako linie przesyłowe były wtedy stosowane wyłącznie pary kabli miedzianych o ograniczonej częstotliwości pracy, wymagające skomplikowanych filtrów, korektorów linii (pupinizacja, krarupizacja) i tłumików zakłóceń przy przesyłaniu sygnału o większych częstotliwościach.

Sytuacja radykalnie uległa zmianie wraz z wprowadzeniem przekształcenia sygnału mowy na postać cyfrową za pomocą techniki modulacji kodowo-impulsowej PCM (ang. Pulse Coce Modulation). Koncepcja tej techniki, która jest fundamentem telefonii cyfrowej, została opatentowana już w 1926 r. Jednak dopiero 1962 r. zastosowano ten wynalazek w telekomunikacji przy budowie 24-kanałowego traktu PCM o przepływności T1 (1,544 Mb/s), a następnie 96-kanałowego systemu o przepływności T2 (6,312 Mb/s), oddanego do eksploatacji w 1972 r. Technika ta umożliwia konwersję standardowego sygnału mowy w paśmie podstawowym około 4 kHz (niekiedy 7 kHz) na postać cyfrową przez ciągłe próbkowanie amplitudy z częstotliwością 8 kHz (co 125 us) i kodowanie tych wartości w ciąg znaków 8 bitowych (256 różnych wartości), uzyskując podstawową przepływność binarną 64 kb/s. Kanał o tej przepływności jest podstawą do komutacji na wyższych poziomach multipleksowania (krotnice telefonii nośnej).

Multipleksowanie PCM. Znormalizowane cyfrowe kanały rozmowne o przepływności 64 kb/s stały się podstawą do tworzenia strumieni cyfrowych o dużej przepływności przez łączenie pojedynczych kanałów metodą zwielokrotnienia cyfrowego z podziałem czasowym TDM (ang. Time DMsion Multiplexing). Sposób ten umożliwia wprowadzenie pojedynczych bajtów z kolejnych kanałów PCM do szczelin czasowych jednego strumienia zbiorczego, co odpowiada klasycznej komutacji kanałów w systemach cyfrowych, zwanej w telekomunikacji multipleksowaniem za pomocą krotnic telekomunikacyjnych.

Multipleksowanie kanałów PCM jest realizowane odmiennie na różnych kontynentach, przy czym wyróżnia się dwa przyjęte standardy multipleksowania kanałów o przepływności 64 kb/s:

- do/z strumienia zbiorczego o przepływności 1544 kb/s (24x64 kb/s) na kontynencie północnoamerykańskim i w Japonii;

przykładem metody „zapamiętaj i prześlij". Również ona ujawnia zalety jak i wady (Tabela 2.7.).

Tabela 2.7. Zalety i wady komutacji wiadomości

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

Źródło: *Kierowanie obronnością państwa w stanach nadzwyczajnych*, Praca naukowa pod kier. M. Krauze, AON, Warszawa 2000, s. 125.

Jest ona szczególnie przydatna do organizacji systemów dystrybucji wiadomości MHS (ang. Message Handling Systems). Na bazie komutacji wiadomości może być organizowana np. poczta elektroniczna (e-mail) oraz współpraca służb teleksowych i teletekstowych. Komutacja wiadomości znajduje zastosowanie w sieciach teleinformatycznych „cywilnych" oraz wojskowych. W systemach wykorzystujących komutację wiadomości zachodzi na ogół konieczność dodatkowej strukturyzacji informacji dla celów transmisyjnych.

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

Ewolucja komutacji. W systemach telekomunikacyjnych do połowy lat siedemdziesiątych stosowano powszechnie technikę przesyłania sygnałów analogowych za pomocą kanałów telefonicznych w podstawowym paśmie

Ze względu na realizowane funkcje istnieje bardziej szczegółowa specjalizacja uwzględniająca podział central na: abonenckie, miejskie, satelickie, wyniesione (oddalone), tandemową tranzytowe, międzymiastowe i międzynarodowe, jak też ci mieszanym charakterze – łączące kilka podanych funkcji. Podział ten w miarę wzrostu integracji między siecią telekomunikacyjną i komputerową ulega stopniowemu zanikowi.

Centrale analogowe. Pierwsze systemy automatycznych central telefonicznych (analogowych) działały w systemie bezpośrednim opartym na impulsach wybierczych - nadawane tarczą numerową abonenta bez rejestracji numeru w centrali -wprost na wybieraki centrali komutującej. Poszczególne cyfry (serie impulsów wybierczych) powodowały bezpośrednio „krok po kroku" zestawianie trasy kolejnych odcinków, co prowadziło do usztywnienia funkcji trasowania całości połączenia.

Zwiększenie elastyczności trasowania uzyskano w systemach rejestrowych, w których impulsy wybiercze są najpierw pamiętane w rejestrach, a po zakończeniu nadawania numeru służą do budowania w miarę bezkolizyjnej drogi połączeniowej. Największy postęp w automatyzacji central analogowych uzyskano przez wprowadzenie systemów elektronicznych do trasowania połączeń, wśród których wyróżnia się:

- quasi-elektroniczne - w których sterowanie jest elektroniczne, a wybieraki połączeń pozostają nadal elektromechaniczne (biegowe, podnosząco-obrotowe, krzyżowe);
- systemy całkowicie elektroniczne - o przestrzennym i czasowym rozdziale dróg rozmownych w polu komutacyjnym.

Cechą charakterystyczną wszystkich central analogowych jest przekaz i komutacja sygnałów głosowych w postaci analogowej (bez cyfrowego przetwarzania głosu) w obrębie systemu komutacji.

Sieci tranzytowe. Początkowo telefoniczne sieci tranzytowe, działające między centrami komutacji, wykorzystywały telefonię nośną, zastępującą grube wiązki międzycentralowe z setkami par linii telefonicznych transmitujących przekazy głosowe w naturalnym paśmie kanału o szerokości 4 kHz (300÷3400 kHz). W systemach telefonii nośnej następuje zwielokrotnienie częstotliwościowe

- do/z strumienia o przepływności 2048 kb/s (30x64 kb/s) w Europie.

W europejskim systemie multipleksowania z podziałem czasowym TDM stosuje się ramkę o 32 szczelinach i czasie trwania 125 :s, w której dwie szczeliny są przeznaczone odpowiednio do synchronizacji F (ang. Framing) i sygnalizacji S (ang. Signaling), natomiast pozostałe, do przenoszenia bajtów informacyjnych z kolejnych 30 kanałów PCM, tworząc w ten sposób strumień zbiorczy E 1 o przepływności 2048 kb/s, oznaczany zwykle 2 Mb/s.

Łącze telekomunikacyjne. Główne łącze telekomunikacyjne jest identyfikowane z każdym łączem typu telekomunikacyjnego, zakończonym u użytkownika urządzeniem końcowym, zwanym terminalem. W centrali końcowej łącze główne jest skojarzone z przyporządkowanym mu numerem abonenckim.

Istnieją dwa rodzaje zakończeń łączy telekomunikacyjnych: terminalem indywidualnym, zespołem terminali w zakończeniu grupowym. Typowymi zakończeniami terminali indywidualnych są: aparat telefoniczny, urządzenie faksujące, modem, komputer osobisty lub coraz częściej spotykane wideo konferencyjne i multimedialne aparaty abonenckie. Zakończeniem grupowym są najczęściej centrale abonenckie typu PABX, spełniające funkcje reduktorów łączy telekomunikacyjnych. W zależności od wielkości generowanego trafiku liczba łączy głównych przeznaczonych do obsługi PABX lub wyniesionych stacjonarnych modułów komutacji może być różna, jednak zawsze mniejsza (redukcja) od liczby przyłączonych do nich abonentów. W języku potocznym łącze główne jest zwykle niezbyt precyzyjnie identyfikowane z linią miejską systemu komutacji lub łączem abonenckim.

Ad. b) centrale analogowe

Klasyfikacja central. Istnieje kilka sposobów klasyfikacji systemów komutacyjnych. Za względu na formę prezentacji przekazów głosowych rozróżnia się centrale:

- analogowe, z komutacją sygnałów analogowych (pasmo 4 kHz);
- cyfrową i przetwarzaniem głosu na postać cyfrową PCM64 (64 kb/s);
- zintegrowane, w których oprócz cyfrowego przekazu głosy możliwa jest integracja wielu usług (teleks, telefaks, poczta elektroniczna, poczta głosowa, usługi Internetu, usługi obrazowe, sieci komputerowe i inne).

modulacji kodowo-impulsowej PCM. Dotychczasowe linie abonentów analogowych mogą być dołączone do centrali cyfrowej (cyfrowego systemu komutacji) przez kodek PCM znajdujący się na obrzeżu systemu komutacji, natomiast cyfrowe linie abonenckie są przyłączone bezpośrednio do portów wyjściowych traktowanych jako łącze główne systemu komunikacji. Kodek brzegowy PCM zamienia dwukierunkowy sygnał analogowy symetrycznej linii abonenckiej na dwa jednokierunkowe tory cyfrowe, każdy o przepływności 64 kb/s. Sygnały cyfrowe PCM 64 mogą być komutowane bezpośrednio z innymi abonentami tego samego systemu lub podlegają zwielokrotnieniu przed ich przesłaniem do innego systemu komutacji. Taka koncepcja pozwala na całkowicie cyfrowe komutowanie, przetwarzanie i przesyłanie informacji oraz sygnalizacji na wszystkich poziomach wielowarstwowej sieci telekomunikacyjnej.

Rewolucyjne zmiany w cyfrowych systemach komutacji nastąpiły w momencie, gdy okazało się, że tanie sieci pakietowe pierwotnie przeznaczone do transmisji danych nadają się do przekazów głosowych prowadzonych w czasie rzeczywistym. Stało się to możliwe, dzięki znacznemu postępowi w technikach konwersji głosu do postaci cyfrowej PCM 64 kb/s (G.711), a następnie jego kompresji do strumienia o przepływności kanałowej: początkowo 32 kb/s (G.723), 16 kb/s (G.728), 8 kb/s (G.729) i 6,3 kb/s (G.723.1), a obecnie 5,3 kb/s (G.723.1). Są one uzyskiwane z wykorzystaniem szybkich procesorów sygnałowych DSP (ang. Digital Signal Processing), jeszcze nie w pełni powszechnie dostępnych w rozwiązaniach komercyjnych.

Integralną cechą nowoczesnego systemu komutacji jest cyfrowe pole komutacyjne, umożliwiające przestrzenno-czasowy rozdział szczelin czasowych TDM (ang. Time DMsion Multiplexing) między wszystkimi współpracującymi modułami komunikacyjnymi centrali komutującej. Zapewnienie bezkonfliktowej komutacji wymaga zwykle stosowania światłowodowego medium transmisyjnego o gigabitowej przepływności bitowej, w którym znajduje się kilkadziesiąt tysięcy przyporządkowanych na stałe lub zmiennych w czasie szczelin. Swobodna alokacja szczelin czasowych w topologii sieci komutującej jest najnowszym rozwiązaniem komutatorów przestrzenno-szczelinowych. Topologie sieci komutującej mogą przyjmować różne formy: cyfrowej sieci pierścieniowej, kratowe) lub mieszanej;

kanałów rozmownych przez przesunięcie podstawowego pasma 4 kHz w odpowiednio wyższe zakresy częstotliwości, oddzielnie dla każdej rozmowy. Po stronie odbiorczej analogowa postać sygnałów mowy jest rozdzielana za pomocą filtrów pasmowych (4÷8 kHz, 8÷12 kHz, 12÷16 kHz itp.) na pojedyncze kanały rozmowne. Kłopotliwy proces wzmacniania i filtracji kanałów analogowych telefonii wielokrotnej był jednym z głównych powodów niskiej jakości rozmów i przesłuchów, co doprowadziło do ewolucji tych łączy w kierunku tranzytowych sieci cyfrowych.

Funkcjonujące do tej pory pojęcie sieci tranzytowej opartej m centralach tranzytowych traci stopniowo na znaczeniu. Warstwowa struktura sieci transportowych PDH i SDH (także ATM) na najwyższych poziomach komutacji funkcjonuje obecnie za pomocy węzłów cyfrowych łączących poszczególne fragmenty sieci synchronicznych o różnych przepływnościach, poczynając od szybkości 155 Mb/s w górę. Instalacja krotnic synchronicznych DXC, SXC oraz różnorodnych typów multiplekserów ADM (ang. Add Drop Multiplexer), działających bezpośrednio na torach optycznych ze zwielokrotnieniem falowym WDM, gwarantuje optymalne wykorzystanie przepustowości istniejących kanałów światłowodowych między systemami komutacji na różnych poziomach multipleksacji.

Ad. c) centrale cyfrowe

Określenie systemów komutacji nie jest obecnie jednoznaczne. Tradycyjnie obowiązujący do tej pory podział na systemy komutacji (centrale telefoniczne powyżej 10 000 abonenckich numerów NN) i centrale lokalne (prywatne, zakładowe) przestaje funkcjonować, gdyż wiele abonenckich systemów cyfrowych PABX może już obsługiwać trafik[138] powyżej 25 000 numerów NN przejmując większość funkcji komunikacyjnych z nadrzędnych systemów komutacjii umożliwiając trafik powyżej 10 000 erlangów[139].

Zasadniczym przełomem w rozwoju central i systemów komutacji było wprowadzenie do telekomunikacji cyfryzacji sygnałów głosowych za pomocą

---

[138]Trafik – wartość średniego natężenia ruchu w kanale telefonicznym, złączu lub węźle sieciowym.

[139]Erlang – jednostka natężenia ruchu (trafiku) w liniach i węzłach komutacji telefonicznej określająca średnią intensywność ruchu telefonicznego. Jeden erlang oznacza ruch, w którym jedno łącze telefoniczne jest ciągle zajęte np.: jednogodzinna rozmowa w ciągu godziny.

- □ teledacyjne sieci z komutacją kanałów CSPDN (ang. Circuit Switched Public Data Network);
- □ teledacyjne sieci z komutacją pakietów PSPDN (ang. Public Switched Packet Data Network);
- □ sieci telegraficzne (Telex);
- □ radiotelefoniczne sieci komórkowe MT (ang. Mobile Telephony), a także wiele sieci wydzielonych o charakterze lokalnym lub prywatnym (PABX, LAN, dyspozytorskie, specjalne).

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

- międzynarodowych, central międzymiastowych i niektórych central okręgowych i zespolonych;
- system krzyżowy (Pentaconta 1000C, K66, LNI) na poziomie central okręgowych, międzymiastowych, także zespolonych;
- system elektroniczny (E-1OA) na poziomie central okręgowych;
- nowoczesne systemy komutacji cyfrowej (Alcatel 1000 S12, Lucent Technologies 5ESS-2000, 5ESS/7R/E, Siemens EWSD, krajowe DGT 3450) działające w najwyższych i środkowych warstwach sieci telekomunikacyjnej na poziomie łączy międzynarodowych, central międzymiastowych i niektórych central okręgowych i zespolonych.

Ad. d) sieć inteligentna IN

Początek usług telekomunikacyjnych datuje się od zastosowania aparatu telegraficznego w połowie ubiegłego stulecia. Przez ponad 100 lat standardową ofertą sieci była stacjonarna usługa POTS (ang. Plain Old Telephone Service) nawiązująca do transmisji głosu przez komutowane łącza telefoniczne. Dopiero od niedawna usługi realizowane przez sieci telekomunikacyjne analogowe i cyfrowe rozwinęły się w kilka dziedzin: usługi głosowe, dźwiękowe, tekstowe, graficzne, obrazowe i transmisji danych, zarówno dla abonentów stacjonarnych, jak i znajdujących się w ruchu.

Rozwój środków telekomunikacji satelitarnej i naziemnej (przewodowej, światłowodowej i radiowej) dał podstawy do zastąpienia klasycznej stacjonarnej usługi telefonicznej POTS usługą audiowizualną z dystrybucją dźwięku wysokiej

stosowane najczęściej topologie mieszane stanowią Indywidualną i chronioną cechę każdego systemu komutacji.

Sposób zarządzania siecią telekomunikacyjną określa architektura funkcjonalna zwana TMN (ang. Telecommunication Management Network). Definiuje ona funkcje związane ze sterowaniem, monitorowaniem i rejestrowaniem zasobów sieci w celu zapewnienia efektywnego jej wykorzystania zgodnie z przeznaczeniem. Funkcje zarządzania telekomunikacją TMN obejmują następujące obszary działań:

- □ administrowanie - zmierzające do wspomagania świadczenia usług telekomunikacyjnych;
- □ sterowanie - ujmujące zbiór działań technicznych do realizacji funkcji i adaptacji do zachodzących zmian w otoczeniu telekomunikacji;
- □ utrzymanie - obejmujące technikę zapewniającą sprawne funkcjonowanie sieci;
- □ zabezpieczanie - ma na celu planowanie i przygotowanie do wdrożeń nowych cech usług sieci telekomunikacyjnej w przyszłości.

Zasadnicze funkcje TMN są zgrupowane w dwóch kategoriach:

- ▪ ogólnej -wspólna dla wszystkich systemów komutacyjnych (przesyłanie, przechowywanie, wyszukiwanie, przetwarzanie i ochrona informacji);
- ▪ aplikacyjnej - obejmująca podstawowy zbiór funkcji zarządzania aplikacjami (zarządzanie konfiguracją, uszkodzeniami, jakością, bezpieczeństwem i taryfikacją).

Elastyczna realizacja zarządzania TMN ma konfigurowalne styki Q3, umożliwiające śledzenie, nadzór i monitorowanie stanu użytkowników sieci oraz prowadzenie dialogu za pomocą sekwencji ekranów wejściowych, a także generowanie sygnałów wyjściowych do sterowania siecią telekomunikacyjną w celu jej naprawy lub optymalizacji.

Systemy komutacji w Polsce. W Polsce działa wiele typów sieci telekomunikacyjnych o charakterze publicznym:

- □ komutowane sieci telefoniczne PSTN (ang. Public Switched Telephone Network);

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

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

W efekcie narzuconych zebranych na świecie doświadczeń i analizy zapotrzebowań na nowe niestandardowe usługi telekomunikacyjne stworzono uniwersalną koncepcję, obejmującą rozwiązania techniczne, sposoby ich świadczenia i nadano jej nazwę sieci inteligentnej[142] (Mapa 2.2.).

Budowa sieci inteligentnej umożliwia operatorowi natychmiastowe reagowanie na zapotrzebowanie rynku telekomunikacyjnego i pełną otwartość na potrzeby klienta, praktycznie niezależnie od użytkowanej infrastruktury telekomunikacyjnej.

Zainteresowanie usługami IN wynika przede wszystkim z ich dużego znaczenia dla zastosowań komercyjnych, które mają pośredni lub bezpośredni wpływ na wyniki działalności firmy. Pomagają one poprawić wyniki ekonomiczne (zwiększenie obrotu w wyniku poprawy jakości usług i ułatwienia kontaktów z klientami, możliwości telefonicznego składania zamówień, uzyskiwania informacji i pomocy, np. serwisowej, przeprowadzanie teleankiet badających zapotrzebowanie rynku itp.).

Analiza rozwoju usług sieci IN dowodzi, że dokonywał się on etapowo, poszerzając z etapu na etap skalę i zakres swej funkcjonalności. Ogólnie można stwierdzić, że sieć inteligentna IN (ang. Intelligent Network) stanowi pojęciowy model fizycznej sieci telekomunikacyjnej, identyfikowany jako środek zwiększający atrakcyjność istniejących usług przez ofertę nowych, dodatkowych usług telekomunikacyjnych.

---

[142]TP S.A. rozpoczęła eksploatację sieci IN na istniejącej strukturze sieci telekomunikacyjnej według projektu firmy Siemens.

jakości, zapewniając komunikację typu „każdy z każdym"- niezależnie od miejsca pobytu abonentów.

Sieć inteligentna (IN – ang. Inteligent Network). Przez pierwsze lata historii rozwoju telefonii głównym problemem było zapewnienie dostatecznej liczby łączy telefonicznych o odpowiedniej jakości, dających możliwość nieograniczonej realizacji połączeń telefonicznych na dowolną odległość. Problem ten stał się podstawowym i na nim skupiała się uwaga wszystkich operatorów sieci telekomunikacyjnych. W miarę rozwoju sieci telefonicznych abonentom przestały wystarczać klasyczne usługi telefoniczne i pojawiło się zapotrzebowanie na coraz bardziej złożone usługi realizowane za pomocą aparatu telefonicznego. w początkowym okresie rozwoju telefonii, „inteligencja", sieci była w dużym stopniu zapewniana przez personel central, który dbał o właściwy przebieg scenariuszy realizacji usługi.

Od kilkunastu lat inteligencja jest wprowadzana na wszystkich poziomach sieci, za pomocą specjalizowanych systemów komputerowych i oprogramowania, które są w różny sposób integrowane z podstawową infrastrukturą sieci telefonicznej. Istnieje wyróżniona koncepcja techniczna, definiująca znormalizowaną architekturę sieci, zestaw usług i zasady ich kreacji, która jest określana terminem sieci inteligentnej. Istotą sieci inteligentnej jest odseparowanie podstawowych funkcji komutacyjnych od funkcji związanych z realizacją scenariuszy usług[140]. Sieć telefoniczna jest, więc wzbogacana o elementy umożliwiające wykonywanie tych funkcji.

Z punktu widzenia użytkownika sieci telefonicznej, usługa inteligentna umożliwia indywidualizację realizacji usługi podstawowej, wykorzystanie dodatkowej informacji (dostarczanej przez abonenta lub odwrotnie, niejawnej dla abonenta), pozwala na wirtualizację środowiska realizacji usług. Z punktu widzenia operatora, usługa inteligentna jest odwołaniem się do obiektów nadzorujących realizację usługi z wykorzystaniem informacji zawartej w bazach danych. „Inteligencja" sieci jest, zatem zawarta w oprogramowaniu[141]. Warto zauważyć

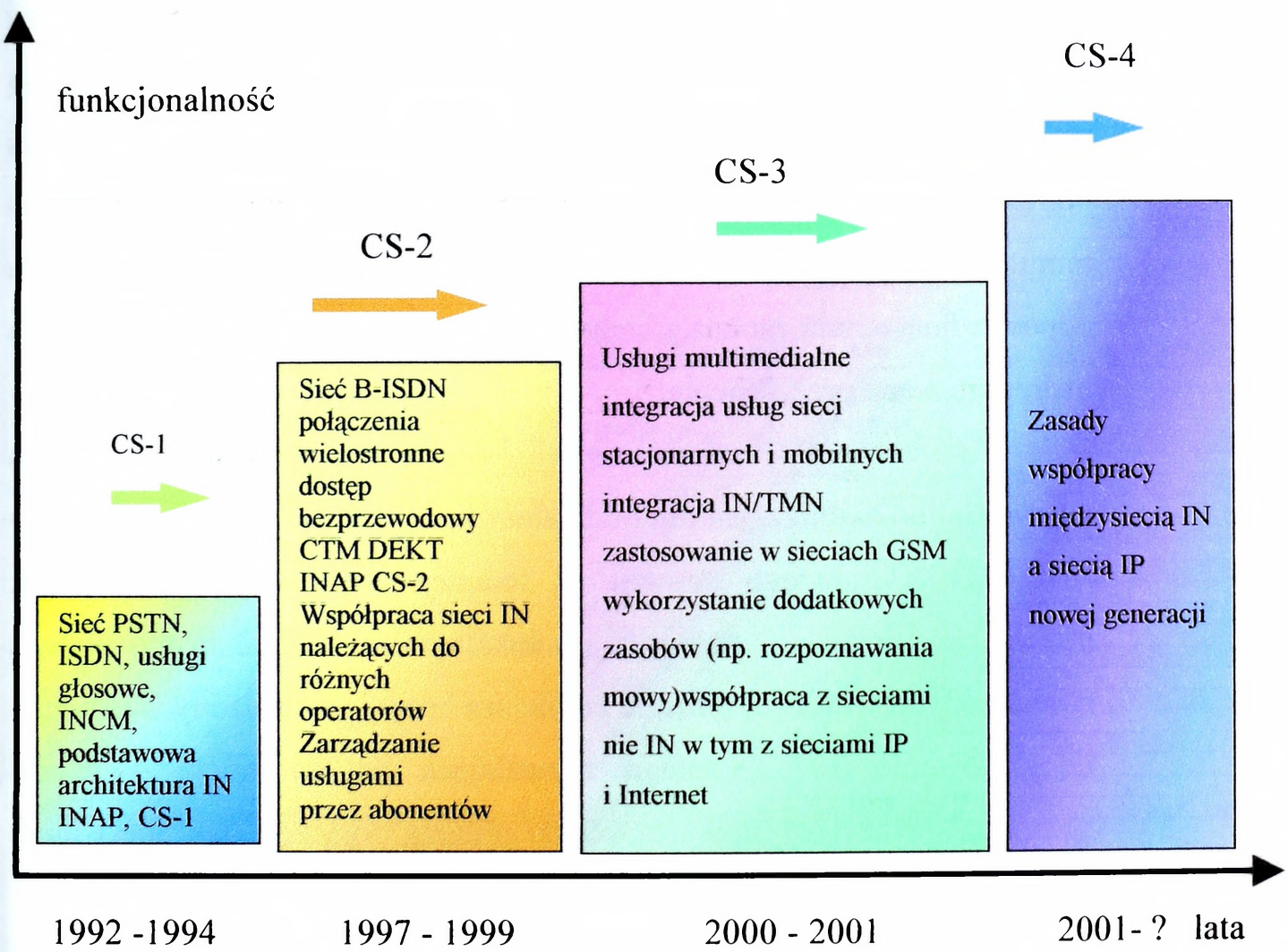
---

[140]Por. M. Bromirski, *Sieci inteligentne w telekomunikacji,* Instytut Łączności, Warszawa 1999.
[141]Por. M. Średniawa, *Sieci inteligentne – architektura, usługi, zastosowania,* Politechnika Warszawska, Warszwa 1998.

- usługa sieciowego Centrexu (AWC);
- połączenia rozliczane kartą VCC (Virtual Card Calling);
- uniwersalna łączność osobista UPT (ang. Universal Personal Telecommunication);
- poczta głosowa VMS (ang. Voice Message Service);
- wybieranie numeru głosem VAD (ang. Voice Activated Dialing).

Wykres 2.1.

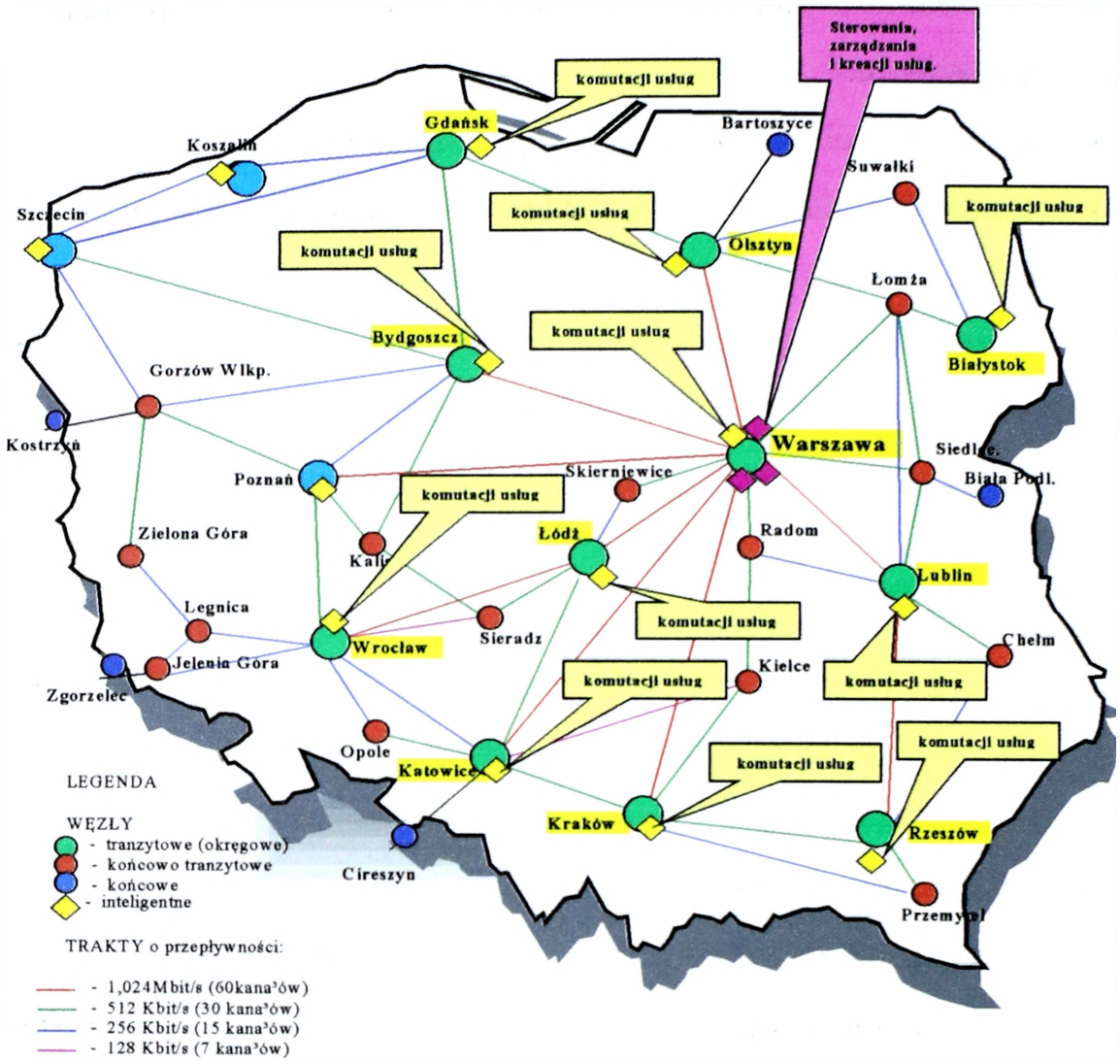
Etapy rozwoju usług sieci inteligentnej



Źródło: W. Ziemski, *Usługi sieci inteligentnej*, TP S.A., Warszawa 1998, s. 27.

Realizacja większości tych usług jest już w ofercie operatorów telekomunikacyjnych stosujących nowoczesne systemy komutacji CM i PABX, wyposażone dodatkowo w inteligentne węzły komunikacyjne (systemy komputerowe o dużej mocy obliczeniowej typu RISC, procesory sygnałowe DSP, pamięci dyskowe o pojemności rzędu kilku gigabajtów). Pierwsze cztery usługi

Mapa 2.2. Struktura sieci inteligentnej IN (Uproszczony)



Źródło: Opracowanie własne na podstawie materiałów firmy Siemens.

W większości usługi sieci inteligentnej IN są oparte na istniejącej sieci cyfrowej i wykorzystują specjalizowane rozwiązania producenta lub operatora sieci telekomunikacyjnej, wśród których dominuje zestaw podstawowy CS - 1, wszechstronnie już sprawdzony w eksploatacji (Wykres 2.1.). Należą do niego następujące usługi rozszerzone, już realizowane przez sieć inteligentną:

- bezpłatne połączenia telefoniczne FPH (Freephone);
- interaktywna odpowiedź głosowa IVR (Interactive Voice Response);
- wydzielona sieć wirtualna VPN (Virtual Private Network);
- połączenia z opłatą prowizyjną (PRS);
- teleglosowanie TVS (TeleVofmg Service);

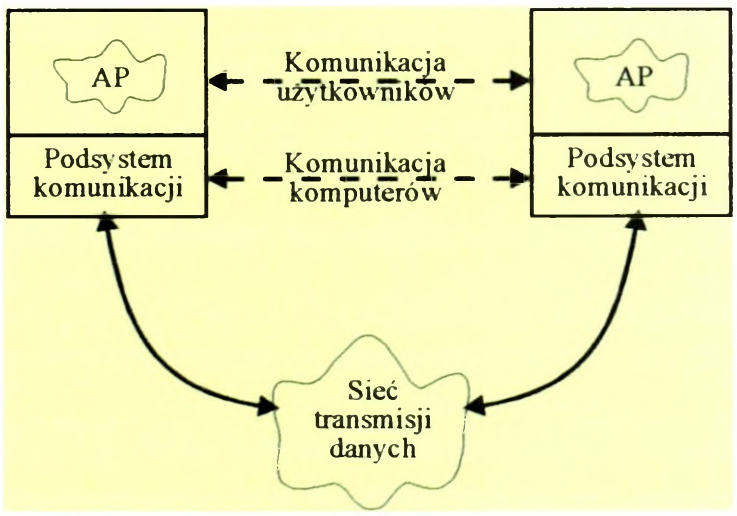
transmisja między dwiema innymi stacjami. Aby w tak rozumianej sieci informacje wysyłane przez określoną stację nadawczą trafiły do określonej stacji odbiorczej, każda z nich musi mieć swój adres wyróżniający ją spośród innych stacji zainstalowanych w sieci.

Sieci komputerowe mogą być zbudowane w różny sposób, ale zawsze w ich architekturze można wyróżnić trzy podstawowe, hierarchicznie uporządkowane elementy (Schemat 2.10):

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

Schemat 2.10.

Podstawowe elementy sieci komputerowych



Źródło: Opracowanie własne na podstawie: *Net World Vademecum teleinformatyka cz. 1*, International Data Group Poland S.A., Warszawa 2004, s.123.

Wyraźnie w literaturze przedmiotu rozróżniane są dwa pojęcia: sieć i intersieć. Najczęściej w języku polskim zarówno sieć, jak i intersieć są nazywane siecią. Intersieć po prostu, jest większą i bardziej złożoną siecią. Intersieć składa się z wielu sieci najczęściej połączonych routerami pełniących rolę urządzeń kierujących pakiety między sieciami. Sieci w intersieci mogą być także łączone innymi urządzeniami intersieciowymi, na przykład mostami. W intersieci każda sieć musi mieć swój unikatowy adres, a w ramach danej sieci - każda stacja sieciowa. Ćwierć wieku temu w pierwszych sieciach komputerowych stosowano duże

sieci inteligentnej IN w krajowej sieci telekomunikacyjnej TP SA uruchomiła w lutym 1999 r. Należą do nich następujące usługi:

- linia bezpłatna 800 (0-800) stanowiąca unowocześnioną wersję dotychczasowej usługi Infolinii 0-800 - świadczonej przez TP SA już od 1995 r. Korzystanie z numeru z prefiksem 800 jest bezpłatne dla klienta niezależnie od miejsca wywoływania połączenia, a pełny koszt usługi ponosi wyłącznie abonent tej usługi (agencja badań rynkowych, media, firma zainteresowana bezpośrednim informowaniem o swoich promocjach, produktach i usługach);
- linia ulgowa 801 z umownym podziałem opłaty taryfikacyjnej między abonenta wywołującego i właściciela usługi. Abonenci tej usługi mają trzy warianty podziału kosztów połączenia: opłata tylko za jeden impuls niezależnie od czasu trwania połączenia, impuls za każde rozpoczęte trzy minuty rozmowy bądź zaliczanie impulsu za każdą minutę. Za odpowiednią opłatą można ubiegać się o numery „srebrne", „złote" lub zaproponowane przez klienta;
- linia firmowa 804 umożliwiającą automatyczne łączenie klienta z terytorialnie najbliższym mu oddziałem firmy, sklepu, usługi, policji czy straży. Oferta jednego numeru na terenie całego kraju (zapowiedzi, informacje miejscowe, połączenia z lokalnym oddziałem firmy) ułatwia kontakt użytkownikowi, a firmie zmniejsza koszty prowadzonych usług;
- teległosowanie 707 - usługa zezwalająca na rejestrację – w celu późniejszego użytkowania - nawet do miliona połączeń (tak, nie i inne) przychodzących w ciągu jednej godziny.

Ad. 3) Sieci komputerowe

Siecią komputerową nazywamy strukturę składającą się ze stacji sieciowych i łączącego je kabla sieciowego, ogólnie zwanego medium transmisyjnym. Inaczej mówiąc, jedna sieć ma jeden wspólny dla wszystkich stacji kabel sieciowy, służący do transmisji informacji między nimi.

W praktyce oznacza to, że w tym samym momencie, gdy w sieci odbywa się przesyłanie informacji między dwiema stacjami sieciowymi, nie może odbywać się

oprogramowania i sprzętu. Pozostałe warstwy niższe są realizowane programowo. Najniższa warstwa (fizyczna) jest najbliższa medium transmisyjnego (kabla sieciowego) i jest odpowiedzialna za przesyłanie informacji ze stacji do tego medium (i odwrotnie). Często jest używany termin wyższa warstwa. Oznacza on dowolną warstwę znajdującą się powyżej innej warstwy w modelu OSI.

Schemat 2.11.

Funkcje realizowane przez warstwy modelu OSI/ISO

	Funkcje specyficzne aplikacji
7	***Usługi rozproszonego przetwarzania danych***
	Warstwa aplikacji Transfer plików (FTAM - File Transfer, Access and Manipulation) Transfer dokumentów (EDE - Electronic Data Exchange) Transfer zadań (JTM - Job Transfer and Manipulation)
6	***Usługa wymiany wiadomości** (niezależna od składni)*
	Warstwa prezentacji Przekształcanie formatu danych
5	**Warstwa sesji** Sterowanie dialogiem pomiędzy aplikacjami
4	***Usługa wymiany wiadomości** (niezależna od sposobu transmisji)*
	Warstwa transportowa Transfer wiadomości przez sieć (end-to-end), fragmentacja, obsługa błędów
3	**Warstwa sieciowa** Dobór trasy, adresowanie, ustanawianie oraz likwidacja połączeń
2	**Warstwa łącza danych** Niezawodna transmisja pomiędzy węzłami sieci
1	**Warstwa fizyczna** Styki mechaniczne i elektryczne
	Dołączenie fizyczne do medium transmisyjnego
	MEDIUM TRANSMISYJNE

Źródło: *Net World Vademecum teleinformatyka cz. 1,* International Data Group Poland S.A., Warszawa 2004, s.124.

Należy wyraźnie zaznaczyć, że model OSI jest tylko ogólnym modelem koncepcyjnym komunikacji między stacjami podłączonymi do sieci. Model OSI nie określa szczegółowych metod komunikacji. Mechanizmy rzeczywistej komunikacji są określone w formie protokołów komunikacyjnych (ang. Communication Protocols).

komputery oraz podłączone do nich terminale. Rozwiązania takie były używane przez amerykańskie firmy IBM i DEC w systemach: SNA (ang. Systems Network Architecture) i DNA (ang. Digital Network Architecture).

Sieci lokalne - LAN (ang. Local Area Networks) - pojawiły się po uruchomieniu masowej produkcji i upowszechnieniu zastosowań komputerów personalnych PC (ang. Personal Computers). Sieci LAN umożliwiały wymianę zbiorów informacji i komunikatów między użytkownikami znajdującymi się na niewielkim obszarze geograficznym, a także wspólne użytkowanie zasobów, np. serwerów zbiorów.

Sieci rozległe - WAN (ang. Wide Area Networks) - łączą ze sobą oddzielne sieci LAN używając do tego celu zwykłych sieci telefonicznych lub innych mediów. W ten sposób sieci WAN łączą ze sobą geograficznie oddalonych użytkowników. Coraz częściej są stosowane szybkie sieci LAN i przełączane duże sieci - intersieci przede wszystkim dlatego, że - pracując z dużymi przepływnościami - umożliwiają realizację takich zastosowań jak tele- i wideokonferencje.

Do opisu sposobu przepływu informacji między aplikacjami software'owymi w jednej stacji sieciowej a software'owymi aplikacjami w innej stacji sieciowej przy użyciu kabla sieciowego utworzony został model OSI (ang. Open Systems Interconnection). Model OSI jest modelem koncepcyjnym, skomponowanym z siedmiu warstw, z których każda opisuje określone funkcje sieciowe (Schemat 2.11.). Model został opracowany przez ISO (ang. International Standardization Organization) w 1984 r. i w zasadzie powinien być znany przez każdego, kto zajmuje się sieciami komputerowymi.

Model OSI dzieli zadanie przesyłania informacji między stacjami sieciowymi na siedem mniejszych zadań składających się na poszczególne warstwy. Zadanie przypisane każdej warstwie ma charakter autonomiczny i może być implementowane niezależnie. Model OSI składa się z siedmiu niezależnych warstw. Można go podzielić na dwie części: warstwy wyższe i niższe. Warstwy wyższe, związane z aplikacjami, są realizowane programowo. Warstwa najwyższa (aplikacji) jest najbliżej użytkownika. Warstwy niższe modelu realizują transport danych. Warstwy fizyczna i łącza danych są realizowane za pośrednictwem

użytkownikami oraz komunikację między użytkownikami za pośrednictwem poczty elektronicznej i innych aplikacji. Obecnie są stosowane trzy podstawowe technologie sieci LAN:

- Ethernet/IEEE 802.3;
- Token-Ring/IEEE 802.5;
- FDDI (ang. Fiber Distributed Data Interface).

Sieci LAN powinny spełniać trzy istotne wymagania: możliwie dużej przepływności (szybkości), skalowalności i wysokiej niezawodności. Dowolna stacja może rozpocząć transmisję w sieci tylko wtedy, gdy medium (np. miedziany 4-parowy kabel sieciowy) nie jest zajęte przez inną transmisję. Mechanizm kontrolujący stan medium i uruchamiania transmisji nazywamy metodą dostępu do medium. Protokoły LAN używają jednej z dwóch metod dostępu do medium:

- CSMA/CD (ang. Carrier Sense Multiple Access Collision Detect) - wielodostęp z rozpoznaniem stanu kanału i wykrywaniem kolizji;
- Token Passing (ang. Token Passing) - wielodostęp z przekazywaniem uprawnień.

W metodzie dostępu CSMA/CD stacje sieciowe konkurują między sobą o dostęp do medium. Przykładami technologii używających metody dostępu CSMA/CD są: Ethernet, IEEE 802.3 i l00 Base-T.

W metodzie dostępu Token Passing stacje sieciowe uzyskują dostęp do medium w zależności od tego, gdzie aktualnie znajduje się token (specjalna ramka sterująca). Przykładami technologii sieciowych, w których stosuje się metody dostępu Token Passing są: Token-Ring, i FDDI.

Topologia LAN określa sposób wzajemnego połączenia stacji w sieci. Wyróżnia się cztery najczęściej stosowane topologie LAN:

- szynowa;
- pierścieniowa;
- gwiaździsta;
- drzewiasta.

Wymienione topologie są strukturami logicznymi i technicznie nie muszą być w taki sposób zorganizowane. Na przykład logicznie rozumiane topologie szynowa i pierścieniowa są zorganizowane jako gwiazda fizyczna.

Protokołem komunikacyjnym nazywamy zbiór formalnych reguł i konwencji szczegółowo określających mechanizmy wymiany informacji między stacjami połączonymi medium transmisyjnym (kablem sieciowym). Protokół realizuje funkcje jednej lub wielu warstw modelu OSI. Należy dodać, że istniejąca obecnie bardzo duża liczba różnych protokołów komunikacyjnych utrudnia często zorientowanie się w mechanizmach działania sieci.

Pomocne może okazać się uświadomienie podziału wszystkich protokołów komunikacyjnych na następujące klasy:

- protokoły sieci lokalnych LAN;
- protokoły sieci rozległych WAN;
- protokoły trasowania;
- protokoły sieciowe.

Protokoły sieci lokalnych obsługują funkcje dwóch najniższych warstw modelu OSI (warstw fizycznej i łącza danych). Protokoły sieci rozległych obsługują funkcje trzech najniższych warstw modelu OSI (fizycznej, łącza danych i sieciowej) i definiują komunikację przez różne media stosowane w sieciach rozległych. Protokoły trasowania, obsługujące warstwę sieciową modelu OSI, są odpowiedzialne za określanie tras przepływu pakietów. Protokoły sieciowe to zbiory wielu różnych protokołów obsługujących wyższe warstwy modelu OSI (np. SNA, IP, IPX).

Informacja przesyłana z aplikacji programowej w jednej stacji sieciowej do aplikacji software'owej w innej stacji sieciowej musi przejść każdą warstwę modelu OSI w obu stacjach. Warstwy modelu OSI używają różnych form informacji sterujących służących do komunikowania się równorzędnych warstw różnych stacji sieciowych. Wspomniane informacje sterujące zawierają żądania i instrukcje wymieniane między równorzędnymi warstwami modelu OSI.

Ad. a) sieci LAN

Powszechnie używany skrót LAN oznacza lokalną sieć komputerową, obejmującą swoim zasięgiem stosunkowo mały obszar geograficzny i łączącą ze sobą stacje sieciowe (stacje robocze, komputery personalne, komputery sieciowe, serwery, drukarki i inne urządzenia). LAN umożliwiają współdzielony dostęp wielu użytkowników do tych samych urządzeń i aplikacji, wymianę plików między

(warstwa 3). Rozszerzacze LAN dobrze spełniają funkcję skalowania sieci, ponieważ główny router odfiltrowuje niepożądane pakiety typu broadcast i multicast. Rozszerzacze LAN nie zapewniają ani segmentowania, ani nie służą do budowy zapór ogniowych.

Ad. b) sieci WAN

WAN (ang. Wide Area Network) jest siecią transmisji danych obejmującą swoim zasięgiem stosunkowo duży obszar geograficzny, często używającą środków transmisji będących w dyspozycji towarzystw telekomunikacyjnych. Technologie sieci WAN funkcjonują w trzech najniższych warstwach modelu OSI: fizycznej, łącza danych i sieciowej.

Łącze punkt-punkt zapewnia pojedyncze, zawczasu zestawione połączenie komunikacyjne między siedzibą użytkownika a siecią odległą, z użyciem sieci operatora, na przykład sieci telefonicznej. Łącza punkt-punkt znane są także pod nazwą linii dzierżawionych, ponieważ ich trasa (ścieżka) jest stała i określona dla każdej zdalnej sieci dostępnej przez zasoby sieci operatora. Operator sieci rezerwuje łącza punkt-punkt na prywatne cele użytkownika. Łącza te umożliwiają dwa typy transmisji: transmisję datagramów skomponowanych z indywidualnie adresowanych ramek oraz transmisję strumienia danych, dla którego sprawdzanie adresów odbywa się tylko raz.

Stosowane w sieciach WAN przełączanie obwodów polega na zestawianiu, utrzymywaniu i rozłączaniu fizycznego obwodu przez sieć operatora dla każdej sesji komunikacyjnej. Przełączanie obwodów obsługuje dwa typy transmisji: transmisję datagramów, na które składają się indywidualnie zaadresowane ramki, i transmisję strumienia danych, dla których następuje tylko jednokrotne sprawdzenie adresu. Przełączanie obwodów jest szeroko stosowane w sieciach telefonicznych. ISDN jest typowym przykładem przełączania obwodów.

Stosowane w sieciach WAN przełączanie pakietów polega na współdzieleniu przez urządzenia sieciowe łącza punkt-punkt przeznaczonego do transportu pakietów między stacją nadawczą a stacją odbiorczą, poprzez sieć operatora. Dla współdzielenia obwodów przez urządzenia sieciowe używa się statystycznej multipleksacji. ATM, Frame Relay, SMDS (Switched Multi-megabit Data Senvice) i X.25 to przykłady technologii przełączania pakietów w sieciach WAN.

W topologii szynowej pakiet wysyłany przez dowolną stację sieciową dociera, za pośrednictwem medium, do wszystkich stacji sieciowych. W sieciach Ethernet/IEEE 802.3, jest stosowana topologia szynowa.

Topologia pierścieniowa jest strukturą, w której stacje sieciowe są podłączone do okablowania tworzącego pierścień. Topologię pierścienia stosuje się w technologiach Token Ring/IEEE 802.5 i FDDI.

W topologii gwiaździstej kable sieciowe są połączone w jednym wspólnym punkcie, w którym znajdują się hub lub przełącznik.

Topologia drzewiasta jest strukturą podobną do topologii szynowej, z tą różnicą, że są tu możliwe gałęzie z wieloma węzłami.

Sieci LAN buduje się z biernych i aktywnych urządzeń sieciowych. Bierne urządzenia sieciowe to komponenty systemów okablowania strukturalnego. Do aktywnych urządzeń sieci LAN należą:

- regeneratory;
- huby;
- mosty;
- przełączniki LAN;
- rozszerzacze LAN.

Regenerator (koncentrator) jest urządzeniem pracującym w warstwie fizycznej modelu OSI, stosowanym do łączenia segmentów kabla sieciowego. Łączący wiele kabli regenerator logicznie jest traktowany jak jeden kabel sieciowy. Po prostu regenerator, odbierając sygnały z jednego segmentu sieci, wzmacnia je, poprawia ich parametry czasowe i przesyła do innego segmentu. W rezultacie zabiegi te regenerują (stąd nazwa) sygnały zniekształcone długimi kablami i dużą liczbą podłączonych urządzeń. Liczby regeneratorów i segmentów są ograniczone.

Hub jest urządzeniem pracującym również w warstwie fizycznej. Jest czasami określany jak wieloportowy regenerator. Hub służy do tworzenia fizycznej gwiazdy przy istnieniu logicznej szyny lub pierścienia.

Rozszerzacz LAN to wielowarstwowy przełącznik zdalnego dostępu, podłączony do głównego routera. Rozszerzacze LAN przesyłają ruch z wszystkich standardowych protokołów warstwy sieciowej (np. IP, IPX, Apple Talk) i filtrują go zależnie od adresów MAC lub typu protokołu warstwy sieciowej modelu OSI

Modem jest urządzeniem, które interpretując sygnały cyfrowe i analogowe, umożliwia przesyłanie danych przez zwykłą linię telefoniczną. Modem usytuowany przy stacji nadawczej zamienia sygnały cyfrowe na formę wygodną do transmisji przez linię analogową, podczas gdy modem znajdujący się przy stacji odbiorczej sygnały analogowe ponownie zamienia na formę cyfrową.

Urządzenie CSU/DSU (ang. Channel Sewice Unit/Data Serwce Unit) jest urządzeniem dopasowującym fizyczny interfejs urządzenia DTE (ang. Data Terminal Equipment), np. interfejs terminala, do interfejsu urządzenia DCE (ang. Data Communications Equipment), np. interfejs przełącznika. Urządzenie CSU/DSU ponadto zapewnia impulsy czasowe niezbędne dla komunikacji między tymi urządzeniami.

Adapter terminala ISDN jest urządzeniem zapewniającym połączenia interfejsu BRI (ang. Basic Rate Interface) z innymi interfejsami, np. EIA/TIA-232. W istocie adapter terminala jest modemem ISDN.

Międzynarodowa Organizacja Standaryzacji (ISO) wniosła wielki wkład w opracowanie standardów sieci komputerowych. Model opracowany przez tę organizację jest bardzo przydatny do tego, aby zrozumieć istotne funkcje systemu zarządzania. Składa się on z pięciu podstawowych części:

- zarządzanie wydajnością;
- konfiguracją;
- sprawozdawczością;
- uszkodzeniami;
- bezpieczeństwem.

Zarządzanie siecią. Pojęcie to często ma inne znaczenia dla różnych specjalistów. Niekiedy jest ono interpretowane jako monitorowanie sieci z użyciem analizatora protokołów sieciowych. Innym razem przywodzi na myśl rozproszoną bazę danych, automatyczne zbieranie danych o urządzeniach sieciowych czy wreszcie wysokowydajne stacje robocze wyświetlające na swoich ekranach schematy zmian w topologii lub zmian w ruchu pakietów w rozpatrywanej sieci.

Zarządzanie siecią to usługa angażująca wiele różnych narzędzi, aplikacji i urządzeń wykorzystywanych przez specjalistów ze służby administratora sieci w trakcie monitorowania i utrzymywania sieci w stanie poprawnej pracy.

Obwody wirtualne. Obwodem wirtualnym (ang. Virtual Circuit) nazywamy obwód logiczny utworzony dla zapewnienia niezawodnej komunikacji między dwoma urządzeniami sieciowymi. Rozróżniamy dwa typy obwodów wirtualnych:

- przełączane obwody wirtualne;
- stałe obwody wirtualne.

Przełączane obwody wirtualne zestawiane są dynamicznie na żądanie oraz rozłączane po zakończeniu transmisji. Komunikacja przez obwód składa się z trzech faz: zestawienie obwodu, transmisja danych i rozłączanie obwodu. Faza zestawiania obwodu polega na tworzeniu obwodu między stacją nadawczą a stacja odbiorczą. Transmisja danych polega na ich przesyłaniu (przez obwód wirtualny) między stacją nadawczą a odbiorczą. Rozłączenie obwodu powoduje zakończenie jego funkcjonowania.

Przełączane obwody wirtualne są używane w sytuacjach, gdy transmisja danych między stacjami odbywa się sporadycznie. Jest to głównie związane z tym, że w obwodzie zwiększa się szerokość pasma w fazie zestawiania obwodu i w fazie jego rozłączania oraz zmniejsza koszt związany ze stałą dostępnością obwodu wirtualnego.

Stały obwód jest zestawiany na stałe i pracuje tylko w trybie transmisji danych. Obwód jest stosowany w sytuacjach, gdy transmisja między stacjami jest stała. Stały obwód zmniejsza szerokość pasma związanego z zestawianiem i rozłączaniem obwodu wirtualnego, zwiększa natomiast koszt w związku ze stałą dostępnością obwodu wirtualnego.

W sieciach WAN stosuje się wiele różnych produktów sprzętowych. Do typowych należą: przełączniki WAN, serwery dostępowe, modemy, urządzenia CSU/DSU i adaptery terminali ISDN. Ponadto stosowane są routery, przełączniki ATM i multipleksery.

Przełącznik WAN jest wieloportowym urządzeniem intersieciowym stosowanym do przełączania ruchu w sieciach, takich jak Frame Relay, X.25 i SMDS (ang. Switched Multimegabit Data Serwce), działającym w warstwie 2 modelu OSI.

Serwer dostępowy gra rolę punktu koncentrującego połączenia „do sieci" i „od sieci".

transmisję. W tych okolicznościach obie transmisje zostają unieważnione, a stacjom zezwala się transmitować później. Odpowiednie algorytmy określają, kiedy kolidujące stacje powinny retransmitować.

Technologia Token Ring. Technologia Token Ring została opracowana przez IBM w latach siedemdziesiątych. Jest to ciągle najpopularniejsza technologia sieciowa IBM i w ogóle druga pod względem popularności (po Ethernecie) technologia sieci lokalnych LAN. Specyfikacja IEEE 802.5 jest niemal identyczna z opracowaną przez IBM. Termin Token Ring jest stosowany zarówno w odniesieniu do opracowania IBM-owskiego, jak i specyfikacji IEEE 802.5. Pomimo 25 lat, jakie mijają od opracowania przez IBM technologii Token Ring, jest ona ciągle jeszcze stosowana.

Token Ring i IEEE 802.5 stosują metodę dostępu nazywaną Token-Passing. Metoda ta jest również stosowana w technologii FDDI. W pierścieniu sieci Token Ring krąży mała ramka zwana token (żeton). Stacja sieciowa uzyskuje prawo do transmisji informacji tylko wtedy, gdy posiada token. Jeśli więc dowolna stacja sieciowa przejmuje token, ale w tym momencie nie zamierza transmitować, to przesyła żeton do następnej w kolejności stacji sieciowej. Każda stacja może przetrzymywać token tylko przez określony czas.

Stacja nadawcza, przy której znajdzie się token, mająca informację do przesłania, zmienia jeden bit w token, dając w ten sposób początek sekwencji startu ramki, dodaje informację, którą chce transmitować, po czym całość wysyła do następnej stacji zainstalowanej w pierścieniu. W czasie, gdy ramka przesuwa się w pierścieniu, nie ma w nim żetonu, co oznacza, że inne stacje, chcące w tym czasie rozpocząć transmisję, muszą czekać. Oznacza to także, że w sieciach Token Ring nie występują kolizje. Po zakończeniu transmisji generowany jest nowy token. Ramka informacyjna, krążąc w pierścieniu, osiąga wreszcie stację odbiorczą, która kopiuje ją do dalszego przetwarzania. Ramka kontynuuje dalszą wędrówkę w pierścieniu aż do momentu osiągnięcia stacji nadawczej. Tutaj zostaje usunięta z pierścienia. Stacja nadawcza może sprawdzić, czy ramka dotarła do stacji odbiorczej i tam została skopiowana. Inaczej niż sieć Ethernet (z metodą dostępu CSMA/CD), sieci z dostępem Token-Passing mają charakter deterministyczny, co oznacza możliwość wyliczenia maksymalnego czasu, który upłynie do momentu

Ad. c) technologie sieci lokalnych

Technologia Ethernet. Należy zaznaczyć, że pojęcie Ethernet odnosi się nie do jednej, lecz do wielu technologii sieci lokalnych LAN, z których wyróżnić należy trzy podstawowe kategorie:

- Ethernet i IEEE 802.3 –jest to kilka specyfikacji określających LAN, z których każda pracuje z przepływnością 10 Mb/s;
- Ethernet 100 Mb/s - jest to pojedyncza specyfikacja, znana również jako Fast Ethernet, określająca sieć pracującą z przepływnością 100 Mb/s;
- Ethernet 1000 Mb/s -jest to pojedyncza specyfikacja, znana również jako Gigabit Ethernet, określająca sieć pracującą z przepływnością 1000 Mb/s (lGb/s).

Ethernet od ponad 20 lat pozostaje grupą najpopularniejszych technologii sieciowych. Decydują o tym duża elastyczność i prostota Ethernetu. Technologia Ethernet, używająca metody dostępu CSMA/CD (ang. Carrier Sense Multiple Access Collision Detect), została opracowana w firmie Xerox w latach siedemdziesiątych. Obecnie nazwa Ethernet odnosi się nie tylko do sieci Xerox, ale do wszystkich sieci „pochodnych" i korzystających z metody dostępu CSMA/CD. Specyfikację IEEE 802.3 opracowano w 1980 r., opierając się na rozwiązaniu Xeroxa. Natomiast wersja 2 specyfikacji Ethernet to już wspólne dzieło firm DEC, Intel i Xerox. Jest ona kompatybilna z IEEE 802.3.

W sieciach tych każda stacja „widzi" wszystkie przepływające ramki. W czasie dowolnej transmisji stacje zainstalowane w sieci muszą sprawdzać, czy przepływająca ramka nie jest wysłana do jednej z nich, jako stacji odbiorczej. Ramki przeznaczone do odbioru przez określoną stację odbiorczą są przesyłane do protokołów wyższych warstw tej stacji. Przy metodzie dostępu CSMA/CD stacja zamierzająca transmitować może mieć dostęp do sieci w dowolnej chwili. Przed wysłaniem danych stacja „nasłuchuje", czy w sieci odbywa się ruch. Stacja, chcąc wysłać dane, musi czekać aż do momentu, kiedy w sieci nie ma żadnego ruchu. Inaczej mówiąc, na transmisję dowolnej stacji zezwala się, jeżeli w sieci jest cisza (brak ruchu).

W sieci mamy do czynienia z kolizją wtedy, gdy dwie stacje - po stwierdzeniu, że sieć jest wolna – w tym samym momencie usiłują rozpocząć

nieczynny. Zasadniczym celem podwójnego pierścienia jest zapewnienie wysokiego poziomu niezawodności. FDDI jest standardem sieci lokalnej LAN o następujących parametrach:

- przepływność: 100 Mb/s;
- metoda dostępu: Token-Passing;
- medium transmisyjne: kabel światłowodowy;
- topologia: podwójny pierścień .

Należy dodać, że stosunkowo niedawno wprowadzono odmianę FDDI, tzw. technologię CDDI (ang. Copper Distributed Data Interface), której istotą jest stosowanie protokołów FDDI, ale na infrastrukturze kablowej zbudowanej z miedzianego kabla, również zapewniającej przepływność 100 Mb/s.

W technologii FDDI jako podstawowego medium transmisyjnego używa się kabla światłowodowego. Jak zaznaczono już wcześniej, technologia FDDI, w której stosuje się kabel miedziany, nosi nazwę CDDI. Kabel światłowodowy ma cały szereg zalet w porównaniu z kablem miedzianym, w szczególności w zakresie bezpieczeństwa, niezawodności i przepływności. Źródłem tych zalet jest to, że światłowód nie emituje sygnałów elektrycznych. Medium fizyczne emitujące sygnały elektryczne (np. kabel miedziany) może być „podsłuchiwane" i dlatego nie jest całkowicie zabezpieczone przed nieautoryzowanym dostępem do danych transmitowanych przez to medium.

Ponadto światłowód jest odporny na interferencję pochodzącą od częstotliwości radiowych RFI (ang. Radio Frequency Interference) oraz interferencję elektromagnetyczną EMI (ang. Electromagnetc Interference). Światłowód zawsze zapewniał szersze pasmo niż kabel miedziany, chociaż ostatnio opracowane miedziane kable skrętkowe również zapewniają pracę z dużymi przepływnościami. Reasumując, FDDI umożliwia rozstawianie stacji między sobą na odległości do 2 km przy kablu wielomodowym i dopuszcza większe odległości przy kablu jednomodowym.

Technologia FDDI została opracowana przez Komitet amerykańskiego Instytutu ANSI (ang. American National Standards Institute) w pefowie lat 80. Nieco wcześniej rozpoczęto wprowadzanie do praktyki stacji inżynierskich „nadmiernie pożerających pasmo istniejących już sieci Ethernet i Token Ring.

rozpoczęcia transmisji przez dowolną stację. Właściwość ta oraz inne cechy omówione dalej czynią z Token Ring sieć przydatną w aplikacjach, w których opóźnienie musi być przewidywalne. Przykładem może być sieć wspomagająca automatyzację fabryki.

Sieć Token Ring używa systemu priorytetu zezwalającego stacjom o wysokim priorytecie na częstsze używanie sieci. W tym celu ramka sieci Token Ring ma dwa pola sterujące priorytetem: pole priorytet i pole rezerwacja. Tylko stacje z priorytetem równym lub większym od priorytetu w token mogą przechwycić żeton. Po przechwyceniu token i zamianie na ramkę informacyjną tylko stacje z wartością priorytetu większą od wartości priorytetu stacji transmitującej mogą rezerwować token do następnego obiegu w pierścieniu sieciowym. Gdy następny token jest generowany, ma on wyższy priorytet stacji rezerwującej.

W sieciach Token Ring stosuje się wiele mechanizmów umożliwiających detekcję i eliminację uszkodzeń. W tym celu jedna stacja w sieci Token Ring zostaje wybrana jako monitor aktywny. Stacja ta, którą teoretycznie może być dowolna stacja w sieci, pracuje jako centralne źródło informacji czasowych używanych przez inne stacje podłączone do pierścienia oraz generuje cały szereg funkcji konserwacyjnych pierścienia. Jedną z tych funkcji jest usuwanie z pierścienia ciągle krążących ramek. Gdy stacja nadawcza ulega uszkodzeniu, jej ramka może kontynuować obieg w pierścieniu, co może doprowadzić do wstrzymania transmisji ramek pochodzących od innych stacji i w praktyce zablokować sieć.

Technologia FDDI. Technologia FDDI (ang. Fiber Distributed Data Interface) jest obecnie często używana do budowy sieci szkieletowych ze względu na jej istotne zalety: dużą przepływność i niezawodność oraz możliwość stosowania na długich dystansach.

W technologii FDDI stosuje się topologię podwójnego pierścienia, czyli struktury składającej się z dwóch różnych fizycznie pierścieni światłowodowych. Ruch ramek w każdym z nich odbywa się w przeciwnym kierunku. Pierwszy z pierścieni nazywamy podstawowym, a drugi - dodatkowym. W czasie normalnej pracy, pierścień podstawowy służy do transmisji danych, a pierścień dodatkowy jest

Protokoł Frame Relay - podobnie jak X.25 - jest protokołem transportowym w trybie pakietowym, ale wykorzystuje prostszy mechanizm korekcji błędów. Sieć wykrywa błędy nagłówka, formatu i cyklicznego kodu nadmiarowego FCS (ang. Frame Check Sequence). Ramki z błędem są kasowane, a ich skompletowanie przeprowadzają stacje końcowe, odwołując się do procedur powtarzania części sesji, gdyż ramki nie są numerowane. Ponadto sieć modyfikuje nagłówki ramek i FCS. Pakiety przełącza się programowo.

Sieć FR WAN składa się z przełączników połączonych kanałami fizycznymi, w których są multipleksowane obwody wirtualne rozpoznawane po niepowtarzalnych numerach DLCI, i z urządzeń dostępowych. Normy FR określają też dwa poziomy protokołów: jeden dla transferu danych między urządzeniami dostępowymi, drugi dla sygnalizacji (sprawdzanie integralności interfejsu z siecią, przekazywanie informacji o stanie obwodów wirtualnych itp.).

Protokół Frame Relay określa dwie kategorie urządzeń:

- DTE (ang. Data Terminal Equipment) - programowalne urządzenia dostępowe do sieci Frame Relay WAN spoza jej obrzeża, jak: FRADy (Frame Relay Access Devices), terminale, komputery, routery, mosty czy multipleksery;
- DCE (ang. Data Circuit - terminating Equipment) - urządzenia międzysieciowe, węzły po stronie sieci Frame Relay WAN, przeznaczone do synchronizacji i przełączania usług między urządzeniami DTE komunikującymi się ze sobą przez sieć rozległą. Podstawowymi urządzeniami DCE FR są prawie wyłącznie przełączniki ramek.

Właściwości połączenia między DTE i DCE wynikają zarówno z warstwy fizycznej, jak i łącza danych. Warstwa fizyczna definiuje mechaniczne, elektryczne, funkcjonalne i proceduralne specyfikacje połączenia między tymi urządzeniami, na przykład interfejs RS-232 (ang. Recommended Standard). Z kolei warstwa łącza danych określa protokół ustanawiania połączenia między przełącznikiem a urządzeniem dostępowym, jak router czy FRAD.

Sieć Frame Relay WAN zapewnia dwukierunkową komunikację połączeniową każdej parze urządzeń dostępowych DTE: Ścieżka łącząca dwa takie urządzenia może przebiegać przez kilka węzłów DCE połączonych ze sobą

Wtedy ewidentnym okazało się, ze istnieje zapotrzebowanie na siec o większej wydajności i niezawodności. Wymagania te spełnia technologia FDDI Po opracowaniu standardu FDDI, instytut ANSI przekazał go do ISO, który sporządził wersję międzynarodową. Obie wersje są całkowicie kompatybilne.

Ad. d) technologie sieci rozległych

Technologia Frame Relay. Technologia Frame Relay (FR), do chwili zdominowania sieci przez ATM, miała stać się dosyć powszechnym standardem sieciowym zwłaszcza w regionach, gdzie nie dotarła wcześniej technologia X.25. Zdołała jednak zmienić swój status i z technologii przejściowej szybko stała się technologią ogólnie uznaną, tworząc rynek wartości wielu miliardów dolarów. Sieć FR jest znacznie szybsza od X.25 i tańsza niż ATM. Wnosi niewielkie opóźnienia i zapewnia sprawiedliwy dostęp do pasma wszystkim użytkownikom. Na taką właśnie technologię czekali administratorzy sieciowi średnich i wielkich przedsiębiorstw. Protokół Frame Relay funkcjonuje w dwu pierwszych warstwach modelu ISO/OSI.

Technologia Frame Relay jest znana od 1984 r., ale dopiero w 1991 roku utorowała sobie szerszą ścieżkę do sieci w USA. Szybką technologią programowego przełączania ramek - stała się w 1993 r. po włączeniu do jej protokołu procedur przełączania obwodów wirtualnych.

Sieć Frame Relay zapewnia komunikację połączeniową o przepływności do 45 kb/s. Funkcjonuje na łączach cyfrowych dobrej jakości, odznaczających się niską stopą błędów. Lista zastosowań FR jest coraz szersza i obejmuje:

- łączenie sieci LAN;
- dostęp do ATM;
- transmisje danych i głosu;
- wideokonferencje i telekonferencje;
- transport plików przez WAN między stacjami wysokiej rozdzielczości a bazą danych;
- komunikację interaktywną między terminalami a zasobami dużych komputerów, ale w ograniczonym zakresie przepływności.

praktycznie niedostępnych przez łącza analogowe (znacznie powyżej 100 kb/s);

- wykorzystanie istniejącej miedzianej infrastruktury okablowania na najniższym poziomie w otoczeniu abonenta, bez ponoszenia wydatków na wymianę lokalnych instalacji, co w istotny sposób wpływa na obniżenie kosztów wdrażania techniki ISDN.

Dodatkowym atrybutem sieci ISDN jest możliwość transmisji w dwóch trybach pracy, przez integrację techniki przełączania obwodów (komutacja i linii) z przełączaniem pakietów (transmisje pakietowe). Sieć ISDN jest jednak bardziej ukierunkowana na klasyczne przełączanie obwodów, co dobrze służy aplikacjom izochronicznym, jak też aplikacjom asynchronicznym typu pakietowego dla stosunkowo dużych porcji danych. Transmisje z przełączaniem pakietów są natomiast bardziej korzystne dla aplikacji transakcyjnych i efektywnego prowadzenia sygnalizacji.

Pełne wykorzystanie oferty usług sieci cyfrowej wymaga stosowania urządzeń i terminali (także telefonów) cyfrowych i uaktywnienia nowych usług w systemie komutacyjnym, dostępnych przez istniejącą do tej pory, dwuprzewodową linię telefoniczną między abonentem a centralą. Telefony analogowe przyłączone do sieci ISDN przez odpowiedni adapter komunikacyjny mogą funkcjonować tylko w ograniczonym zakresie usług.

Poprawne funkcjonowanie sieci ISDN wymaga standaryzacji wielu elementów komunikacyjnych znajdujących się na rozległym obszarze i obejmujących:

- przetwarzanie sieciowe, w tym - wyposażenie abonenta, zasady transmisji i systemy przełączania (centrale, routery, przełączniki);
- kanały komunikacyjne zawierające kanały informacyjne typu B oraz kanały sygnalizacji pakietowej D, a także możliwość agregowania kanałów informacyjnych do postaci H;
- protokoły UNI (ang. User Network Interface) do transmisji przez dwa rodzaje interfejsów: BRI ($2B+D_6$) i PRI ($23/30B+D_{64}$);

kanałami fizycznymi. W efekcie przez jedno międzywęzłowe połączenie fizyczne może przebiegać wiele wspomnianych ścieżek, nazywanych obwodami logicznymi lub wirtualnymi. Każdy taki obwód jest oznaczany przez operatora numerem DLCI, spełniającym funkcje lokalnego adresu pakietu, ale tylko w obrębie FR WAN. Pasmo transmisyjne kanału fizycznego może być dzielone dynamicznie między stowarzyszone z nim obwody wirtualne. Oznacza to, że użytkownik uzyskuje dostęp do pasma dopiero w chwili nawiązywania transmisji, a po jej zakończeniu całe to pasmo przypadnie innemu obwodowi wirtualnemu. Ścieżki między dwoma DTE można zestawiać na dłuższe okresy lub tylko sporadycznie, na życzenie. Z tych względów obwody wirtualne FR zostały podzielone na dwie grupy: stałe połączenia wirtualne i przełączane.

Sieci ISDN. Istotnym czynnikiem kreującym nowe kierunki w telekomunikacji jest wzrost zapotrzebowania na usługi odbiegające od klasycznego przekazu telefonicznego. Próby wykorzystania istniejących łączy analogowych do transmisji strumieni cyfrowych pomiędzy urządzeniami komputerowymi wykazały małą efektywność takich łączy oraz związanych z nimi urządzeń pośredniczących, a więc konieczność przejścia na technikę cyfrową nowoczesnych systemów komunikacji.

Sieci ISDN stosowane początkowo w prywatnych, a następnie publicznych cyfrowych sieciach telekomunikacyjnych, umożliwiają nie tytko przekaz głosu, tekstu, grafiki i obrazów ruchomych, ale mają zdolność współpracy zarówno z sieciami komputerowymi LAN, jak i różnymi typami sieci rozległych. Są takie podstawą do tworzenia bardziej zaawansowanych sieci szerokopasmowych BISDN. Wyróżnia się trzy czynniki leżące u podstaw rozwoju sieci cyfrowej z integracją usług ISDN w sieci rozległej, odróżniające je od tradycyjnych sieci analogowych:

- opanowanie techniki przekazu cyfrowego na wszystkich etapach łączności od abonenta (telefony, telefaksy, terminale, komputery, przełącznice, krotnice) do cyfrowej centrali abonenckiej i systemu komutacyjnego włącznie;
- wzrost zainteresowania abonentów usługami niefonicznymi (przekazy cyfrowe, dostęp do baz danych, grafika, obrazy ruchome), wymagającymi połączeń z sieciami LAN o znacznie wyższych przepływnościach,

z komutowaniem obwodów (komutacja łączy). Dzięki temu użytkownik ma dostęp do różnorodnych przepływności strumienia cyfrowego o wielokrotności 64 kb/s, definiowanych indywidualnie przez niego w miarę potrzeb. Do tej pory wykształciły się następujące popularne przepływności strumieni cyfrowych oferowanych przez kanały sieci ISDN:

- kanał B o przepływności 64 kb/s w trybie przełączania obwodów;
- kanał 2B o przepływności 128 kb/s (144 kb/s łącznie z kanałem D);
- kanał D o przepływności od 16 kb/s lub 64 kb/s (przełączanie pakietów);
- kanały typu H z przełączaniem obwodów o szybkościach:
  - H0 o przepływności 384 kb/s (agregowanie 6 kanałów B);
  - Hll o przepływnościach 1472 kb/s (23 kanały B), 1536 kb/s (24 kanały B);
  - H12 o przepływności 1920 kb/s (30 kanałów B);
  - H2 o przepływności 6312 kb/s lub 8448 kb/s;
  - H3 o przepływności 23,064 Mb/s lub 34,368 Mb/s albo 44,736 Mb/s;
  - H4 o przepływności 97,728 Mb/s lub 139,264 Mb/s.

W kanałach B i D funkcjonują protokoły transportowe. Dla kanału B takim protokołem jest LAP-B (ang. Link Access Protocol 6), a w kanale D protokół LAP-D (ang. Link Access Protocol on D channel). Procedury LAP-B obsługują dostęp typu punkt-punkt, a LAP-D przekazy typu punkt-wielopunkt i na tym polega podstawowa różnica między tymi protokołami.

W standardach ISDN przewiduje się sprzęganie z siecią zupełnie nowych, cyfrowych terminali TE 1 (ang. Terminal Equipment type 1) oraz włączanie istniejących analogowych terminali TE 2 (ang. Terminal Equipment type 2) przez specjalizowane adaptery TA (ang. Terminal Adapter). Połączeń z siecią ISDN dokonuje się przez zakończenie sieciowe NT, przyjmujące różne postaci (NT, NT1, NT1+TA i in.).

Urządzenia końcowe zaliczane do grupy TE1 (cyfrowe, wyłącznie dla ISDN) można podzielić ze względu na złożoność i stopień integracji funkcji na trzy grupy:

- terminale jednofunkcyjne (proste) - przeznaczone do realizacji wybranej usługi ISDN. Typowymi przykładami są: telefon cyfrowy ISDN

- sygnalizacja abonencka DSS1 (ang. Digital Subscriber Signaling 1) wraz ze scentralizowaną sygnalizacją SS7 (ang. Signaling System 7) między centralami.

Użytkownik ma możliwość wyboru jednego z dwóch sposobów dostępu do sieci cyfrowej ISDN. Dla niewielkiego ruchu generowanego przez pojedynczy terminal (lub najwyżej kilka terminali użytkownika) wystarcza dostęp podstawowy BRA (ang. Basic Rate/Access), natomiast dostęp pierwotno-grupowy PRA (ang. Primary Rate Access) uwzględnia znacznie bardziej intensywne generowanie strumieni pochodzących z sieci lokalnych (np. z Ethernetu), intranetów, serwerów wideokonferencyjnych czy centralek abonenckicn PABX.

W dostępie podstawowym BRA, oznaczanym $2B+D_{16}$, maksymalna przepływność 144 kb/s (2x64 kb/s + 16 kb/s) jest oferowana przez dwa kanały B po 64 kb/s w każdym oraz jeden kanał D (Delta) z przepływnością 16 kb/s. Kanałami informacyjnymi B przesyła się głos w postaci cyfrowej, telekopie (faks G4) i inne dane cyfrowe (pliki), natomiast kanałem typu D sekwencje sygnalizacyjne stosowane przy konfigurowaniu komunikacji, nadzór nad przebiegiem transmisji w kanałach B i inne informacje serwisowe. Kanały B można wykorzystywać niezależnie i pojedynczo (po 64 kb/s) lub łącznie (128 kb/s), bądź z integracją kanału D (razem 144 kb/s), jeśli nie jest on zajęty sygnalizacją połączenia. W niektórych sytuacjach wydzielony kanał D (16 kb/s) może być używany jako kanał informacyjny użytkownika do prowadzenia transmisji pakietowej. Jako medium transmisyjne w dostępie BRA stosuje się pospolitą miedzianą skrętkę telefoniczną o minimalnej przepływności kanałowej 192 kb/s. W dostępie pierwotnym PRA, oznaczanym $30B+D_{64}$, oferta obejmuje 30 kanałów B, a maksymalna przepływność wynosi 1984 kb/s. W systemie amerykańskim i japońskim ($23B+D_{64}$) przepływność ta jest mniejsza i wynosi tylko 1536 kb/s. Łączem fizycznym (medium transportowym) w dostępie pierwotnym PRA jest zwykle skrętka miedziana wykonana w technologii HDSL (2048 kb/s), także kanał radiowy bądź światłowód o podobnych własnościach.

Rekomendacja serii 1.400 dla sieci ISDN przewiduje agregowanie wielu kanałów typu B, oznaczanych jako kanały typu H, a działające zarówno w trybie komutacji obwodów jak i pakietów, raczej ze wskazaniem na przekazy

- współdziałanie i innymi sieciami (X.25, Franie Reiay, SMDS, ATM i innych);
- korzystanie ze standardowych (istniejących i komutowanych) linii telefonicznych dla dostępu podstawowego;
- identyczna lub zbliżona taryfikacja jak dla usług podstawowych POTS.

Technologia SMDS. SMDS (ang. Switched Multimegabit Data Senvice) należy do rodziny technologii szybkich sieci pakietowych, w których kontrolą błędów zajmują się stacje końcowe. Pakiety z błędami są z założenia odrzucane. Bezpołączeniowy tryb pracy sieci zapewnia komunikację typu każdy z każdym bez konieczności nawiązywania połączenia i uruchamiania procedur rozłączania. Metodą dostępu jest DQDB, a najważniejszym protokołem komunikacyjnym - interfejs SIP. Do kanału dostępowego dopuszcza się pakiety po każdorazowym sprawdzeniu adresu źródłowego. Nośnikiem informacji mogą być światłowody lub przewody miedziane. Sieci oparte na technologii SMDS zapewniają:

- przepływności odpowiadające zwykle pięciu klasom dostępu: 4, 10, 16, 25 i 34 Mb/s, a coraz częściej - 45 i 140 Mb/s;
- transport pakietów o długości do 9188 bajtów;
- sprawdzanie adresów źródłowych;
- przesyłanie adresów źródłowych i docelowych;
- adresowanie grupowe;
- wsparcie SNMP (ang. Simple Network Management Protocol).

SMDS charakteryzuje się wysoką dostępnością usług. Prawdopodobieństwo dostępności usługi w dowolnie wybranej chwili wynosi z założenia 0,999, a więc dużo więcej niż w typowej sieci lokalnej. Około 95 proc. transmisji najdłuższego pakietu między dwoma CPE pod systemem DS-3 nie powinno trwać dłużej niż 20 ms. Średni czas transferu danych jest niższy od 10 ms i sieć SMDS staje się praktycznie niewidoczna dla abonentów.

Technologia SMDS powstała w laboratoriach BELLCORE (ang. BELL COmmiaincations REssearch). Upowszechnia się od 1989 r. jako technologia szybkich sieci pakietowych WAN z usługami bezpołączeniowymi. W Europie upowszechnia się ekwiwalentna technologia o nazwie CBDS (ang. Connectionless Broadband Data Service), zaakceptowana przez ETSI (ang. European

wyposażony w wyświetlacz z klawiaturą oraz usługi dodatkowe, urządzenie faksowe grupy 4, terminal ekranowy z klawiaturą itp.;

- terminale mieszane (niefoniczne) - integrujące wiele rodzajów usług transmisyjnych (drukarki, skanery, pamięci masowe różnego rodzaju) w celu realizacji usług nowego typu: prezentacji i korekty tekstów, przetwarzania obrazów graficznych, aktualizacji przeglądanych zbiorów, edycji i archiwowania;
- terminale wielofunkcyjne (złożone) - spełniające proste funkcje stacji roboczej sieci ISDN przez łączenie usług obliczeniowych z telekomunikacyjnymi i obejmujące również terminale wideokonferencyjne.

Usługi w sieci rozległej ISDN są identyczne jak usługi cyfrowym dostępie abonenckim. W strukturze dostępowej sieci cyfrowej ISDN wyróżnia się pięć punktów odniesienia R, S, T, U, V, z których tylko trzy styki R, S, T są objęte standaryzacją międzynarodową, a pozostałe związane z rodzajem linii i typem centrali komutacyjnej pozostają w gestii operatora sieci lub producenta centrali.

Podstawowe cechy sieci rozległej ISDN. Cechy charakterystyczne transmisji cyfrowej przez sieci ISDN obejmują:

- przekaz cyfrowy z gwarantowaną przepływnością 64 kb/s bez względu na odległość dzielącą abonentów, z możliwością zastosowania dwóch kanałów typu B udostępniających gwarantowaną przepływność 128 kb/s;
- krótki czas zestawiania połączeń (routery) i możliwość ich likwidacji natychmiast po zrealizowaniu sesji komunikacyjnej;
- szeroki zakres usług i równoczesnym przekazem głosu i danych (wideotelefonia);
- transmisja i komutacją obwodów oraz pakietów;
- deklarowana szeretość pasma (Nx64 kb/s), agregowanie kanałów;
- sygnalizacja pozapasmowa (kanał D), nowoczesny system sygnalizacji 587;
- automatyczna identyfikacja numeru (ANI);
- identyfikacja abonenta wywołującego (CLI);

Technologia asymetrycznego dostępu abonenckiego xDSL zapewnia szeroki zakres zmian szybkości informacji w kierunku abonenta: od 16 kb/s do 8 Mb/s. Ta najnowsza, szerokopasmowa technologia przekazu cyfrowego przez zwykłą linię telefoniczną jest konkurencyjna w odniesieniu zarówno do abonenckich przekazów cyfrowych ISDN, jak również hybrydowych - opartych na kablu współosiowym i światłowodowym.

Rodzaje technologii xDSL. Technologia asymetrycznych i symetrycznych przekazów xDSL obejmuje kilka odrębnych technologii o różnych szybkościach działania:

- zintegrowaną IDSL (ISDN DSL);
- o podwyższonej przepływności HDSL (ang. High bitrate Digital Subscriber Line);
- asymetryczną ADSL (ang. Asymmetric DSL);
- powszechną CDSL (ang. Consumer DSL);
- symetryczną SDSL (ang.Symmetric DSL);
- adaptacyjną RADSL (ang. Rate Adaptive DSL);
- o bardzo wysokiej przepływności VDSL (ang. Very High Speed DSL) dochodzącej do 52 Mb/s w kierunku dosyłowym.

Dwukierunkowe i zwykle asymetryczne końcowe urządzenia komunikacyjne - nazywane coraz częściej modemami DSL - umożliwiają transmisje w szerokim zakresie szybkości przez jedną parę przewodów miedzianych łączących użytkownika z najbliższym węzłem telekomutacyjnym o przepływnościach:

- od 16 kb/s do 2 Mb/s w kierunku od abonenta do sieci oraz
- od 640 kb/s do kilkudziesięciu Mb/s w kierunku z sieci do abonenta.

Coraz większą popularność uzyskuje łącze asymetryczne ADSL o przepływności od 640 kb/s w kierunku sieci i 6-8 Mb/s w kierunku dosyłowym do abonenta.

Standaryzacja cyfrowych pętli lokalnych rozpoczęła się (1981 r.) od zaleceń dla sieci ISDN (technologia i IDSL); a podstawowe specyfikacje dla przekazów w technologii ADSL zostały sformułowane przez ANSI jako standard 11,413. Wielokrotne modernizacje i adaptacja tych zaleceń do warunków europejskich prowadzane praż ETSI, ATI Forum 1 DAWIC (ang. Digital Audio Visual Conucil) doprowadziły (1994 r.) do ustalenia zasadniczych kierunków rozwoju architektury

Telecommunications Standard Institute). Jest to w istocie pierwsza kompletna architektura, która implementuje usługę ATM i jest dobrze specyfikowana.

Pierwsze sieci ATM spełniają specyfikacje CBDS. Obydwie technologie są identyczne przy dostępie na kanałach El lub E3. Czołowym europejskim dostawcą urządzeń zgodnych z protokołami SMDS/CDBS jest Siemens. W architekturze sieci SMDS wyróżnia się 4 podstawowe elementy:

- CPE (ang. Customer Premises Equipment) - urządzenia abonenta, takie jak komputery, terminale i różne węzły pośrednie w postaci routerów, multiplekserów czy modemów;
- MSS (ang. MAN Switching System) - sieciowy system komutacyjny, w praktyce -prawie zawsze oparty na szybkich przełącznikach WAN;
- SNI (ang. Subscriber Network Interface) - interfejs między CPE i MSS, dzięki któremu sieć SMOS jest przezroczysta dla użytkownika. Każdy taki interfejs ma przypisany przynajmniej jeden adres zgodny z CCITT E.164;
- ISSI (ang. Inter Switching System Interface) - wewnętrzny interfejs SMDS, przez który węzły MSS łączą się ze sobą i z systemem zarządzania.

Do podstawowych zastosowań technologii SMDS zalicza się łączenie odległych sieci LAN i kampusowych oraz poszerzanie ich zasięgu na obszarze miasta lub większym. Inne zastosowania wynikają z typowych przymiotów połączeń komutowanych: komunikacja między stacjami roboczymi lub grupami użytkowników, połączenia dużych komputerów z terminalami itp.

Technologie xDSL. Różnorakie technologie cyfrowych przekazów xDSL (ang. Digital Subscriber Line), w tym również asymetrycznych typu ADSL (ang. Asymmetric Digital Subscriber Line), wiążą się ze wzrastającym zapotrzebowaniem na szerokopasmowe usługi abonenckie, takie jak: multimedia, szybki dostęp do Intemetu oraz przekaz obrazów wideo o wysokiej jakości, z wykorzystaniem istniejących dwuprzewodowych linii telefonicznych bezpośrednio w otoczeniu abonenta. Wspólną ich cechą jest asymetria przepływności w obydwu kierunkach przenoszenia, którą zapewniają końcowe urządzenia komunikacyjne - nazywane również modemami DSL

o przepływności bitowej od 64 kb/s do 2 Mb/s, Jest stopniowo wypierany przez bardziej efektywny przekaz pakietowy w technologii Frame Realy - działający do szybkości 45 Mb/s.

Pozytywne wyniki w eksploatacji tych sieci doprowadziły w latach siedemdziesiątych do powstania wielu komercyjnych wersji rozległych sieci pakietowych (Telnet, Graphnet, Datapac, Cyclades, Scannet, Euronet i inne) obejmujących swym zasięgiem coraz większe obszary, wykraczając poza granice jednego kraju. Wzajemna wymiana informacji między różnymi sieciami nie byłaby możliwa bez odpowiedniej standaryzacji protokołów i łączy. Jednym z najstarszych i ciągle jeszcze popularnym standardem dla funkcjonowania sieci pakietowych pozostaje protokół X.25, ustanowiony przez CCITT/ITU-T jako standard międzynarodowy sieci rozległych.

Standard sieci pakietowej z protokołem X.25 opisuje zbiór protokołów definiujących styk użytkownika z siecią rozległą z komutacją (przełączaniem) pakietów oraz zasady łączenia terminali i komputerów przez tę sieć. Wyróżnia się następujące podstawowe cechy tego standardu:

- komutację pakietów o zmiennej długości z zastosowaniem trybu połączeniowego do ich transmisji, co oznacza, że poszczególne pakiety nie muszą zawierać adresów nadawcy i odbiorcy;
- możliwość tworzenia połączeń wirtualnych, gwarantujących przybywanie pakietów do użytkownika końcowego w tej samej kolejności, w jakiej zostały wystane;
- implementację rozbudowanego systemu korekcji błędów i sterowania przepływem, co oznacza, że każdy węzeł sprawdza kompletność i poprawność odebranego pakietu przed dalszym jego wysłaniem;
- wykrywanie nieprawidłowości informacji przez dowolny węzeł na trasie przekazu, powodujące żądanie retransmisji błędnego pakietu i nadmiarowość w transmisji pakietów, co powoduje zmniejszenie ogólnej przepustowości sieci;
- niezawodny przekaz informacji przez łącza o niższej jakości, lecz z opóźnianiem pakietów przez kolejne węzły;

systemów ADSL, protokołów i interfejsów dla większości aplikacji ADSL. Ze względu na ciągły rozwój technologii standaryzacja nie jest zakończona ostatecznie.

Sieć z ofertą usług multimedialnych obejmuje trzy elementy infrastruktury telekomunikacyjnej:

- węzły sieci odpowiedzialne za produkcję, magazynowanie i dostawę programów z wideotek, łącznie z transmisją programów stacji telewizyjnych działających w czasie rzeczywistym;
- szerokopasmową sieć transportową z komutacją przekazów cyfrowych, opartą na technice synchronicznej SDH lub asynchronicznej ATM;
- dostępową sieć abonencką realizowaną nie tylko przez duże korporacje telekomunikacyjne (telekomy), ale również przez lokalnych operatorów telewizji kablowej i bezprzewodowej.

Technologia ADSL jest jedną z cyfrowych technologii DSL umożliwiających szerokopasmowy i asymetryczny dostęp abonentów do publicznych sieci telekomunikacyjnych i Internetu w sytuacjach, gdzie już istnieje tradycyjna abonencka sieć miedziana (skrętka linii telefonicznej), a budowa od podstaw nowoczesnych światłowodowych linii opartych na technologiach FITL nie jest uzasadniona ekonomicznie.

Sieć X.25. Technika przełączania pakietów, która stała się podstawą budowy zarówno komputerowych, jak i rozległych sieci pakietowych, została wprowadzona po raz pierwszy na terenie amerykańskim we wczesnych latach sześćdziesiątych (RAND Corporation - 1964 r.). Badania eksperymentalne nad siecią pakietową, prowadzone w latach 1968-1975, zakończyły się wdrożeniem pierwszej rozległej sieci pakietowej ARPANET (ang. Advanced Research Project Agency Network), łączącej liniami dzierżawionymi wiele rozproszonych strategicznych ośrodków wojskowych, rządowych i badawczych.

Militarna część infrastruktury została wydzielona z sieci (w 1983 r.) pod nazwą MILNET (ang. Military Network), a z pozostałych zasobów utworzono nową sieć pakietową DARPA (ang. Defense ARPA), przeobrażoną później w ogólnoświatową sieć Internet.

Najstarszy i ciągle jeszcze popularny protokół X.25 był podstawą tworzenia komputerowych sieci pakietowych i gorszej jakości sieci rozległych

Technologia ATM. Technologia ATM (ang. Asynchronous Transfer Mode) powstała w wyniku kompromisu między dwoma już funkcjonującymi technikami cyfrowej transmisji szerokopasmowej: STM (ang. Synchronous Transfer Mode) i PTM (ang. Packet Transfer Mode), łącząc zalety istniejących technologii przy jednoczesnej eliminacji większości wad tych systemów. Technika STM jest stosowana w sieciach ISDN, PTM zaś w lokalnych sieciach komputerowych.

Wywodząca się z telekomunikacji technologia ATM jest coraz częściej postrzegana jako technika łącząca standard przekazów telekomunikacyjnych sieci SDH (ang. Synchronous Digital Hierarchy) na poziomie warstwy fizycznej z różnymi sieciami komputerowymi.

Współcześnie tworzone sieci ATM osiągają bardzo duże rozmiary zarówno ze względu na rozpiętość geograficzną, jak też liczbę podłączonych do niej urządzeń końcowych, powodując wzrost komplikacji budowanych struktur. ATM staje się obecnie najbardziej rozpowszechnianą technologią szkieletową dla złożonych sieci kampusowych, korporacyjnych, metropolitalnych i regionalnych.

Technologia ATM jest obecnie jedna, z najbardziej efektywnych technologii przekazu z wirtualizacją kanałów komunikacyjnych przeznaczonych do przesyłania usług multimedialnych (głosu, obrazu i danych), i także jest uważana za docelową technikę transmisji w szerokopasmowych sieciach rozległych WAN. Łączy zalety techniki pakietowej z przekazami synchronicznymi przez sieci SDH.

Regionalne i metropolitalne sieci ATM są przystosowane do świadczenia usług w różnorodnych zastosowaniach:

- tworzeniu wirtualnych sieci korporacyjnych dla indywidualnych klientów;
- udostępnianiu usług centralnych baz danych poszczególnym klientom działającym w środowisku rozproszonym;
- zapewnianiu klientom sprawnego dostępu do sieci zewnętrznych, przede wszystkim do usług internetowych;
- świadczeniu usług informatycznych wybranym klientom.

Standard ATM, opracowany pierwotnie jako element specyfikacji BISDN (CCITT, 1988 r.), nie definiuje dokładnie konkretnego medium transmisyjnego między węzłami, lecz zasady komunikacji w sieci. Umożliwia to zastosowanie

- zapewnianie współpracy z liniami transmisyjnymi o standardowej przepływności do 64 kb/s z rozszerzeniem (od 1993 r.) do 2 Mb/s.

Funkcjonowanie sieci X.25 i technika przełączania pakietów są określone zaleceniami CCITT/ITU-T, obejmującymi:

- X.3 - zalecenia w zakresie funkcjonowania urządzeń konwersji pakietowej PAD;
- X.25 - funkcje interfejsu między DCE i DTE przez sieci publiczne;
- X.28 - formaty komunikacji między terminalem a multiplekserem PAD;
- X.29 - formaty komunikacji między hostem a multiplekserem PAD;
- X.32 - zalecenia dla synchronicznej transmisji X.25 przez sieci komutowane;
- X.75 - procedury kontroli międzysieciowej łączące odrębne sieci X.25.

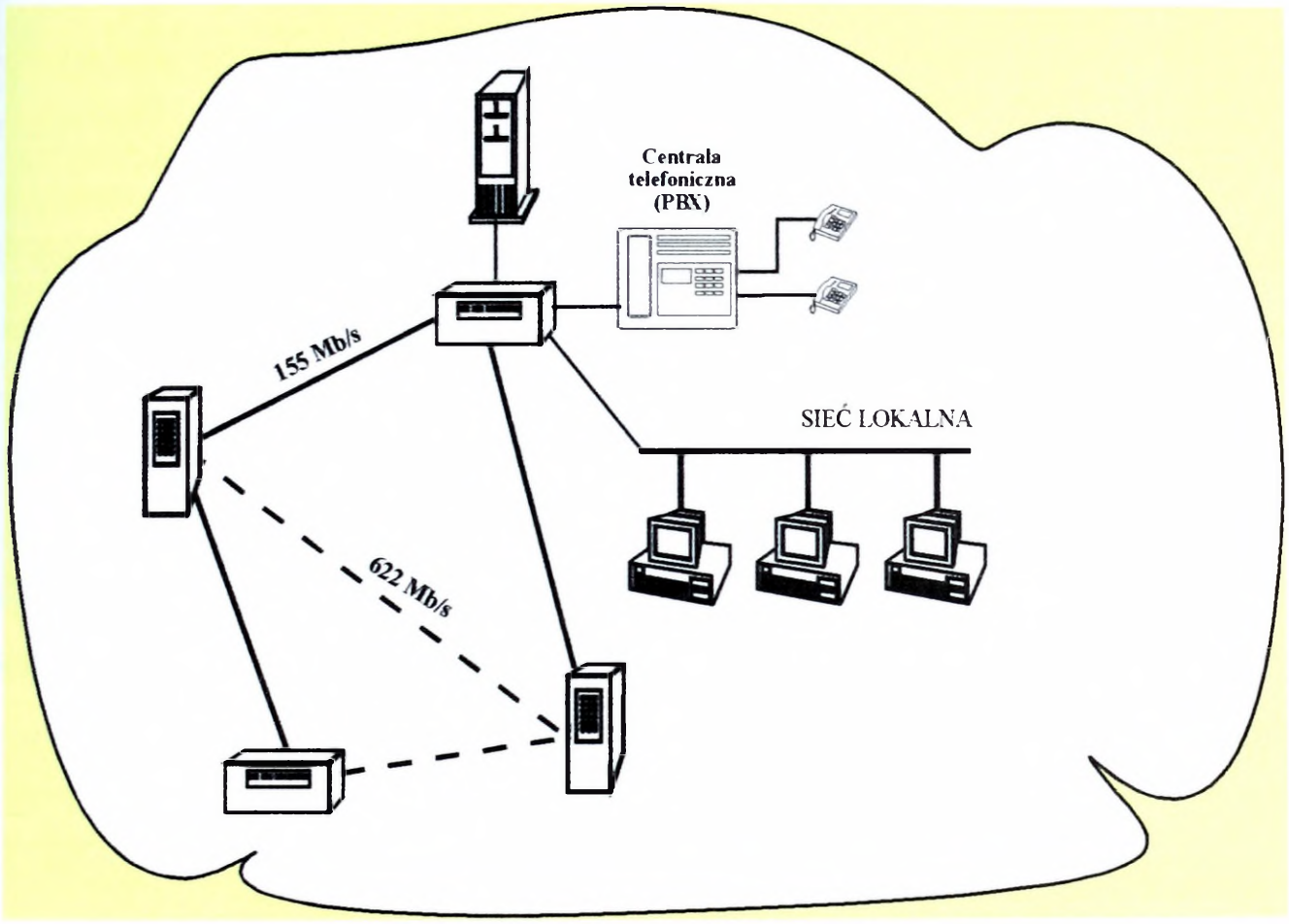
W zależności od wyposażenia technicznego urządzeń końcowych dostęp użytkownika do sieci z protokołem X.25 uzyskuje się za pomocą następujących metod:

- dostępu bezpośredniego dla abonentów posiadających wydzielone łącza i synchroniczne urządzenia typu DTE (ang. Data Terminal Equipment). Urządzeniami końcowymi DTE mogą być: terminal, karta synchroniczna komputera PC lub router sieci lokalnej z protokołem X.25. Telekomunikacyjne łącze dzierżawione jest wyposażone po obydwu stronach w modemy synchroniczne typu DCE (ang. Data Communication Equipment);
- dostępu komutowanego za pomocą sieci publicznej PSTN (ang. Public Switched Telephone Network) oraz protokołów X.25 łącznie z X.32. Protokół X.32 jest podobny do X.25, lecz umożliwia połączenia urządzeń DTE z siecią X.25 w trybie synchronicznym przez łącza komutowane;
- dostępu komutowanego PAD przez port szeregowy asynchronicznego urządzenia typu DTE (terminale znakowe) i sieć komutowaną. Urządzenie końcowe użytkownika w tym przypadku jest wyposażone w oprogramowanie z protokołem X.28, a sieć pakietowa (X.25) w porty asynchroniczne sieciowego multipleksera PAD (ang. Packet Assembler Disassembler).

początkowo jako sieć podkładowa, docelowo jako jednorodna forma transmisji globalnej ATM.

Schemat 2.12.

Sieć ATM integrująca sieć lokalną oraz sieć rozległą (Wariant)



Źródło: Opracowanie własne na podstawie: *Koncepcja wykorzystania technicznych środków najnowszej generacji w systemie łączności na potrzeby sytuacji kryzysowych*, Praca pod kier. M. Krauze, AON, Warszawa 2000.

Przekaz informacji w standardzie ATM charakteryzuje się następującymi właściwościami:

- przesyłaniem stałych porcji informacji o pojemności 53 bajty (w tym 48 bajtów informacji użytecznej), co ułatwia proces ich obróbki w węzłach sieci ATM;
- ustalaniem indywidualnych połączeń o dowolnej szybkości w obrębie przyjętych lub istniejących standardów (25 Mb/s, 100 Mb/s, 155 Mb/s, 622 Mb/s, 2500 Mb/s), dzięki przyporządkowaniu dowolnej liczby komórek do konkretnego połączenia użytkownika;

technologii ATM w różnorodnych już istniejących środowiskach transmisyjnych wykorzystujących jako medium zarówno przewody koncentryczne (sieci lokalne, sieci rozsiewcze), światłowodowe (sieci LAN, MAN), jak i bezprzewodowe (sieci globalne). Od 1993 r. wszyscy liczący się producenci implementują technologię ATM we własnych urządzeniach przełączających (huby, przełączniki, routery).

Uniwersalność technologii ATM polega na możliwości przesyłania informacji o dowolnym przeznaczeniu przez różne rodzaje nośników, niezależnie od stosowanych przepływności czy rozmiarów już istniejących sieci. Technologia ATM zapewnia podstawowy przekaz informacji w trybie połączeniowym, co oznacza, że przed przesłaniem informacji właściwej musi wystąpić faza zestawienia łącza (również wirtualnego) na podstawie parametrów deklarowanych przez abonenta (typ usługi, przewidywana przepływność, docelowy adres), a po zakończeniu przekazu - jego likwidacja.

Technologia ATM jest techniką asynchroniczną, co oznacza, że szybkość transmisji w ramach kanału wirtualnego jest zmienna, zgodna z szybkością źródła lub najbliższego węzła. Parametry zadeklarowane we wstępnej fazie mogą ulegać renegocjacji, przy czym sieć zwykle redukuje częstotliwość negocjacji, jak też zapotrzebowanie na szerokość pasma.

W sieci ATM węzły nie sprawdzają poprawności przesyłanej informacji, a kontrola błędów jest prowadzona w systemach użytkowników końcowych. Do tej pory ukształtowały się następujące klasy przepływności w sieciach ATM: 25 Mb/s (w zaniku), 100 Mb/s, 155,52 Mb/s (powszechnie stosowane) oraz 622 Mb/s i 2,5 Gb/s dla sieci transportowych SDH (Schemat 2.12.).

Za pomocą technologii ATM są świadczone usługi na wielu poziomach:

- sieci lokalnych ATM/LAN - współpracujących bezpośrednio ze stacjami roboczymi w tradycyjnych technologiach komputerowych (Ethernet; Token Ring, FDDI);
- sieci rozległych - stosujących różne technologie dostępu (Frame Relay, SMDS) lub ATM, ale zapewniające przepływ danych w formacie ATW do urządzeń sieci publicznej;
- urządzeń sieci publicznej - jako centrale komutacyjne ATM współpracujące z siecią transmisyjną PDH, SDH lub SONET;

Tabela 2.8. Zalety i wady technologii ATM

Zalety ATM.	Wady ATM.
- przekaz cyfrowy o wysokiej i skalowanej przepływności; - jeden interfejs fizyczny z siecią szerokopasmową, zapewniający dostęp do wszystkich usług możliwych do realizacji w sieci (transmisja głosu, obrazu i danych o dowolnej szybkości bitowej); - elastyczne konfigurowanie (komutacja i transmisja) sieci niezbędne dla usług o nieprzewidywalnych parametrach transmisji; - integracja fizyczna i funkcjonalna zapobiegająca zwielokrotnianiu zasobów i łączy dla wielu usług w odrębnych sieciach (separacja kanałów i łączy); - połączenie z sieciami transportowymi o innej strukturze (FR, SMDS, X.25); - możliwość tworzenia cyfrowych sieci hybrydowych.	- wysoki narzut na sygnalizację systemową wynoszący 9,4%, - wnoszenie opóźnień podczas pakietowania przy nadawaniu i rozpakietowaniu po stronie odbiorczej, - losowe opóźnienie przejścia pakietów przez sieć, - możliwość utraty pakietów z powodu przepełnienia buforów w przełącznikach źle zwymiarowanych pod kątem aplikacji, - konieczność ciągłego nadzoru nad rzeczywistymi parametrami wszystkich aktywnych połączeń.

Źródło: Opracowanie własne na podstawie: *Net World Vademecum teleinformatyka cz. 1, 2, 3,* International Data Group Poland S.A., Warszawa 2004.

Ad.4. Urządzenia końcowe
Ad. a) telefony analogowe i cyfrowe

Telefon analogowy. Najprostszym, powszechnie stosowanym urządzeniem telefonii abonenckiej, służącym do przetwarzania mowy na sygnały elektryczne i przesyłania ich na odległość przez system komutacji (centralę telefoniczną), jest aparat telefoniczny. Mowa abonenta nadającego jest przetwarzana w mikrofonie na sygnały elektryczne w paśmie przenoszenia od 300 Hz do 3400 Hz, natomiast sygnały elektryczne odbierane z linii są przetwarzane na dźwięki w słuchawce lub głośniku. Mikrofon i słuchawka tworzą zwykle zespół o wspólnej obudowie, zwanej mikrotelefonem, a układy dzwonienia i wybierania numerów (kilka typów) są zasilane bezpośrednio z linii telefonicznej.

Rozróżnia się wiele podziałów aparatów telefonicznych ze względu na:

- sposób dostępu: abonenckie, towarzyskie, wewnętrzne, publiczny samoinkasujące (automaty wrzutowe, na kartę i kodem PIN SIM);

- obsługą transmisji izochronicznych (głos, obraz ruchomy, HDTV) z opóźnieniem nie większym niż 10 ms, przez zastosowanie przełączników ATM z szybkim przełączaniem komórek i połączeń;
- skalowaniem przepływności ścieżek i węzłów ATM, dzięki czemu wykorzystuje się w pełni maksymalną przepływność dowolnego medium transportowego. Wysoka przepływność torów światłowodowych w sieciach LAN i WAN stosowana do multipleksacji statystycznej poszczególnych kanałów pozwala na efektywne gospodarowanie łączem transmisyjnym;
- tworzeniem przekazów głównie w trybie połączeniowym, co oznacza, że przed wysłaniem informacji właściwej występuje faza zestawienia łącza - według parametrów deklarowanych przez abonenta (typ usługi, przewidywana przepływność, deklarowany adres), a po zakończeniu przekazu -jego likwidacja;
- wirtualizacją połączeń przez sieć zarówno dla pojedynczych kanałów, jak i definiowanych grup kanałów zwanych ścieżkami. Jest to możliwe dzięki istnieniu odpowiednich identyfikatorów VCI (ang. Virtual Channel Identifler) dla kanałów oraz identyfikatorów VPI (ang. Virtual Path Identifier) dla ścieżek wirtualnych. Pola tych identyfikatorów znajdują się w nagłówku każdej komórki ATM przesyłanej przez sieć;
- adaptacją strumienia komórek ATM do dowolnej przepływności medium transportowego, przez wprowadzanie komórek pustych, pomijanych w węźle docelowym;
- przypisaniem komórkom ATM (kanałowi, ścieżce, połączeniu między użytkownikami) konkretnej usługi, której parametry mogą być dynamicznie zmieniane, zarówno w fazie nawiązywania łącza, jak i w trakcie działania usługi komunikacyjnej;
- zapewnianiem „przezroczystości" przenoszenia informacji przez sieć ATM, a więc dostosowanie pracy sieci z różnymi protokołami komunikacyjnymi i do realizacji różnych usług.

Z analizy właściwości sieci asynchronicznej ATM wynika, że podczas jej eksploatacji przeważają zalety nad wadami (Tabela 2.8.).

narodowych, z podstawowymi znakami interpunkcji) i wyświetlacza alfanumerycznego.

W nowoczesnych telefonach ISDN, zamiast 32- lub 64-znakowego wskaźnika alfanumerycznego, są instalowane monitory graficzne LCD w formatach CIF i QCIF stanowiące pomoc w realizacji wielu funkcji aparatu ISDN, takich jak: Interpretacja funkcji klawiszy, zegar, budzik, kalendarz, sekretarka, miniksiążka telefoniczna, taryfikacja i przenoszenie rozmów oraz wyświetlanie: numerów telefonów realizowanego połączenia, nadsyłanych komunikatów SMS (ang. Short Message System), stanu skrytki pocztowej i wielu innych.

Aparat ISDN jest wyposażony w:

- system sterujący do przeglądania klawiatury, sterowania wyświetlaczem, wysyłania i odbierania danych w kanałach B i D;
- kodek do przetwarzania A/C i C/A sygnałów fonicznych zgodnie ze standardem PCM (niekiedy ADPCM). Tor akustyczny może mieć dodatkowe wzmacniacze - w aparatach „głośno mówiących";
- klawiaturę numeryczną i dodatkowo funkcyjną lub alfanumeryczną, w zależności od rozbudowy funkcji i udogodnień dla usług dodatkowych;
- wyświetlacz alfanumeryczny do wizualizacji krótkich komunikatów, aktualnego stanu połączenia, znaczenia klawiszy funkcyjnych, numeru abonenta wywołującego, innego zgłoszenia itp.;
- blok sygnalizacji akustycznej do wytwarzania sygnału wywołania i alarmu w razie występowania trudności w uzyskaniu połączenia;
- układy interfejsowe dostępu do styku S.

Do podstawowego zestawu usług ISDN i udogodnień świadczonych przez sieć dla telefonów cyfrowych są włączone również funkcje: zestawianie połączeń konferencyjnych, pamiętanie zbioru najczęściej używanych numerów, rejestracja zgłoszeń w czasie nieobecności abonenta, przekazywanie zgłoszeń pod wskazane numery, informacje o opłatach, czas trwania rozmowy, zegar, kalendarz, zamawianie automatycznego budzenia, czy rozmów na określoną godziną itp.

Ad. b) teleksy

Teleks to drukujący aparat telegraficzny pracujący w wydzielonej komutowanej sieci teleksowej według 5-bitowego alfabetu Baudota, stosowany

- sposób wybierania numerów: w systemie dekadowym, w systemie tonowym DTMF;
- metodę przyłączenia: przewodowe, bezprzewodowe (radiowe, bezsznurowe, komórkowe analogowe, komórkowe cyfrowe);
- rodzaj transmisji; analogowe tradycyjne (300-3400 Hz), cyfrowe (16, 32, 64 kb/s);
- różnorodność funkcji: klasyczne, wielofunkcyjna (pamięć numerów, wybieranie skrócone, blokada wywołań, przenoszenie rozmów, rotacja przywołań, wybierania automatyczne Hp.), z usługą ISDN przez łącza cyfrowe 2B+D;
- konstrukcję: dyspozytorskie, sekretarsko dyrektorskie głośno mówiące, dla niepełnosprawnych, dla trudnych warunków pracy, itp.;
- bezcentralowe, z wbudowanymi układami priorytetu i kanałami do równoczesnego prowadzenia rozmów wewnętrznych i zewnętrznych na jednej współdzielonej linii.

Telefon cyfrowy. Mianem telefonu cyfrowego ISDN określa się aparat telefoniczny przystosowany do współpracy ze stykiem S cyfrowej sieci telekomunikacyjnej ISDN. Od strony sieci funkcję styku S realizuje urządzenie zwane zakończeniem sieciowym NT (ang. Network Termination). Węzeł ten zapewnia cyfryzację linii abonenckiej, umożliwiając jednoczesną, dwukierunkową transmisję w dwóch kanałach B i jednym kanale D o łącznej przepływności (2x64+16)=144 kb/s na normalnej parze miedzianych przewodów kablowych, dotychczas używanych do przyłączenia pojedynczego telefonu analogowego.

Aparat telefoniczny ISDN jest typowym przedstawicielem jednofunkcyjnych terminali ISDN przeznaczonych do realizacji wybranej usługi z wielu oferowanych przez sieć ISDN. Tor rozmowny zajmuje jeden z kanałów typu B (64 kb/s); sygnalizacja przez kanał D (16 kb/s) realizuje protokoły połączeniowe i sygnalizacyjne LAP-D i DSS1, w tym również obsługę usług dodatkowych. Aparat ISDN zawiera kodek PCM i złożony układ sterowania do sygnalizacji oraz realizacji usług dodatkowych. Usługi te wymagają dodatkowo, poza normalną klawiaturą numeryczną, uproszczonej klawiatury alfabetu (bez znaków

cyfrowe łącza telekomunikacyjne. Umożliwia przekaz 1 strony formatu A4 w czasie krótszym od 10 s.

Zwiększanie szybkości przekazów faksowych dokonuje się dzięki odpowiedniej kompresji i kodowaniu informacji pierwotnej, zmniejszającej nawet kilkanaście razy pliki obrazowe podlegające transmisji. Z wielu metod kodowania informacji, standaryzację uzyskały trzy metody: kodowanie jednowymiarowe MH za pomocą słów kluczowych kodu MH (ang. Modyfied Huffman) w obrębie każdej pojedynczej linii rozwinięcia, kodowanie dwuwymiarowe uwzględniające podczas kodowania stan informacji w sąsiednich linii skanujących, kodowanie z podwójną modyfikacją zapewniające najwyższy stopień kompresji obrazu.

Do najbardziej cenionych parametrów urządzeń telefaksowych zalicza się: wysoką rozdzielczość (720x360,600x600), druk laserowy, druk kolorowy i wykonywanie dokumentów na zwykłym papierze.

Ad. d) pagery

Niezwykle prosta konstrukcja niewielkich (ok. 75x50x15 mm) i lekkich (50 do 100 g) odbiorników przywoławczych sprawia, że pagery są produkowane w milionach egzemplarzy i przy stosunkowo niskiej cenie zapewniają najprostsze usługi przywołań w zasięgu kilkudziesięciu kilometrów. Spośród kilkunastu już funkcjonujących w Polsce klasycznych systemów przywoławczych pagery działają w dwóch typach sieci:

- standardu MBS - w ogólnopolskiej sieci Polpager (TP SA) przywołującej za pomocą nadajników radiowych UKF-FM (na trzeciej harmonicznej pilota sygnału stereofonicznego 57 kHz) emitujących w dolnej części pasma UKF;
- standardu POCSAG - z przywołaniami w zakresie 160 MHz - w sieciach zarządzanych przez prywatnych operatorów.

Z wyjątkiem jedynego krajowego („pisklak" w sieci Puls) pagera wszystkie pozostałe urządzenia przywoławcze (bipery) pochodzą od światowych i renomowanych firm.

Ad. e) zestawy wideofniczne

Ze względu na złożoność i stopień integracji funkcji występujących w terminalach cyfrowych do przekazów wideofonicznych urządzenia końcowe są

wyłącznie do przekazów tekstowych. Urządzenie, zwane dawniej dalekopisem, pracuje z szybkością 66 słów na minutę przy szybkości modulacji 50 Bd w asynchronicznym trybie pracy. Abonent ma własne doprowadzenie abonenckie, numer oraz tarczę cyfrową do uzyskania połączenia z innymi abonentami.

Dalekopis pracuje jako urządzenie bez obsługi, przesłanie wiadomości z sieci powoduje automatyczne włączenie, wydrukowanie tekstu i wyłączenie urządzenia. Ze względu na konstrukcję wyróżnia się dalekopisy mechaniczne i elektryczne oraz taśmowe i arkuszowe. Obecnie są zastępowane telefaksami i faksmodemami umożliwiającymi przekaz dokumentów w postaci graficznej.

Ad. c) faksy

Przekazu kopii obrazów graficznych i dokumentów na odległość można dokonać łączem telefonicznym za pomocą urządzeń telefaksowych, zwanych również telefaksami (faksmodemami). Zarówno urządzenia, jak i sposób transmisji podlegają standaryzacji, która wyróżnia następujące grupy faksowania:

- telefaks grupy 1 (TFX1), przestarzały międzynarodowy standard komunikacji faksowej, umożliwiający transmisję jednej strony w czasie 6 s. Obecnie bardzo rzadko stosowany;
- telefaks grupy 2 (TFX2), standard umożliwiający transmisję jednej strony (format A4) w czasie 3 min. Jest wciąż realizowany przez większość urządzeń faksujących;
- telefaks grupy 3 (TFX3), obecnie stosowany międzynarodowy standard komunikacji faksowej przez linie analogowe. Umożliwia transmisję jednej strony w ciągu 1 min, przy zastosowaniu kompresji danych. Dla telefaksów tej grupy rozdzielczość pionowa wynosi 98 lub 196 linii na cal, a rozdzielczość pozioma 203 linie na cal - co daje 1,86 lub 3,72 min elementów na stronę o wymiarach 8,5x11 (cali). Strumień bitów przed transmisją jest kompresowany, a przywracany do postaci pierwotnej po stronie odbiorczej. Transmisja obrazu jest przeprowadzana z szybkością 14 400 b/s lub 9600 b/s (zastępczo 7200, 4800 i 2400 b/s);
- telefaks grupy 4 (TFX4), nowy międzynarodowy standard komunikacji faksowej, obsługujący transmisję przy szybkości 19 200 b/s za pośrednictwem linii telefonicznych oraz przy szybkości 64 kb/s przez

- wirtualny serwis ekonomiczny zawierający informacje o depozytach i kredytach bankowych, kursach walut, notowaniach giełdowych, informacje ze spółek oraz informacje dla kierowców o warunkach panujących na drogach;
- cztery inne serwisy informacyjne prezentujące bieżące komunikaty o pogodzie, tygodniowy horoskop, giełdę samochodową oraz informacje o firmie i abonentach sieci Centertel (książka telefoniczna abonentów);
- poczta głosowa, w której można pozostawiać (maks. przez 3 dni) informacje pod nieobecność wywoływanego abonenta;
- połączenia trójstronne umożliwiające porozumiewanie się jednocześnie trzech rozmówców;
- informacja o nowym połączeniu oczekującym w trakcie trwania rozmowy. Po usłyszeniu sygnału o kolejnym połączeniu abonent może połączyć się na chwilę z osobą dzwoniącą - bez przerywania połączenia z poprzednim rozmówcą;
- przekazywanie połączeń przychodzących do abonenta na dowolnie wybrany inny numer. Rozmowy są przekazywane, gdy numer abonenta jest zajęty, nie odbiera on telefonu lub gdy aparat jest wyłączony;
- blokada rozmów wychodzących umożliwiająca zablokowanie wszystkich połączeń lub tylko międzynarodowych.

Cyfrowy telefon komórkowy. Asortyment telefonów komórkowych stosowanych od 1996 r. w dwóch krajowych sieciach cyfrowych GSM 900 (Era GSM zarządzana przez PTC oraz Plus GSM znajdująca się w gestii Polkomtela) oraz od marca 1998 r. w trzeciej cyfrowej GSM 1800 (Idea kierowanej przez Centertela) obejmuje wiele typów aparatów, działających dzięki najnowszej technologii przekazów cyfrowych.

Do cech charakterystycznych współczesnej generacji cyfrowych telefonów komórkowych należą:

- niewielka masa i grubość aparatów (ciężar poniżej 120 g, grubość nie przekraczająca 20 mm);
- czas rozmowy bez doładowania akumulatorów (powyżej 100 min);
- czas nasłuchu liczony w tygodniach (nie mniej niż 2 tyg.);

dzielone na trzy klasy:

- terminale wideofoniczne - proste urządzenia cyfrowe zaopatrzone w tekstowy wskaźnik ciekłokrystaliczny LCD lub niewielki ekran (Alcatel 2838);
- terminale komputerowe klasy PC wyposażone w kartę ISDN z kodekiem, kamerę, słuchawki i mikrofon do realizacji niektórych usług wzbogaconych (Vicon - Armada Cruiser 100);
- specjalizowane zestawy multimedialne spełniające funkcję stacji roboczej sieci z pełną ofertą usług w sieciach korporacyjnych.

Największym zainteresowaniem cieszą się gotowe zestawy multimedialne działające zarówno w pakietowych sieciach korporacyjnych, oparte na routerach, spełniające równocześnie funkcję zapory ogniowej, jak też przeznaczone do tworzenia informacyjnych stanowisk wideokonferencyjnych - nie wymagających zwykle szczególnego zabezpieczenia przed nieupoważnionym dostępem.

Ad. f) telefony komórkowe

Analogowy telefon komórkowy NMT. Unowocześniona wersja analogowego systemu NMT, oznaczona jako NMT 450i Plus, została wprowadzona na terenie Polski przez firmę Centertel w 1997 r. Ulepszone aparaty tej wersji produkuje i dostarcza głównie Nokia. Największym udogodnieniem dla abonenta działającego w nowym systemie jest usługa identyfikacji numeru osoby wywołującej rozmowę - CLIP (ang. Calling Line Identification Presentation), adaptowana z sieci telefonii cyfrowej.

Wprowadzana w systemie NMT usługa międzynarodowego prefiksu „+" ułatwia realizację połączeń zagranicznych, bez konieczności pamiętania różnych międzynarodowych kodów wyjściowych stosowanych w systemach komutacji. W nowym systemie możliwe jest również wysyłanie i odbieranie krótkich (do 160 znaków) komunikatów SMS (ang. Short Message Service), optyczna sygnalizacja o nadejściu informacji tekstowej lub komunikatu pozostawionego w pocztowej skrzynce głosowej, a takie możliwość korzystania z zegara wskazującego czas.

Do usług dodanych oferowanych przez Centertel, które już na stałe znajdują się w ofercie sieci analogowej NMT 450, należą:

przekraczające 100 g, z kolorowym ekranem graficznym, a także z kompletem usług fazy 2 standardu GSM umożliwiającym podwyższenie szybkości transmisji do 38 kb/s lub więcej.

Ad. g) terminale

Komputer osobisty - matematyczna maszyna licząca, zawierająca układy wejścia dla danych i wyjścia dla wyników obliczeń oraz wyposażona w zestaw wymiennych programów, umożliwiających modyfikowanie algorytmów postępowania. Pierwowzór komputera (maszyna analityczna) skonstruował Charles Babbage w połowie XIX w.; komputer elektryczny do kryptoanalizy zbudowali Brytyjczycy (1943 r.); pierwsza całkowicie elektroniczna maszyna cyfrowa ENIAC pojawiła się w 1946 r. (18 tys. elektronicznych lamp próżniowych, ciężar 30 ton). Prototyp komputera osobistego dopiero powstał w 1974 r. (MITS, Altair 8800, 256 bajtów pamięci).

Komputer sieciowy NC. Komputer Sieciowy NC (ang. Network Computer) powszechnie używana uproszczona i najtańsza wersja komputera osobistego - nazywana „odchudzonym klientem" - zawierająca jedynie niezbędne oprogramowanie pozwalające na uzyskanie połączenia z siecią. NC ma zainstalowaną przeglądarkę WWW, która umożliwia wykonywanie apletów przesyłanych z sieci (np. aplety ActiveX lub Java). Inne zadania (usługi) są wykonywane zazwyczaj przez tradycyjny system „opasłego klienta", instalowany na odległych serwerach sieciowych.

Pod ogólną nazwą komputer sieciowy (NC) kryją się różne rodzaje stacji terminalowych:

- komputer z oprogramowaniem instalowanym po stronie klienta - stanowiący stację pozbawioną dysku twardego i dysponujący jedynie zubożoną wersją jednego z popularnych sieciowych systemów operacyjnych;
- komputer sieciowy wykorzystujący oprogramowanie instalowane po stronie serwera - stanowi inteligentny terminal (bez dysku twardego) działający na aplikacjach wykonywanych przez serwer;

- przyjazna nawigacja (wybór) funkcji użytkowych za pomocą jednego przycisku;
- rozszerzona książka telefoniczna (powyżej 100 pozycji);
- nadawanie i odbiór krótkich komunikatów SMS (ang. Short Message Service);
- usługi transmisyjne (współpraca z komputerem przez złącze szeregowe RS-232 zamiast karty PCMCIA, także przez złącza podczerwieni);
- obsługa dwóch zakresów częstotliwości DB (Dual Band);
- wyposażenie samochodowe zezwalające na obsługę telefonu bez odrywania rąk od kierownicy pojazdu.

Do nowinek technicznych i funkcji wprowadzanych ostatnio w nowych modelach telefonów cyfrowych należą:

- duże ekrany wyświetlaczy wrażliwych na dotyk, co pozwala na wybieranie opcji lub numerów telefonów za pomocą palca lub specjalnego wskaźnika, także kolorowe ekrany graficzne;
- wdrażanie szybkiej transmisji danych typu HSCSD (ang. High Speed Circuit Switched Data) i transmisji pakietowej typu GPRS (ang. General Packet Radio Service) w telefonach komórkowych;
- głosowe wybieranie połączeń z numerami zarejestrowanymi w pamięci podręcznej aparatu lub na karcie SIM;
- implementacja protokołu WAP (ang. Wireless Application Protocol) udostępniającego abonentom komórkowym bezpośrednią łączność z Internetem i stronami webowymi;
- nowe sposoby kompresji zakodowanych sygnałów mowy za pomocą kodeków: EFR (ang. Enhanced Fuli Rate) i AMR (ang. Adaptive Multi Rate) przewidywanych w generacji 3G;
- wbudowana ekologiczna antena kierunkowa minimalizująca napromieniowanie głowy (Hagenuk - Duet Plus);
- słoneczne doładowanie akumulatorów (Nokia 1611);
- obsługa protokołu WAP (ang. Wireless Application Protocol).

Zaawansowane technicznie modele są zaliczane do nowej grupy aparatów komórkowych zwanych minitelefonami - o wymiarach poniżej 100 mm i masie nie

2.1.2. Analiza rzeczowo - wartościowa i ocena stanu infrastruktury telekomunikacyjnej w Polsce w latach 1989 ÷ 2003

U progu XXI-go wieku obserwujemy ogromny rozwój techniki i technologii cyfrowej. Zawrotna szybkość tego rozwoju przewyższa znacznie inne dziedziny nauki. Ewolucja sieci komputerowych pozwala na realizację wszelkich usług telekomunikacyjnych. Sieci pozwalają na szybką komunikację oraz wymianę danych między odległymi ośrodkami naukowymi bądź oddziałami wielkich firm lub banków. Dzięki aplikacjom stworzonym dla pracy grupowej odległość nie jest już największym problemem.

Bardzo użyteczną stała się elektroniczna poczta *e- mail*, która jest obecnie najlepszą i najszybszą formą przesyłania wiadomości oraz danych. Usługi WWW pozwalają na uzyskiwanie informacji z różnych, bardzo odległych punktów świata za pomocą jednego kliknięcia myszki. Użytkowanie komputerów nie ogranicza się już tylko do wykonywania pracochłonnych i żmudnych obliczeń czy też stosowania ich jako maszyny do pisania. Coraz częściej komputery wykorzystuje się do obróbki i przetwarzania dźwięku lub obrazu. Obecnie komputer podłączony do sieci stanowi doskonałe narzędzie do komunikacji multimedialnej. To wszystko zawdzięczamy w głównej mierze ogromnym możliwościom sieci komputerowych.

Zastosowanie światłowodów jako medium transmisyjnego w sieciach komputerowych i telekomunikacji było ogromnym krokiem w kierunku rozwiązania problemu przepustowości łączy. Uzyskanie szybkości transmisji danych rzędu setek Mb/s dało nowe dużo większe możliwości użytkownikom sieci komputerowych i telekomunikacyjnych. Współczesna infrastruktura teleinformatyczna obejmuje dwie do niedawna odrębne, a obecnie coraz bardziej przenikające się hierarchiczne struktury komunikacyjne:

- sieci telekomunikacyjne przewodowe i światłowodowe dla których centralnym punktem są analogowe i najnowsze cyfrowe systemy komutacji (centrale) wraz z różnorodnymi sieciami dostępu abonenckiego;
- cyfrowe sieci komputerowe oparte na strukturach sieciowych typu LAN, MAN, WAN. Sieci LAN tworzą podstawową infrastrukturę teleinformatyczną dostępu lokalnego sieci komputerowych.

- komputer klasy Net PC - będący specyficznym rodzajem komputera PC (z twardym dyskiem lub bez) platformy Windows, nie magazynującym lokalnie danych, polegając całkowicie na serwerze odległym.

Komputery przenośne - niewielkie, łatwe do przenoszenia komputery z zasilaniem akumulatorowym (bateryjnym). Wyróżnia się 3 coraz bardziej zacierające się kategorie komputerów przenośnych:

- laptopy - małe, ale o dużej mocy obliczeniowej komputery z różnymi systemami operacyjnymi (DOS, MS Windows) i wieloma aplikacjami;
- notebooki - mniejsze od laptopów, z przeznaczeniem do zastosowań ogólnych, coraz częściej zastępujące stacjonarne stacje robocze w przewodowym lub bezprzewodowym trybie pracy lokalnej,
- palmtopy - o wymiarach dłoni, z bardzo małym wyświetlaczem i niestandardową klawiaturą, projektowane do specjalnych zastosowań (terminarze, komunikatory, przekaz poczty elektronicznej), często bez klawiatury, z wprowadzaniem danych za pomocą rysika.

Informatyka, która wkroczyła w ostatnich latach w środowisko telekomunikacyjne, dała podstawy do praktycznej realizacji (adaptacyjne wykorzystanie przepływności kanałów, podniesienie szybkości w układach z kasowaniem echa, zmienna asymetria kierunków transmisji, gwarantowana jakość usług), jak i zmianę środowiska wokół abonenta (personalizacja abonenta, multimedialność usług, wizualizacja przekazów, wirtualizacja środowiska usługowego, rozwój systemów bilingowych, elastyczne korzystanie z zasobów sieci, działanie na rozproszonych bazach i inne). Zastosowanie w sieci telekomunikacyjnej nowoczesnych cyfrowych systemów komutacji, zastępujących dotychczasowe analogowe centrale telefoniczne, a także cyfryzacja sieci komunikacyjnej umożliwiają świadczenie nowych usług, daleko wykraczających poza ofertę dotychczas stosowanych klasycznych usług POTS.

Od strony technicznej przestały istnieć ograniczenia, zarówno na liczbę przyłączanych nowych abonentów, jak i szerokość pasma udostępnianego klientom sieci, otwierając możliwości korzystania z nowoczesnych i szerokopasmowych usług telekomunikacyjnych, wspomaganych komputerami i stale wzbogacanych programowo.

Polska staje obecnie przed nieco łatwiejszymi problemami do rozwiązania niż kiedyś. Nie ma już zastrzeżeń natury techniczno – ekonomicznej, co do kapitalizacji infrastruktury telekomunikacyjnej (nie znaczy to jednak, że takie problemy nie występują). Mamy obecnie szansę „przeskoczenia" pewnych etapów pośrednich w budowie nowoczesnej telekomunikacji. Od stycznia 1992 r. przedsiębiorstwo Poczta Polska, Telegraf i Telefon zostało podzielone na dwie firmy: Państwowe Przedsiębiorstwo Użyteczności Publicznej „Poczta Polska" i Telekomunikację Polską S.A.[145].

Na początku lat dziewięćdziesiątych zaledwie 40% populacji Polski miało dostęp do automatycznych łączy międzymiastowych. Pozostali mieszkańcy Polski byli zmuszeni do wielogodzinnego oczekiwania na zamówione połączenie międzymiastowe. Jakość połączeń i słyszalność były bardzo niskie, bardzo wysoki odsetek połączeń nie był w ogóle realizowany lub był realizowany błędnie. Sieć międzymiastowa była przestarzała i w fatalnym stanie technicznym.

Lata 90-te to przewartościowanie pojęć dotyczących telekomunikacji. Telekomunikacja przestaje kojarzyć się wyłącznie ze świadczeniem „tradycyjnych usług telefonicznych" przez jedynego operatora narodowego, jakim obecnie jest TP S.A. Ustawa o łączności z 1990 r. (i późniejsze jej nowelizacje), a szczególnie obowiązująca ustawa – „Prawo telekomunikacyjne"[146] z dn. 16. lipca 2004 r. dopuściła konkurencję w telekomunikacji. W myśl tej ustawy lokalni operatorzy mogą tworzyć własne sieci, a Telekomunikacja Polska S.A. ma obowiązek przyłączać ich do sieci użytku publicznego (ogólnokrajowej). Obecnie jest już wiele niezależnych operatorów - firm, które uzyskały koncesję na prowadzenie usług telekomunikacyjnych.

Kolejnym istotnym elementem wpływającym na rozwój telekomunikacji jest integracja Polski z UE. W 1994 roku Polska złożyła wniosek o przyjęcie do UE, w czerwcu 1997 roku Komisja Europejska wyraziła pozytywną opinię na temat

---

[145]TP S.A. powstała w wyniku przekształcenia w dniu 4 grudnia 1991 roku państwowej jednostki organizacyjnej "Poczta Polska, Telegraf i Telefon" (PPTiT)w Telekomunikacje Polską S.A. oraz Pocztę Polską. Do zakresu działania PPTiT należało wykonywanie objętych prawem wyłączności państwa usług łączności pocztowej i telekomunikacyjnej. Po przekształceniu na TP S.A. w przedsiębiorstwo telekomunikacyjne w sensie przedmiotowym, do którego przeszła zorganizowana część mienia, pracowników, oraz uprawnień i zobowiązań wydzielona uprzednio z całości majątku PPTiT. Wszystkie akcje nowego przedsiębiorstwa zostały objęte przez Skarb Państwa.

[146]Dz. U. Nr 171 poz. 1800, 2004.

W sieciach telekomunikacyjnych do połowy lat siedemdziesiątych, stosowano powszechnie technikę przesyłania sygnałów analogowych, za pomocą kanałów telefonicznych w podstawowym paśmie przenoszenia lub przez kosztowne, międzycentralowe urządzenia zwielokrotnienia częstotliwościowego o niewielkiej krotności kanałów rozmównych. Jako linie przesyłowe, stosowano wyłącznie pary kabli miedzianych o ograniczonej częstotliwości pracy, wymagające skomplikowanych filtrów, korektorów linii) i tłumików zakłóceń, przy przesyłaniu sygnałów o wyższych częstotliwościach[143].

Istotne zmiany w telekomunikacji stały się możliwe po opanowaniu cyfrowej techniki kodowania mowy, wprowadzeniu techniki zwielokrotnienia kanałów oraz światłowodów, a przede wszystkim włączeniu do sieci telekomunikacyjnej elementów komutacji (przełączania) pochodzących z technologii sieci komputerowych. Od kilku lat rośnie też zainteresowanie budową i modernizacją resortowych sieci telekomunikacyjnych, a w ostatnim czasie nowych sieci multimedialnych. To z kolei, spowodowało wzrost zainteresowania centralami, wyposażonymi w możliwość świadczenia usług ISDN i zaawansowanych usług multimedialnych.

Jeśli przypomnimy sobie dziś jeszcze wcale nie tak odległą przeszłość, to przed rokiem 1989 dostępność do usług telekomunikacyjnych w Polsce[144], ich jakość, powszechność i dostosowanie do potrzeb użytkowników sieci telekomunikacyjnej pozostawiały wiele do życzenia.

W 1989 roku na 100 mieszkańców Polski przypadało 8,2 abonentów, czas oczekiwania na zainstalowanie telefonu wynosił kilkanaście lat, na obszarach wiejskich na 100 mieszkańców przypadało 2,5 abonentów, a kilka tysięcy wsi nie posiadało żadnej łączności. Jakość usług telefonicznych stała na bardzo niskim poziomie, sieć telefoniczna była przestarzała i oparta na wychodzących z użycia w krajach rozwiniętych urządzeniach analogowych.

---

[143]Polska pod względem infrastruktury telekomunikacyjnej zajmowała wtedy jedno z ostatnich miejsc w Europie (przed Albanią i Rumunią). W dodatku zły stan techniczny sieci i urządzeń, pokazywał jak wielki wysiłek finansowy i organizacyjny będzie potrzebny, aby stworzyć warunki do rozwoju kraju.

[144]Występowało wówczas znaczne skumulowanie opóźnień w rozwoju nowoczesnych technik i technologii telekomunikacyjnych. Należy przy tym pamiętać, że istniała organizacja COCOM, która ograniczała sprzedaż sprzętu i rozwiniętej technologii do określonych krajów. Oznaczało to, że każda transakcja z zachodnim producentem, dotycząca sprzętu zastrzeżonego (nadającego się do wykorzystania na potrzeby militarne), mogła być zrealizowana tylko po uzyskaniu specjalnej zgody.

oczekiwania na przyłączenie do przewodowej sieci telefonicznej, którzy oświadczyli chęć przyłączenia się do którejś z działających sieci.

Problemem pozostaje także ciągle wspomniana różnica pomiędzy telefonizacją obszarów miejskich i wiejskich. Problem ten jest znaczący przede wszystkim ze względu na małą aktywność gospodarczą polskiej wsi, co powoduje, że podłączanie abonentów wiejskich jest mało opłacalne ekonomicznie i mało który z operatorów decyduje się na rozwój swojej sieci na obszarach wiejskich. Tymczasem większość przyznawanych koncesji obliguje operatorów do inwestowania zarówno na obszarach miejskich jak i wiejskich.

Liczba standardowych telefonicznych łączy głównych sieci publicznej (abonentów telefonii przewodowej bez łączy ISDN) wg stanu w dniu 31.12.2002 r. wynosiła około 10,92 mln, z tego w miastach - 8,2 mln, a na wsi – 2,75 mln (Tabela 2.9., Wykres 2.2.).

Tabela 2.9. Standardowe telefoniczne łącza główne(abonenci telefonii przewodowej) w latach 1990 – 2002

Standardowe telefoniczne łącza główne (abonenci telefonii przewodowej)	1990	1995	1999	2000	2001	2002
V liczbach bezwzględnych (w tys.)	3.293,0	5.728,5	10.076,2	10.740,2	10.934,4	**10.916,4**
miasta (w tys.)	2.902,0	4.924,3	7.872,0	8.181,9	8.290,0	**8.162,1**
wieś (w tys.)	391,0	804,2	2.204,2	2.558,3	2.644,4	**2.754,3**
Na 100 mieszkańców	8,62	14,84	26,07	27,79	28,30	**28,55**
miasta	12,28	20,62	32,95	34,27	34,76	**34,57**
wieś	2,69	5,46	14,93	17,32	17,89	**18,84**

Źródło: *Raport: Rozwój telekomunikacji - Infrastruktura – klucz do rozwoju, z realizacji programu: Strategia Gospodarcza Rządu - Przedsiębiorczość – Rozwój - Praca*, URM, Warszawa 2003, s. 3.

W 2002 r. utrzymywał się dynamiczny rozwój nowych technologii telefonii przewodowej. W końcu 2002 r. liczba telefonicznych łączy głównych[148] w sieci publicznej telefonii przewodowej wyniosła 11,7 mln (o 2,8% więcej niż przed rokiem), przy czym w miastach – 8,9 mln (o 1,8% więcej), a na wsi – 2,8 mln (o 5,9% więcej).

---

[148]Łącza główne to standardowe łącza główne (abonenci telefonii przewodowej) (POTS) + łącza ISDN.

polskiego członkostwa, a negocjacje w tej sprawie rozpoczęły się w marcu 1999 roku. Polskę przyjęto do UE z dniem 1 maja 2004 roku.

Pierwszy program rządowy dotyczący transformacji polskiej telekomunikacji zakładał, że w pierwszej kolejności zostanie zmodernizowana sieć międzymiastowa i międzynarodowa. W latach dziewięćdziesiątych nastąpił gwałtowny rozwój telefonii przewodowej w Polsce. Z informacji GUS wynika, że pomiędzy rokiem 1990 a 1998 liczba abonentów telefonii przewodowej wzrosła z około 3,3 miliona do 8,8 miliona.

Z dniem 1 stycznia 2002 r. rynek telefonii lokalnej i międzystrefowej został całkowicie zliberalizowany. Obok Telekomunikacji Polskiej SA działało na nim wówczas 63 niezależnych koncesjonowanych przez Ministra Łączności operatorów[147], a Prezes Urzędu Regulacji Telekomunikacji i Poczty (URTiP) wydał w 2002 roku kolejnych 41 zezwoleń, natomiast w 2003 r. - 21. Na koniec 2003 r. niezależni operatorzy, których jest 85, obsługiwali ok. 11 mln abonentów, osiągając ok. 10 proc. udziału w rynku.

W 2002 r. podobnie jak w latach poprzednich, miała miejsce dalsza wymiana i modernizacja sieci telekomunikacyjnej. Sprzedaż usług łączności ogółem (obejmująca wpływy za usługi pocztowe i kurierskie oraz za usługi telekomunikacyjne) była w cenach stałych o 8,8% większa niż w 2001 r., przy czym wzrost ten spowodowany był zwiększeniem sprzedaży usług telekomunikacyjnych.

Ceny związane z łącznością w 2002 r. w stosunku do roku poprzedniego obniżyły się o 0,1%. Usługi telekomunikacyjne były tańsze niż w 2001 r. średnio o 0,2%, w tym znacznie spadły opłaty za zainstalowanie telefonu (o 15,1%) oraz za rozmowy telefoniczne krajowe (o 7,0%). Podniesiono natomiast opłatę za abonament telefoniczny (o 10,5%), a ceny sprzętu telekomunikacyjnego obniżyły się o 2,4%.

Mimo gwałtownego rozwoju telekomunikacji w ciągu ostatnich kilkunastu lat, Polska nadal pozostaje krajem o zacofanej infrastrukturze telekomunikacyjnej. Bardzo duży popyt na usługi telekomunikacyjne powoduje m.in. bardzo długi okres

---

[147]Stan na czerwiec 2002 r. wg danych URTiP.

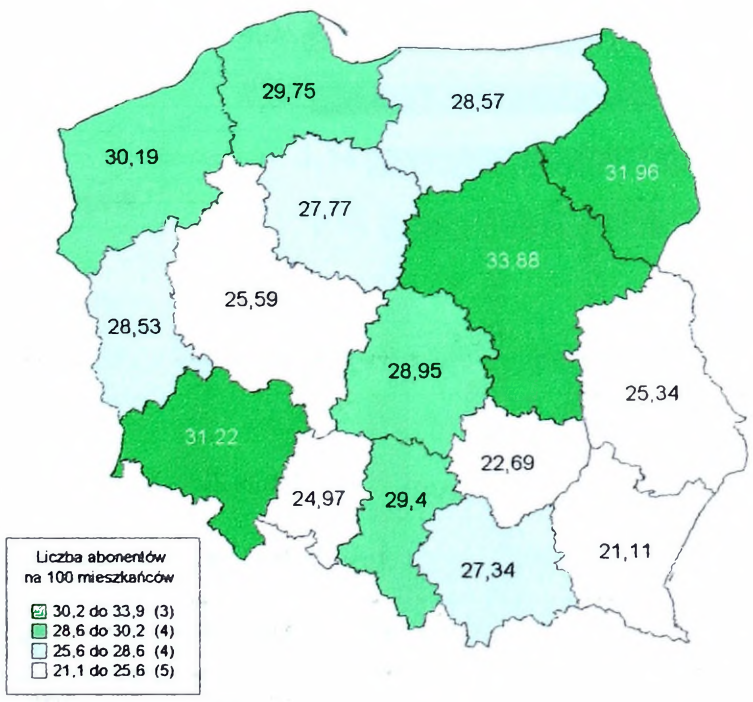
W I półroczu 2003 r. liczba łączy głównych w sieci publicznej telefonii przewodowej wyniosła 12,1 mln i była o 1,6% większa niż w końcu 2002 r. Liczba łączy w dostępach ISDN osiągnęła poziom ok. 1,1 mln (w tym ok. 90% zainstalowano w miastach) i była o ok. 33,5% większa niż w końcu 2002 r.

Udział pojemności telefonicznych central cyfrowych w ogólnej pojemności central automatycznych miejscowych zwiększył się z 87,2% w 2001 r. do 92,7% w 2002 r. W tym też roku pojemność telefonicznych central międzystrefowych automatycznych cyfrowych w porównaniu do roku poprzedniego wzrosła o 7,5%, a liczba telefonicznych łączy międzystrefowych i strefowych zwiększyła się o 11,8%. W końcu 2002 r. na 100 mieszkańców przypadało 28,6 abonentów.

Największą gęstość tej sieci (liczba abonentów na 100 mieszkańców) w końcu 2002 r. zanotowano w województwach: mazowieckim – 33,9, podlaskim – 32,0 i dolnośląskim – 31,2 a najmniejszą w podkarpackim – 21,1 (Mapa 2.3.).

Natomiast w końcu 2002 r. wskaźnik gęstości abonenckiej w Polsce, mierzony liczbą łączy głównych na 100 mieszkańców, wyniósł 30,72, dla Europy 41,5 (Wykres 2.3.).

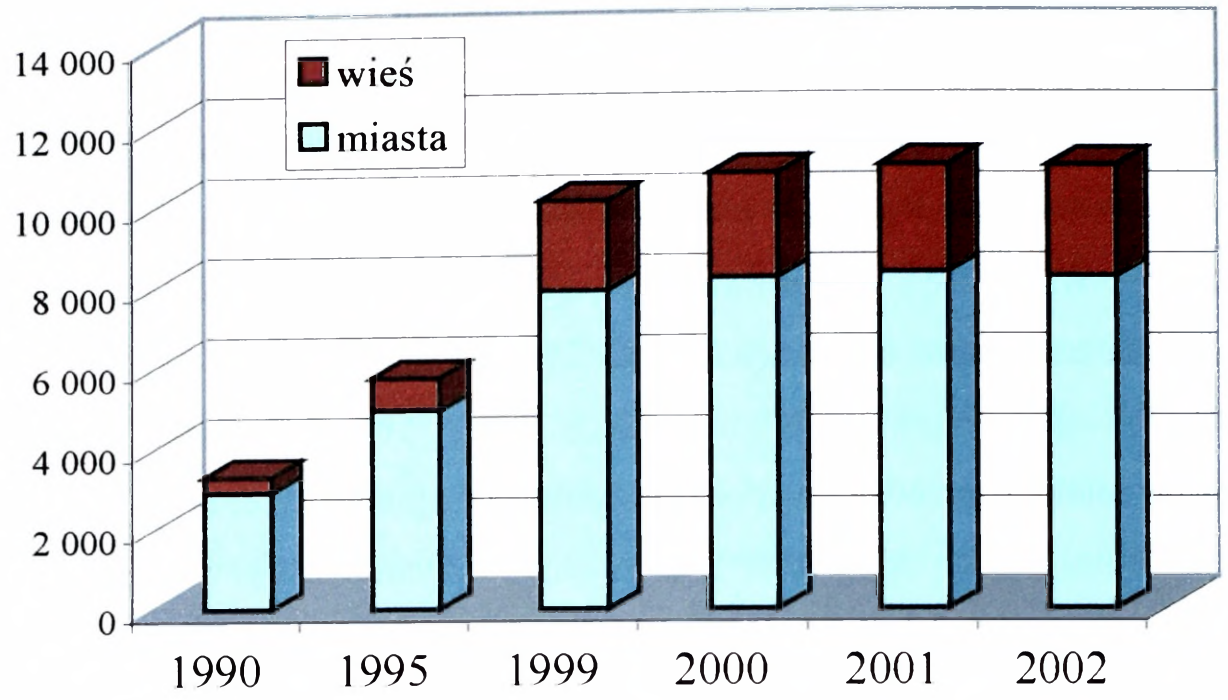
Mapa 2.3. Liczba abonentów na 100 mieszkańców – stan na 31.12.2002 r.



Źródło: *Analiza*: *Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 3.

Wykres 2.2.

Standardowe telefoniczne łącza główne (abonenci telefonii przewodowej – w tys.) w miastach i na wsi w latach 1990 – 2002



Źródło: *Raport: Rozwój telekomunikacji - Infrastruktura – klucz do rozwoju, z realizacji programu: Strategia Gospodarcza Rządu - Przedsiębiorczość – Rozwój - Praca*, URM, Warszawa 2003, s. 4.

W końcu grudnia 2002 r. liczba łączy w dostępach ISDN (sieć cyfrowa z integracją usług) wynosiła 827,8 tys. (w tym w miastach - 735,5 tys.) i była o 67,9% wyższa niż przed rokiem (Tabela 2.10.).

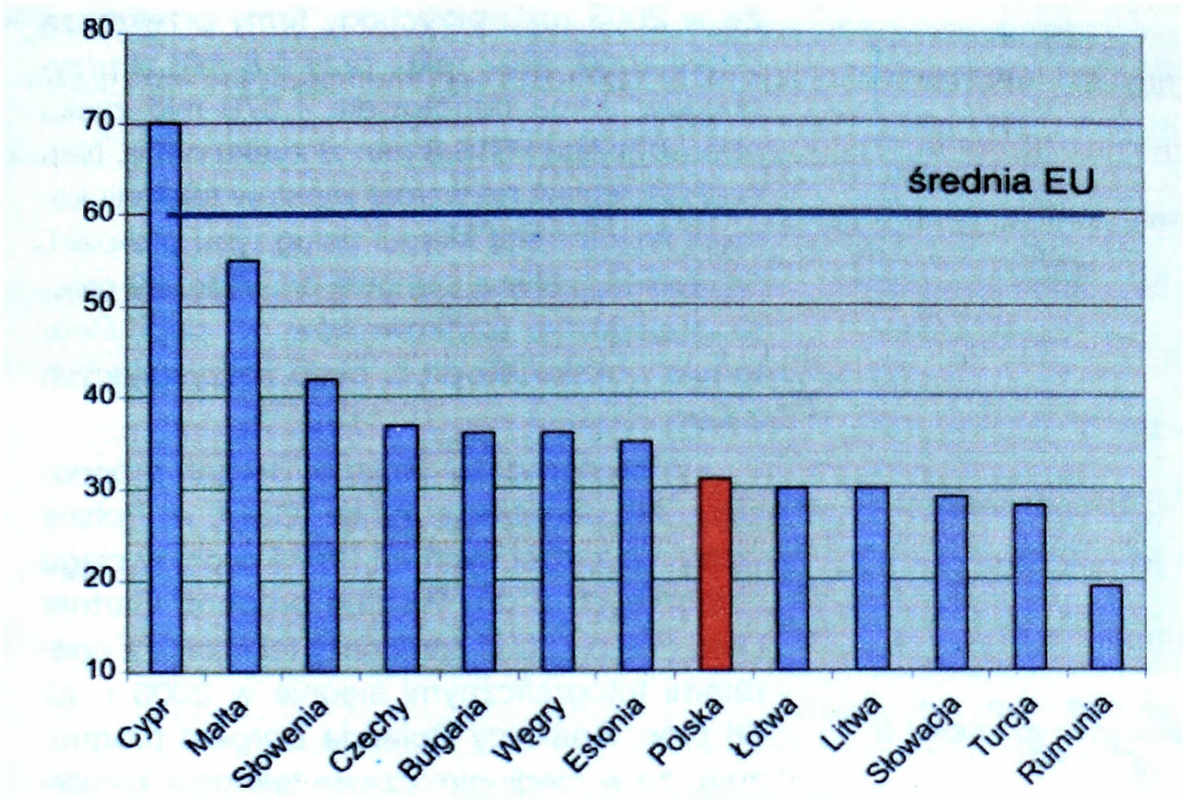
Tabela 2.10. Telefoniczne łącza główne (abonenci telefonii przewodowej + łącza ISDN) w latach 1999 - 2002

Telefoniczne łącza główne (abonenci telefonii przewodowej + łącza ISDN)	**1999**	**2000**	**2001**	**2002**
W liczbach bezwzględnych (w tys.)	10.175,2	10.946,7	11.427,4	**11.744,2**
- miasta (w tys.)	7.966,2	8.375,4	8.739,9	**8.897,5**
- wieś (w tys.)	2.209,0	2.571,3	2.687,5	**2.846,7**
Na 100 mieszkańców	26,32	28,33	29,58	**30,72**
- miasta	33,34	35,08	36,65	**37,68**
- wieś	14,97	17,41	18,18	**19,47**

Źródło: *Analiza: Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 1.

Wykres 2.4.

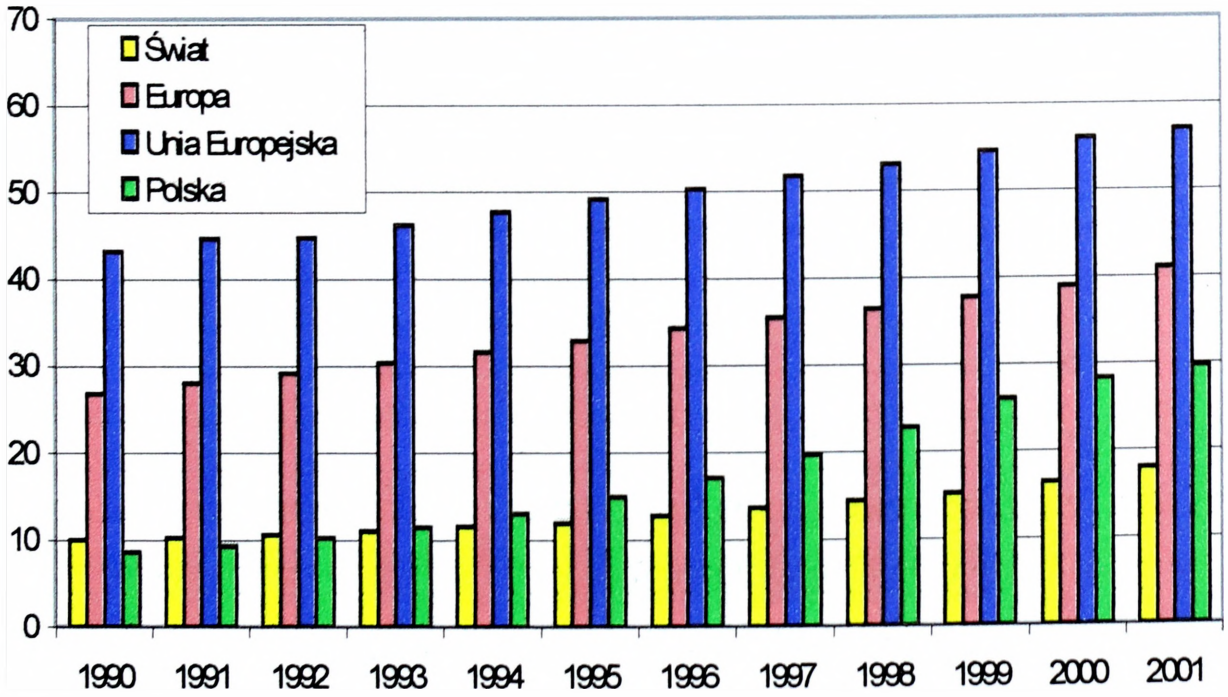
Ilość linii stacjonarnych na 100 mieszkańców w Polsce
na tle niektórych krajów Europy



Źródło: A. Strężyńska, *Raport o stanie i rozwoju sektora telekomunikacyjnego w Polsce za rok 2003*, w: „*Telekomunikacja 2004*", MSG-Media Bydgoszcz 2003, s. 9.

Wykres 2.5.

Liczba abonentów telefonicznych na 100 mieszkańców w Polsce na tle świata,
Europy i Unii Europejskiej

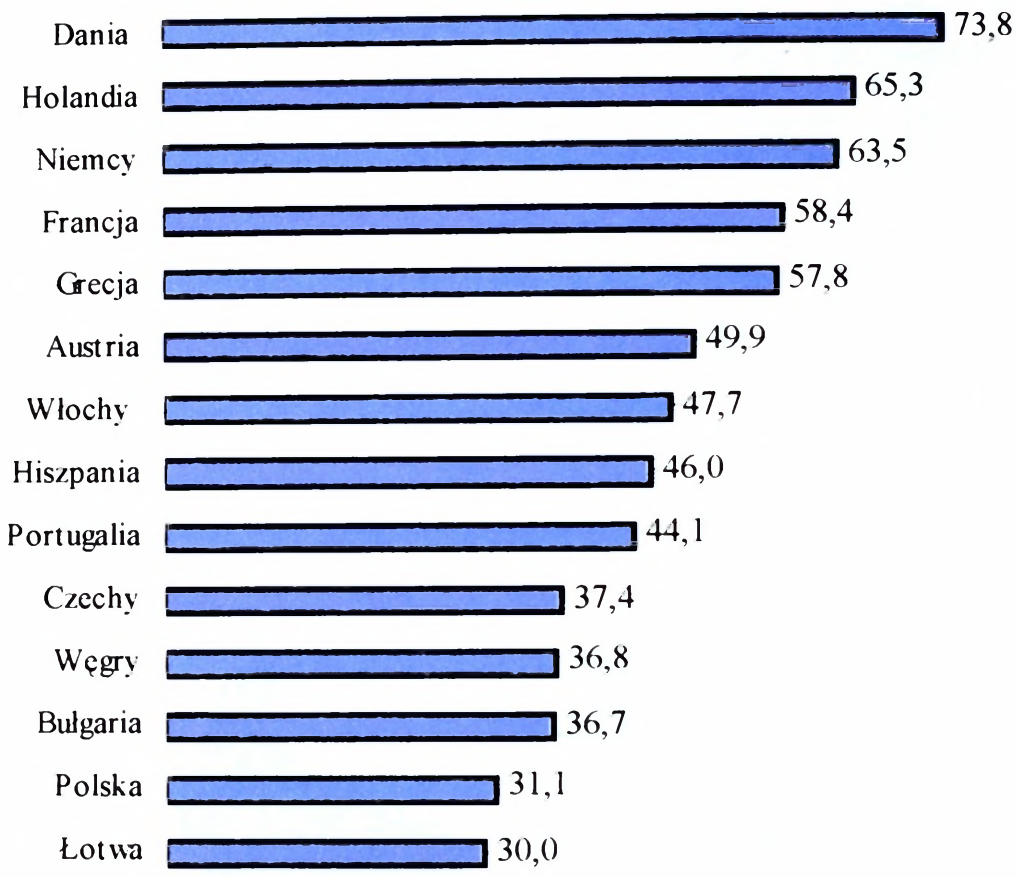


Źródło: Raport: *Rozwój telekomunikacji - Infrastruktura – klucz do rozwoju, z realizacji programu: Strategia Gospodarcza Rządu - Przedsiębiorczość – Rozwój - Praca*, URM, Warszawa 2003, s. 5.

Na koniec grudnia 2002 roku źródła Komisji Europejskiej podają gęstość telekomunikacyjną w Polsce na poziomie 34,7 proc., czyli o 3,6 proc. wyższą niż rok wcześniej i o 5,1 proc. wyższą niż dwa lata wcześniej. Byliśmy jednym z czterech krajów kandydackich, w których wzrosła liczba telefonów stacjonarnych, obok Cypru, Rumunii i Słowenii. Jednak źródła nie są precyzyjne i jednomyślne w swoich obliczeniach.

Wykres 2.3.

Polska na tle Europy - liczba abonentów telefonii przewodowej na 100 mieszkańców

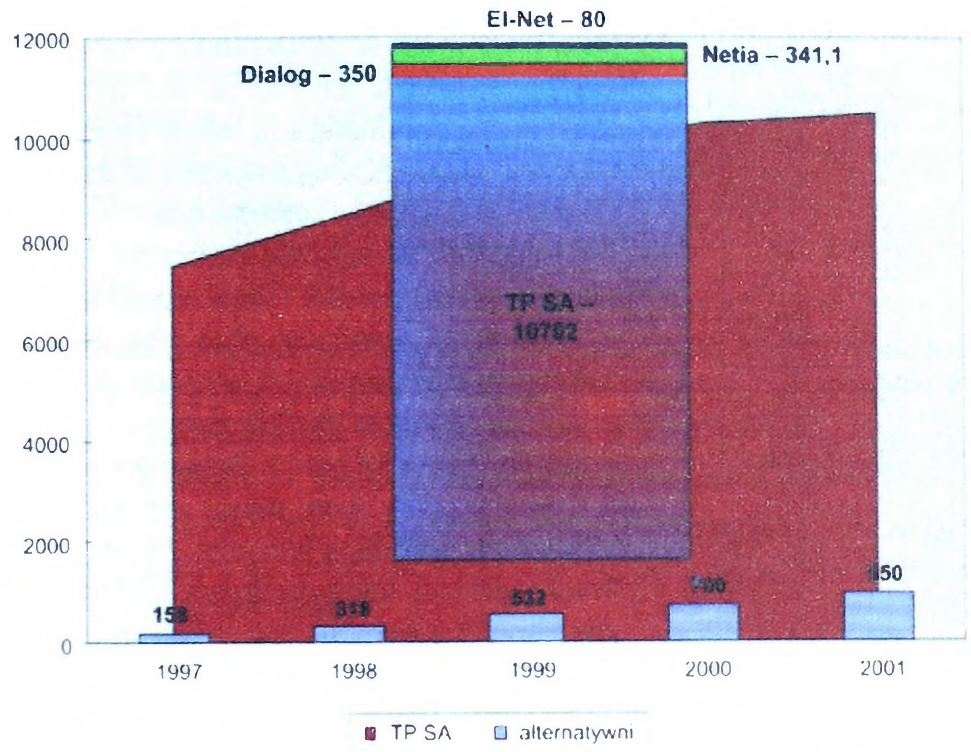


Źródło: *Analiza*: *Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 4.

Natomiast ilość linii stacjonarnych w Polsce na tle średniej w Unii Europejskiej oraz niektórych krajów Europy przedstawiał się w sumie niekorzystnie (Wykres 2.4.). Liczba abonentów telefonicznych na 100 mieszkańców w Polsce na tle Europy, Unii Europejskiej i świata, (Wykres 2.5.) dowodzi wyraźnego opóźnienia w telefonizacji kraju. Rzutuje ona bezpośrednio na obraz tendencji rozwoju infrastruktury telekomunikacyjnej.

Wykres 2.6.

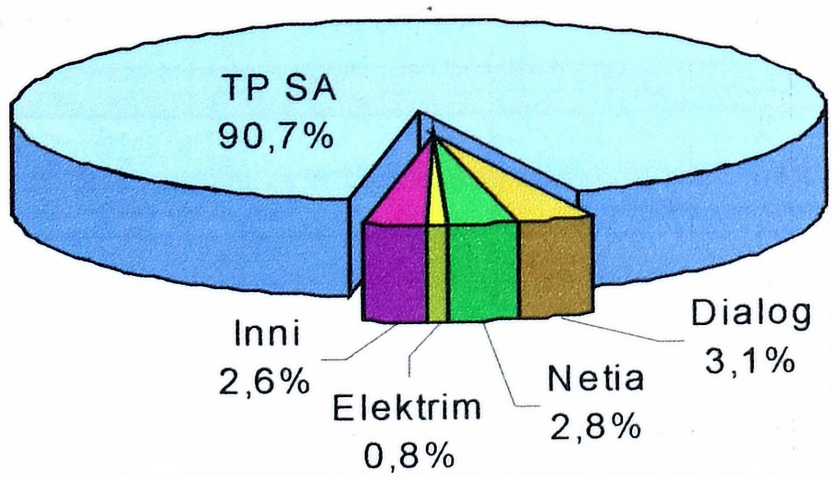
Podział stacjonarnego rynku telekomunikacyjnego pomiędzy TP S.A. i pozostałymi największymi operatorami telekomunikacyjnymi w latach 1997÷2001 (wg liczby linii)



Źródło: A. Strężyńska, *Raport o stanie i rozwoju sektora telekomunikacyjnego w Polsce za rok 2003*, w: „*Telekomunikacja 2004*", MSG-Media Bydgoszcz 2003, s. 9.

Wykres 2.7.

Udział w rynku telefonii przewodowej lokalnej (linie) w 2002 r.



Źródło: *Raport: Rozwój telekomunikacji - Infrastruktura – klucz do rozwoju, z realizacji programu: Strategia Gospodarcza Rządu - Przedsiębiorczość – Rozwój - Praca*, URM, Warszawa 2003, s. 3.

Cyfryzacja sieci sięgnęła 92 proc. na koniec 2002 roku. Dalszy rozwój rynku telekomunikacji przewodowej w Polsce będzie związany zarówno ze wzrostem wskaźnika gęstości abonenckiej jak i zwiększeniem wykorzystania sieci już istniejących. Osiąganie wskaźnika gęstości abonenckiej w wysokości 40%, powinno nastąpić w 2005 roku, będzie wymagało do tego czasu nakładów w wysokości równowartości około 10 mld USD.

W końcu I półrocza 2003 r zezwolenie telekomunikacyjne uprawniające do świadczenia powszechnych usług telekomunikacyjnych w sieciach stacjonarnych posiadało 85 operatorów, w tym 27 - do realizacji połączeń międzystrefowych i międzynarodowych.

Największym operatorem działającym na rynku polskim jest Telekomunikacja Polska S.A., obsługująca ponad 90% wszystkich abonentów telefonii przewodowej i mająca 95% udział w rynku połączeń międzystrefowych. Pozostała część rynku obsługiwana jest przez niezależnych operatorów telekomunikacyjnych (Tabela 2.11.) Podział rynku telekomunikacyjnego pomiędzy operatorami (Wykresy 2.6, 2.7, 2.8.) wskazuje na wiodącą w nim rolę TP S.A.. Rola i ranga pozostałych niezależnych operatorów ma charakter uzupełniający i jest zaledwie uzupełniająca w poszczególnych segmentach rynku.

Tabela 2.11. Ilość abonentów obsługiwanych przez największych niezależnych operatorów telekomunikacyjnych.

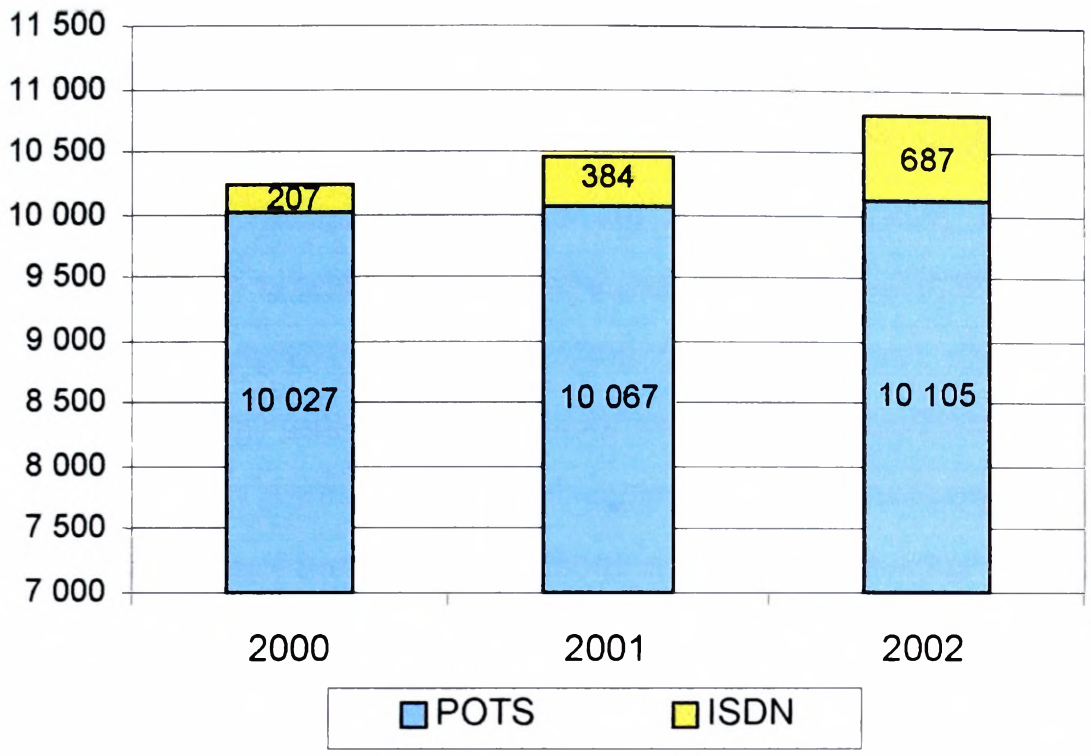
L.p.	Niezależny operator telekomunikacyjny	Ilość abonentów
1.	TPS.A.	10,9 mln
2.	Dialog	380 tys.
3.	Telenet Polska[149]	100 tys.
4.	NOM	100 tys.
5.	El-Net	65 tys.

Źródło: A. Strężyńska, *Raport o stanie i rozwoju sektora telekomunikacyjnego w Polsce za rok 2003,* w: „Telekomunikacja 2004", MSG-Media Bydgoszcz 2003, s. 8.

[149]Spółka grupy Telenet Polska zwiększona o Elektrim - Tv-Tel oraz Telefonię Polską Zachód.

Wykres 2.9.

Liczba łączy głównych TP S.A. w latach 2000 - 2002 r. (w mln)



Źródło: *Analiza: Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 2.

Tabela 2.13. Struktura ruchu wychodzącego z sieci TP S.A. w 2001 i 2002 r.

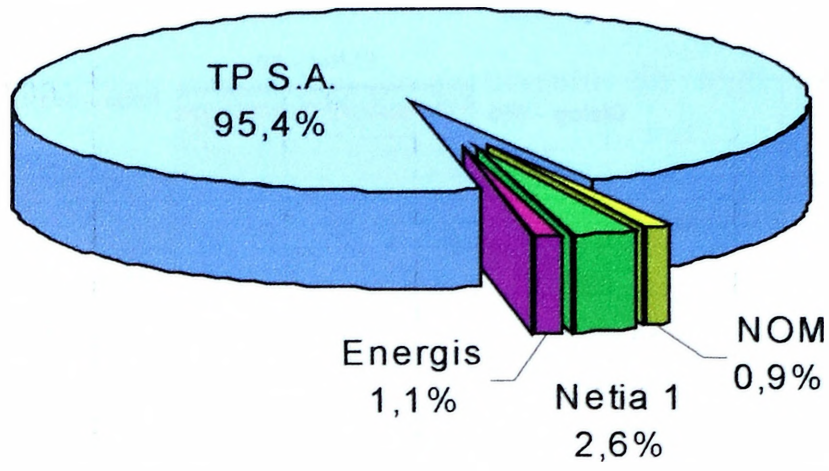
Ruch w mln minut	2001	2002
Połączenia lokalne	20 001	18 655
Połączenia do sieci operatorów komórkowych	1 941	1 836
Krajowe połączenia międzystrefowe	3 282	3 285
Połączenia międzynarodowe	429	381
Połączenia do Internetu (z numerem dostępowym 0202122 / 0202422)	6 028	7 432
Audioteks i usługi sieci inteligentnej	176	261
Ruch wychodzący ogółem	**31 857**	**31 850**

Źródło: *Analiza: Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 3.

Z dokonanej analizy rzeczowo-wartościowej istniejącego stanu infrastruktury telekomunikacji można stwierdzić, że w latach dziewięćdziesiątych międzynarodowe połączenia były obsługiwane w Polsce zaledwie przez dwie centrale znajdujące się tylko w Warszawie. W chwili obecnej funkcjonują centrale

Wykres 2.8.

Udział w rynku międzystrefowym (ruch telefoniczny) w 2002 r



Źródło: *Raport: Rozwój telekomunikacji - Infrastruktura – klucz do rozwoju, z realizacji programu: Strategia Gospodarcza Rządu - Przedsiębiorczość – Rozwój - Praca*, URM, Warszawa 2003, s. 3.

Analiza liczby łączy głównych posiadanych w latach 2000÷2002 przez największego operatora telekomunikacyjnego TP S.A. (Tabela 2.12., Wykres 2.9.) wskazuje na ich systematyczny wzrost, największy w odniesieniu do łączy ISDN.

Tabela 2.12. Liczba łączy głównych TP S.A. na dzień 31 grudnia 2001 i 2002 r.

Łącza główne(tys.)	**2001**	**2002**
POTS[150]	10 067	10 105
ISDN 2B+D	250	533
ISDN 30B+D	134	154
Razem (POTS +ISDN)	**10 450**	**10 792**

Źródło: *Analiza: Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 2.

Analiza wielkości i struktury ruchu wychodzącego z TP S.A. w latach 2001 – 2002 ogólnie utrzymuje się na tym samym poziomie, wyraźnie zwiększyły się połączenia z Internetem oraz audioteks i usługi sieci inteligentnej kosztem znacznego obniżenia liczby połączeń lokalnych i międzynarodowych (Tabela 2.13.).

---

[150]POTS (ang. - Plain Old Telephone Services) najstarsza podstawowa usługa telefoniczna, umożliwiająca analogowy przekaz głosu przez trwałe lub komutowane łącza telefoniczne.

realizującego połączenie międzystrefowe, a od 1 stycznia 2003 r. również połączenie międzynarodowe.

Liberalizacja rynku międzynarodowych usług telefonicznych nastąpiła od 1 stycznia 2003. Prezes URTiP wydał nieliczne decyzje o rozliczeniach na rzecz operatorów konkurencyjnych na połączenie międzystrefowe i międzynarodowe. Ogólnie można stwierdzić, że z powodu braku efektywnej regulacji umowy o połączeniu sieci z siecią TP S.A. podpisało niewielu operatorów międzystrefowych, jeszcze mniej te umowy wdrożyło, a dalsze umowy są negocjowane. Rzeczywiście umowy z TP S.A. podpisało z dniem 1.01.2003 r. zaledwie trzech operatorów zaangażowanych poważnie w działalność na rynku międzystrefowym, dopiero w dalszej kolejności inni operatorzy zaczęli podpisywać umowy z TP S.A. W URTiP-ie spoczywa nadal duża liczba wniosków o rozstrzygnięcie sporów międzyoperatorskich, jednak w drugiej połowie 2003 roku nastąpiło wyraźne przyspieszenie prac.

Pod koniec maja 2003 r. ponad 3,7 tyś. osób i firm czekało na instalację telefonu przez Telekomunikację Polską SA dłużej niż 10 lat. Potencjalni klienci oczekują na podłączenie niemal 370 tyś. linii. W przypadku blisko 107 tyś. linii oczekiwanie trwa dłużej niż przewidziane w ustawie *Prawo telekomunikacyjne* 18 miesięcy. W końcu 2002 r. czas oczekiwania na 7,7 tyś. telefonów był dłuższy niż 10 lat. Z danych na koniec ubiegłego roku wynika, że czekali głównie klienci indywidualni (326 tyś. linii, w tym 7,4 tyś. dłużej niż 10 lat) i głównie na wsi (220 tyś. łączy). W pierwszym półroczu do TP SA wpłynęło ok. 600 tyś. nowych wniosków o podłączenie telefonu[152].

Jeżeli chodzi o stosowaną technologię, to również pod tym względem polska telefonia przewodowa znacznie odbiega od przeciętnej europejskiej. W wielu regionach linie telefoniczne stosowane przez TP S.A. nadal są oparte na kablach miedzianych, a wiele central to centrale analogowe starego typu. Stan techniczny stosowanych urządzeń najlepiej przedstawia się w dużych aglomeracjach miejskich.

W ostatnim czasie TP S.A. kładzie bardzo duży nacisk na rozwój i modernizację swojej sieci obsługującej Połączenia Międzynarodowe

---

[152]Por. A. Streżyńska, *Raport o stanie i rozwoju sektora telekomunikacyjnego w Polsce za rok 2003,* w „Telekomunikacja 2004", MSG-Media Bydgoszcz 2003, s. 9.

cyfrowe w Poznaniu, Katowicach i w Warszawie, które umożliwiają dokonywanie połączeń z większością krajów na świecie. Polska sieć telekomunikacyjna jest powiązana z sieciami międzynarodowymi kilkunastoma liniami teletransmisyjnymi.

Międzynarodowa usługa telekomunikacyjna polega na tym, że przekaz informacji następuje do urządzenia telekomunikacyjnego, znajdującego się poza obszarem Polski. Tak więc zakaz nie obejmuje urządzeń znajdujących się na sztucznych satelitach Ziemi. Zakaz ustawowy nie oznacza, iż operator działający na podstawie koncesji i zezwolenia nie może uczestniczyć w zestawieniu połączenia wychodzącego z Polski, ale powinien on w takim przypadku korzystać z pośrednictwa operatora upoważnionego do dokonania takiej czynności.

Ustawa o łączności przewiduje możliwość wydania koncesji na świadczenie usług i budowę publicznych sieci międzymiastowych. Podmiotem, który pierwszy uzyskał ograniczoną koncesję na świadczenie usług międzymiastowych było m.in. Bankowe Przedsiębiorstwo Telekomunikacyjne „Telbank" S.A., które posiada koncesje na świadczenie usług telefonicznych międzymiastowych wyłącznie na rzecz swoich akcjonariuszy, banków oraz jednostek administracji państwowej.

Poza siecią międzymiastową, której właścicielem jest TP S.A., istnieją w Polsce jeszcze dwie sieci o zasięgu ogólnokrajowym:

- sieć należąca do Polskich Kolei Państwowych – Telekomunikacja Kolejowa S.A. – obecnie;
- nowoczesna sieć światłowodowa, którą zarządza Telekomunikacja Energetyczna Tel-Energo S.A. - spółka utworzona przez Polskie Sieci Energetyczne S.A..

W 1999 roku zezwolenie na zakładanie i używanie międzystrefowej ogólnopolskiej stacjonarnej sieci telekomunikacyjnej użytku publicznego przeznaczonej do świadczenia usług na terytorium RP uzyskała Netia. Zgodnie z rozporządzeniem Ministra Infrastruktury z dnia 5 września 2002 r. w sprawie planu numeracji krajowej dla publicznych sieci telefonicznych[151], posiadają oni numer dostępu do sieci, który jest kombinacją cyfr umożliwiającą wybór operatora

---

[151]Por. Rozporządzenie Ministra Infrastruktury z dnia 5 września 2002 roku w sprawie planu numeracji krajowej dla publicznych sieci telefonicznych w: „Dz. U. RP"2002, nr 145, poz. 1223.

telefonii komórkowej na początku XXI wieku uległ wyraźnemu przyśpieszeniu w porównaniu do końcowych lat XX wieku (Tabela 2.14., Wykres 2.10.)

Na koniec roku 2003 funkcjonowało 22 operatorów mających zezwolenia na eksploatację sieci komórkowej, z których 19 to tak zwani operatorzy wirtualnej sieci komórkowej i trzech największych niezależnych operatorów:

1. Polkomtel S.A. świadcząca usługi pod handlową nazwą Plus GSM 900 w standardzie GSM 900 oraz DCS 1800;
2. Polska Telefonia Cyfrowa Sp. z o.o. świadcząca usługi pod handlową nazwą Era GSM w standardzie GSM 900 oraz DCS 1800;
3. PTK-Centertel Sp. z o.o. świadcząca usługi w standardzie NMT 450, i pod handlową nazwą *Idea* oraz w standardzie GSM 900 i DCS 1800.

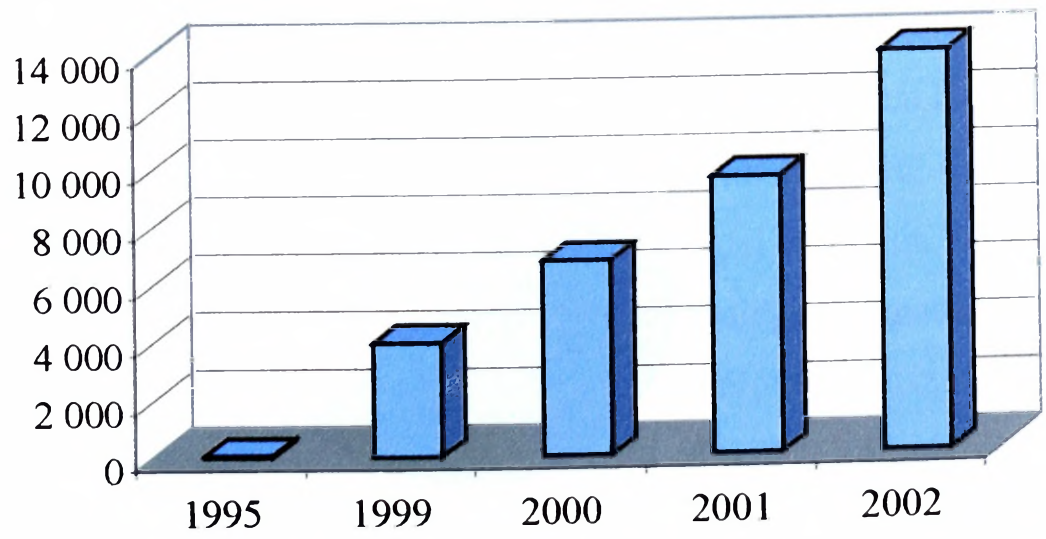
Tabela 2.14. Abonenci i użytkownicy telefonii komórkowej w latach 1995 – 2002

Abonenci i użytkownicy	**1995**	**1999**	**2000**	**2001**	**2002**
W liczbach bezwzględnych (w tys.)	**75,3**	**3.956,5**	**6.748,2**	**9.604,6**	**13.898,5**
Na 100 mieszkańców	**0,19**	**10,24**	**17,46**	**24,86**	**36,4**

Źródło: Analiza: *Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 5.

Wykres 2.10.

Abonenci i użytkownicy telefonii komórkowej w latach 1995 – 2002 (w tys.)



Źródło: Analiza: *Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 6.

i Międzymiastowe, a także sieci lokalnych w największych miastach. Dalszy rozwój technologii telekomunikacyjnej oraz rosnące zapotrzebowanie na urządzenia umożliwiające transmisję danych powodują, że operatorzy wchodzący na rynek telekomunikacyjny muszą opierać rozbudowę swojej sieci na urządzeniach najnowszej generacji, a TP S.A. będzie zmuszona do modernizacji już posiadanych urządzeń.

Wzrost zapotrzebowania na usługi telekomunikacyjne w Polsce będzie w najbliższych latach ściśle powiązany z rozwojem polskiej gospodarki, wzrostem polskiego PKB, wzrostem aktywności gospodarczej polskiego społeczeństwa, oraz napływem inwestorów zagranicznych szczególnie zainteresowanych wysokim standardem usług telekomunikacyjnych. Jak dotychczas osoby prowadzące działalność gospodarczą w Polsce miały ograniczoną możliwość korzystania z zaawansowanych usług telekomunikacyjnych, zwłaszcza z ogólnodostępnej w Europie Zachodniej możliwości transmisji danych. W ostatnich latach w Polsce nastąpił rozwój branży telekomunikacyjnej. W 1996 roku udział tego sektora w PKB wyniósł 2,5 proc., zaś w 2000 r. II wypracował już 4,4 proc. PKB[153]. Tempo rozwoju standardowej telefonii przewodowej nadal należy określać jako stagnację. Segmentami rynku, które nadal rozwijały się burzliwie, były telefonia komórkowa oraz dostęp do Internetu.

Na rynku telefonii komórkowej w latach 2001 - 2002 utrzymywały się tendencje do dynamicznego jego rozwoju. Według stanu na koniec 2001 r. liczba abonentów i użytkowników (usługi a przedpłatą – pre-paid) telefonii komórkowej wynosiła 9.604,6 tys. i była o 42,3% większa niż w końcu 2000 r. W końcu 2001 r. na 100 mieszkańców przypadało 24,9 abonentów. Liczba abonentów i użytkowników telefonii komórkowej powiększyła się w 2002 r. o ok. 4,29 mln osiągając w końcu roku poziom 13,9 mln., tj. o 44,6% większy niż przed rokiem. Na 100 mieszkańców przypadało 36,4 abonentów.

W innych krajach Europy wskaźnik ten w dniu 1 stycznia 2002 r. wyniósł: w Portugalii – 83,1, Wielkiej Brytanii – 75,5, Hiszpanii – 73,3, Holandii – 72,6, Czechach – 67,4, Niemczech – 64,9, Francji – 60,7, na Węgrzech – 48,6. Rozwój

---

[153] *ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce.*, Ministerstwo Infrastruktury, Warszawa 2002.

Z szacunków analityków wynika, że pod koniec 2002 r. liczba stacjonarnych linii telefonicznych wzrosła do 11 min 968 tyś., zaś liczba użytkowników telefonii komórkowej zwiększyła się do 13 min 890 tyś. Oznacza to, że liczba linii stacjonarnych wzrosła o 4,7 proc., a liczba użytkowników telefonii komórkowej zwiększyła się o 44,6 proc. w stosunku do danych URTiP i o 38,8 proc. w stosunku do danych operatorów. Dla porównania - w Czechach, gdzie trwa komórkowy boom, penetracja rynku zbliża się do 80 proc.

Na koniec I półrocza 2003 roku trzy działające w Polsce sieci komórkowe miały około 15,5 mln abonentów i użytkowników, co stanowiło znaczne zwiększenie ilości abonentów telefonii komórkowej w odniesieniu do 2002 roku (Tabela 2.15.). Liczba abonentów różnych operatorów w latach 2001-2002 uległa wyraźnemu wzrostowi (Wykres 2.13.).

Tabela 2.15. Abonenci i użytkownicy telefonii komórkowej (w tys.) w 2002 r.

Centertel		**Polkomtel**		**PTC**	
IDEA	**1 740**	**Plus GSM**	**2240**	**ERA**	**2 531**
POP	**2 728**	**Simplus**	**2310**	**TAK TAK**	**2 337**
NMT	**12**				
Razem	**4 480**		**4 550**		**4 868**
Ogółem	**13 898**				

Źródło: *Analiza: Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 6.

Na rynku telefonii komórkowej liderem jest Polska Telefonia Cyfrowa (PTC), która posiada około 5,6 min użytkowników. Idea w czerwcu br. miała około 5,08 min abonentów, a udział spółki w rynku telefonii komórkowej wzrósł do 32,6 proc. i drugiego miejsca na rynku. Tym samym Polkomtel z 4,9 min użytkowników jest trzecim co do liczby abonentów operatorem. Mniejsza dynamika przyrostu klientów to efekt wiosennej akcji dezaktywacji tzw. martwych dusz. Plus odłączył bowiem 300 tysięcy użytkowników usługi Simplus (usługi telefniczne prepaid[154]).

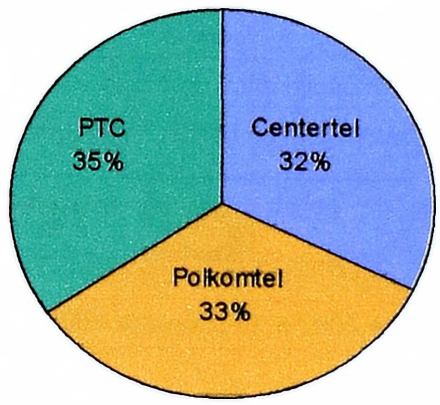
---

[154]Specjalna kredytowa karta telefoniczna do realizacji usługi - uzyskania połączenia telefonicznego przez podanie numeru karty i PIN.

Zezwolenie telekomunikacyjne uprawniające do świadczenia usług telekomunikacyjnych w sieciach ruchomych na terytorium RP (stan na I półrocze 2003 r.) posiadają operatorzy: POLKOMTEL S.A., Polska Telefonia Cyfrowa Sp. z o.o., Polska Telefonia Komórkowa CENTERTEL Sp. z o.o., którzy mogą świadczyć usługi w trzech standardach tj. ETSI/GSM w paśmie 900 MHz, GSM/DCS w paśmie1800 MHz, UMTS w paśmie 2 GHz, ponadto Polska Telefonia Komórkowa CENTERTEL Sp. z o.o. może świadczyć usługi w analogowym systemie NMT 450i oraz 19 operatorów MVNO (tzw. wirtualnych operatorów sieci ruchomej).Udział operatorów w rynku telefonii komórkowej w 2002 roku miał . charakter względnie zrównoważony (Wykres 2.11). Natomiast bardziej zróżnicowany był ich udział w rynku telefonii ogółem (Wykres 2.12.)

Wykres 2.11.

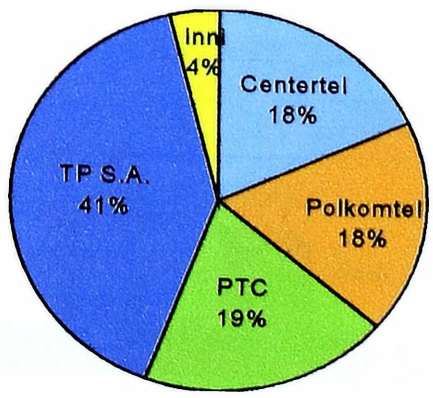
Udział w rynku telefonii komórkowej 2002 r



Źródło: *Analiza: Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 7.

Wykres 2.12.

Udział w rynku telefonii ogółem w 2002 r.



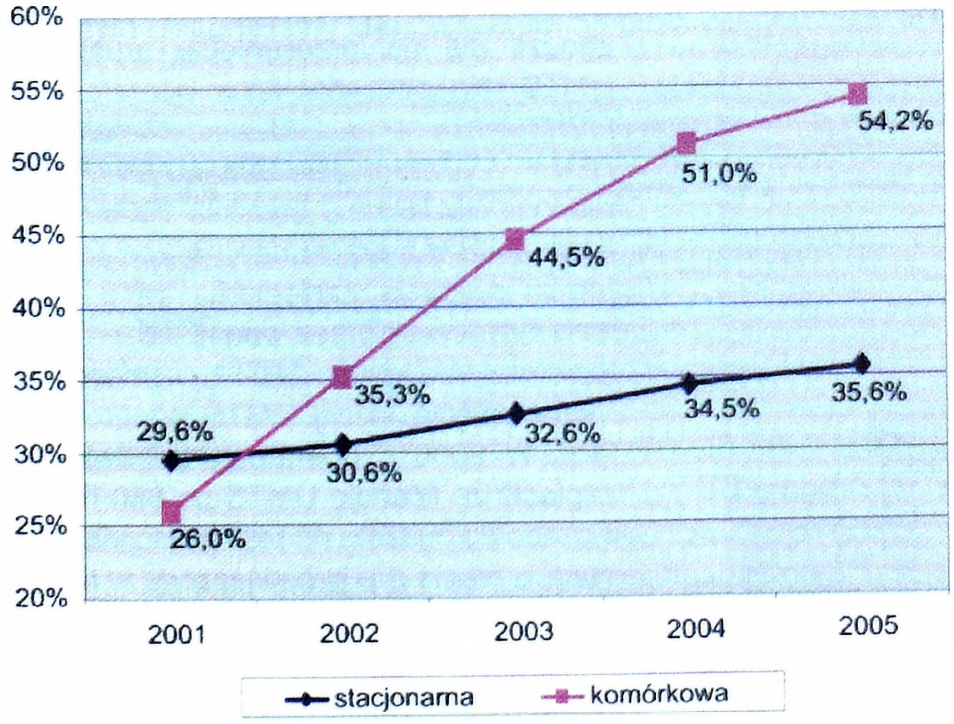
Źródło: *Analiza: Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 7.

Prognozowany rozwój telefonii komórkowej w stosunku do telefonii stacjonarnej dowodzi wyraźnego utrzymania jej tempa wzrostu (wykres 2.14.). Tymczasem jednak Urząd Regulacji Telekomunikacji i Poczty (URTiP) zamierza przesunąć o rok termin uruchomienia sieci 3G w Polsce. Już raz, w kwietniu 2002 r., URTiP zgodził się na przesunięcie uruchomienia UMTS.

Na początku lipca 2003 r. operatorzy sieci GSM - Era, Plus i Idea - zwrócili się do URTiP o przesunięcie terminu uruchomienia telefonii UMTS na 1 stycznia 2006 r. Operatorzy chcą też przesunąć na koniec 2007 r. termin pokrycia zasięgiem UMTS terenów zamieszkanych przez ponad 20 procent Polaków (obecnie koniec 2004 r.) i zniesienia wymogu objęcia siecią UMTS 40 procent populacji. W roku 2000 operatorzy zobowiązali się zapłacić za licencję UMTS po 650 min euro, z czego do budżetu od razu wpłacono 260 mln euro, a reszta ma być uiszczona w ratach do 2022 r.

Wykres 2.14.

Prognozy rozwoju telefonii komórkowej i stacjonarnej do 2005r.

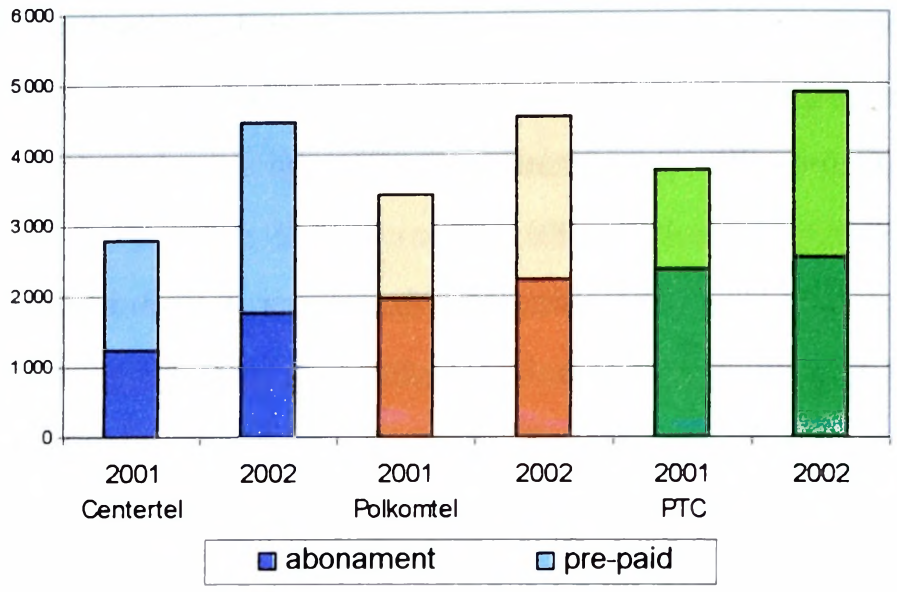


Źródło: A. Strężyńska, *Raport o stanie i rozwoju sektora telekomunikacyjnego w Polsce za rok 2003,* w: „*Telekomunikacja 2004*", MSG-Media Bydgoszcz 2003, s. 9.

Można przypuszczać, że prognozy mogą się potwierdzić ponieważ w pierwszym półroczu 2003 roku liczba abonentów i użytkowników telefonii komórkowej osiągnęła poziom 15,5 mln. i była o ok.11,3% większa niż w końcu

Wykres 2.13.

Abonenci i użytkownicy poszczególnych operatorów telefonii komórkowej w latach 2001-2002



Źródło: *Analiza: Stan telekomunikacji w 2002 r. i I półroczu 2003 r.*, Ministerstwo Infrastruktury, Warszawa 2003, s. 7.

Średni miesięczny przychód na abonenta Idei wyniósł w pierwszej połowie roku 68,8 zł (rok wcześniej - 73,1 zł). Zarząd Polkomtela prognozuje, że w 2004 roku przychody firmy przekroczą 5 mld zł. W 2002 roku, przy 4,8 mld zł przychodów, firma odnotowała 1,078 mld zysku operacyjnego i 515,8 min zł zysku netto. Największy wpływ na wzrost klientów telefonii komórkowych mają klienci usług typu pre-paid. Na koniec czerwca stanowili oni blisko 59 proc. łącznej liczby użytkowników w sieci Centertela i blisko 49 proc. osób korzystających z sieci PTC.

Firma doradcza Roland Berger prognozuje, że penetracja rynku GSM w Polsce wzrośnie z obecnych 40 do 75 proc. w ciągu najbliższych 5 lat. Według prognoz Gartner Data-group, udział sprzedaży telefonów z aparatami fotograficznymi sięgnie w 2006 r. aż 66 proc. Analitycy Rolanda Bergera prognozują, że w niedługim czasie telefonia komórkowa będzie zastępować stacjonarną. Mimo formalnego zniesienia monopolu TP S.A. spośród rynków związanych z dostarczaniem usług telekomunikacyjnych rynek telefonii przewodowej jest ciągle rynkiem, na którym stosunkowo najsłabiej rozwinęła się konkurencja. O ile można mówić o istnieniu konkurencji na poziomie telefonii lokalnej, o tyle na poziomie usług w telefonii międzymiastowej i międzynarodowej monopol TP S.A. jest nadal niewzruszony.

rozprowadzania lub rozpowszechniania programów radiofonicznych lub telewizyjnych.

Analiza ważniejszych danych statystycznych o łączności wskazuje, że na koniec roku 2002 w stosunku do roku 1995 nastąpił dynamiczny rozwój tego sektora we wszystkich płaszczyznach (tabela 2.17.).

Tabela 2.17. Ważniejsze dane zbiorcze o łączności stan w dniu 31.12.2002 r.

Wyszczególnienie	1995	2000	2001	2002
Telefoniczne łącza główne[155] w tys.	-	10947	11427	11744
W tym standardowe łącza główne (abonenci telefonii przewodowej)	5728	10740	10934	10916
W tym abonenci prywatni[156]	4720	8947	9122	9071
Miasta	4924	8182	8290	8162
Wieś	804	2558	2644	2754
Abonenci telefonii komórkowej w tys.	75	6748	9605	13898
Aparaty telefoniczne publiczne[157] samoinkasujące w tys.	36	98	95	93
Połączenia telefoniczne wychodzące w obrocie krajowym w mln	3281,7[158]	12239,6	12086,0	11591,4
Stacje telewizyjne nadawcze	135	249	258	260
Stacje retransmisyjne	248	253	248	243
Stacje satelitarne nadawczo – odbiorcze (naziemne):				
Stacje krajowe główne międzynarodowych systemów satelitarnych	7	7	7	7
Terminale VSAT[159]	73	3921	3756	4036

Źródło: Por. *Rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2003, s.367.

---

[155]Obejmują standardowe łącza główne oraz łącza w dostępach ISDN, tj. telefoniczną sieć cyfrową z integracją usług umożliwiającą wykorzystanie tej samej sieci do transmisji głosu, obrazu, faksów, danych.

[156]Posiadający aparaty telefoniczne zainstalowane w mieszkaniach prywatnych.

[157]Do 2000 r. określane jako ogólnodostępne.

[158]Tylko połączenia międzymiastowe.

[159]Łącznie ze stacjami PUNKT - PUNKT.

2002 r. oraz o 32,7% większa niż w końcu czerwca 2002 r. w trakcie I półrocza 2003 r. przybyło ponad 1,6 mln abonentów i użytkowników.

Przesyłanie głosu za pomocą Internetu ze względu na uwarunkowania technologiczne nie było dotychczas wykorzystywane w szerokim zakresie, jednakże wraz z następującą znaczną poprawą jakości transmisji, stanowi ono obecnie wręcz konkurencyjną alternatywę dla przekazu tradycyjnego. Dość intensywnie rozwija się dostęp do Internetu. Liczba internautów w Polsce, zgodnie z danymi SMG/KRC, wzrosła w 2002 roku o 44,4 proc. w porównaniu z rokiem poprzednim, czyli z 3,6 min do 5,2 min osób. Największą popularnością wśród internautów cieszą się takie portale, jak Onet.pl, który odwiedza 72,84 proc. internautów, Wirtualna Polska (58,57 proc.) oraz loteria (36,4 proc.). Wzrósł także procent osób korzystających z Internetu w domu (do 45,4 proc.), spadła zaś liczba korzystających w pracy (do 24,78 proc.) i - co musi budzić zaniepokojenie -w szkole (do 29,58 proc.).

Dokument e - Polska podaje zupełnie inne dane: według niego z Internetu w Polsce korzysta 7,6 mln osób. Polska podała także podczas badania krajów kandydackich, że zainstalowano na koniec 2002 roku 116 673 linie ADSL, najwięcej ze wszystkich krajów akcesyjnych. Następny kraj w kolejności to Węgry z 28 tysiącami linii.

Liczba operatorów, sieci telewizji kablowej (TVK) i gniazd abonenckich w latach 2000-2003 nieznacznie wzrosła (Tabela 2.16.). Tym samym osiągnęliśmy stan, w którym 55 proc. gospodarstw domowych posiada TVK.

Tabela 2.16. Liczba operatorów, sieci TVK i gniazd abonenckich w latach 2000-2003

Lata	Liczba operatorów	Liczba sieci TVK	Liczba gniazd
2000	534	1.113	3.539.273
2001	526	1.059	3.498.382
2002	507	1.063	3.529.448
2003	520	1.100	3.565.906

Źródło: A. Strężyńska, *Raport o stanie i rozwoju sektora telekomunikacyjnego w Polsce za rok 2003,* w: „*Telekomunikacja 2004*", MSG-Media Bydgoszcz 2003, s. 11.

W latach 2002÷2003 wydano także 5 nowych zezwoleń telekomunikacyjnych na eksploatację sieci publicznych przeznaczonych do

rozbudowy krajowych i międzynarodowych sieci telekomunikacyjnych, które są w znacznym stopniu interaktywne i połączone wzajemnie.

Krajowymi sieciami telekomunikacyjnymi i informatycznymi tworzącymi infrastrukturę telekomunikacyjną, a patrząc z punktu widzenia ich wpływu na kształtowanie bezpieczeństwa ekonomicznego państwa są:

- sieć łączności rządowej i wydzielone sieci teleinformatyczne administracji publicznej;
- radiowa sieć łączności ruchomej służb porządku publicznego i ratownictwa;
- resortowa sieć telefoniczna MSWiA;
- sieć teleinformatyczna MSWiA;
- sieć transmisji danych Policji POLWAN;
- sieć telekomunikacyjna Straży Granicznej;
- sieć alarmowania i ostrzegania OC;
- sieć organizacji pozarządowych.

Sieć łączności rządowej jest to sieć telefoniczna eksploatowana dla potrzeb Kancelarii Prezydenta, Kancelarii Sejmu, Kancelarii Senatu i administracji rządowej. Zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 4 lutego 2003 r. w sprawie szczegółowych warunków wykonywania działalności telekomunikacyjnej i używania urządzeń radiowych przez jednostki organizacyjne podległe i nadzorowane przez ministra właściwego do spraw wewnętrznych należy zapewnienie prawidłowego funkcjonowania i korzystania z sieci łączności rządowej, a szczególnie pod względem bezpieczeństwa i warunków przesyłania informacji niejawnych[160]. Decyzje uprawniające do korzystania oraz decyzje o pozbawieniu prawa do korzystania z sieci łączności rządowej podejmuje minister właściwy do spraw wewnętrznych.

Zadania ***jednostek administracji publicznej*** są realizowane przez wiele ***wydzielonych sieci teleinformatycznych*** typu Intranet[161]. Są to wirtualne sieci

---

[160]Dz. U. z dnia 28 lutego 2003 r.

[161]Współczesne rozwiązanie funkcji sieci Internetu działające w zakresie sieci lokalnej (LAN) i obejmującej swym zasięgiem ograniczony obszar – biuro, zakład, grupę przedsiębiorstw.

Ogólnie na podstawie danych statystycznych można stwierdzić, że telekomunikacja jest najbardziej dynamicznie rozwijającą się dziedziną gospodarki państwa i przynoszącą największe dochody. Świadczą o tym przychody ze sprzedaży wyrobów i usług łączności (Tabela 2.18.).

Tabela 2.18. Przychody ze sprzedaży wyrobów i usług łączności

Rok	Przychód (w mln PLN)
1995	**7 556 mln**
2000	**29 276 mln**
2001	**34 288 mln**
2002	**37 803 mln**

Źródło: *Rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2003, s. 366.

Jednak pomimo pięciokrotnego wzrostu przychodów w roku 2002 w stosunku do roku 1995 z telekomunikacji, nie najlepiej rysują się perspektywy dla operatorów telefonii stacjonarnej, lekarstwem na wszystkie problemy jedynie może okazać się rozszerzanie wachlarza usług w ramach swojej sieci, rozwój sieci cyfrowych z integracją usług (ISDN), a przede wszystkim partycypacja w telefonii ruchomej. Tak więc przetrwają tylko te podmioty, które najintensywniej będą oferować nowe usługi i produkty oparte na najnowszych technologiach, zwiększających ich użytecznoąć dla klienta.

Dziś praktycznie każdy większy operator telefonii stacjonarnej jest posiadaczem lub przynajmniej poważnym udziałowcem co najmniej jednej sieci komórkowej, świadczą także usługi w dziedzinie transmisji danych i usług z wartością dodaną (połączenie bezpłatne 0-800 oraz połączenia o podwyższonej opłacie 0700 (audiotekst).

2.1.3. Analiza rozmieszczenia infrastruktury telekomunikacyjnej

Zapewnieni określonych wymagań użytkowników infrastruktury telekomunikacyjnej w czasie pokoju, na zwiększone zapotrzebowanie na połączenia krajowe i międzynarodowe, możliwe jest dzięki postępowi technologicznemu - głównie przez rozwój cyfrowych systemów transmisyjnych, komutacyjnych, i sygnalizacji a także za pomocą technik zarządzania. Rozwój ten doprowadził do

systemy te nie posiadają możliwości automatycznej obsługi wywołań alarmowych i przekazywania danych o lokalizacji.

Ponieważ w latach dziewięćdziesiątych został wyłączony system łączności radiowej w paśmie 160 MHz, który tworzył zapasowy ogólnokrajowy system łączności dla jednostek administracji publicznej, i obsługiwany był przez Telekomunikacje Polską S.A., gdzie w każdym urzędzie do poziomu gminy były zainstalowane radiotelefony, to planowane jest zastąpienie radiowych systemów analogowych przez system TETRA.

Resortowa sieć telefoniczna MSWiA, nazywana siecią zintegrowaną, składa się z węzłów łączności zlokalizowanych w miastach będących siedzibą władz dawnych województw. Sieć posiada punkty styku z publiczną siecią telefoniczną PSTN/ISDN. Centrale tej sieci zlokalizowane są w węzłach łączności MSWiA. Organizację utrzymania sieci określa rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 4 lutego 2003 r. w sprawie szczegółowych warunków wykonywania działalności telekomunikacyjnej i używania urządzeń radiowych przez jednostki organizacyjne podległe i nadzorowane przez ministra właściwego do spraw wewnętrznych[164]. Sieć wykorzystywana jest wspólnie przez jednostki organizacyjne podległe lub nadzorowane przez ministra właściwego do spraw wewnętrznych.

Zadania w zakresie organizacji i eksploatacji sieci telekomunikacyjnej zintegrowanej oraz koordynacji zadań eksploatatorów wykonuje koordynator sieci telekomunikacyjnej zintegrowanej. Koordynatorem sieci telekomunikacyjnej zintegrowanej jest Komendant Główny Policji.

Do zadań koordynatora sieci telekomunikacyjnej zintegrowanej należy:

- eksploatacja zintegrowanej sieci telekomunikacyjnej;
- obsługa urzędu obsługującego właściwego ministra spraw wewnętrznych w zakresie telekomunikacji;
- sporządzanie i aktualizowanie, wykazu infrastruktury wchodzącej w skład zintegrowanej sieci telekomunikacyjnej;
- podejmowanie działań w celu obniżania kosztów działalności

---

[164]Dz. U. Nr 24, poz. 159 z dnia 28 lutego 2003 r.

teleinformatyczne[162] budowane w oparciu o usługi operatorów komercyjnych, głownie TP S.A. Swoim zasięgiem obejmują jednostki administracji publicznej do poziomu powiatu, a użytkownicy różnych sieci znajdują się nieraz w tym samym budynku lub najbliższej okolicy. Sieci te utworzone zostały przez następujące jednostki: Ministerstwo Finansów, Główny Urząd Statystyczny, Wytwórnię Papierów Wartościowych, Agencja Modernizacji i Rozwoju Rynku Rolnego, Zakład Ubezpieczeń Społecznych, Ministerstwo Finansów oraz Urząd Regulacji Poczty i Telekomunikacji. Potrzeba utworzenia wydzielonej bezpiecznej infrastruktury teleinformatycznej dla instytucji administracji publicznej wynika z zapewnienia bezpieczeństwa obiegu informacji oraz m.in. z zagrożeń np. przestępczością komputerową, aktami wandalizmu i cyberterroryzmem.

Radiowe systemy łączności ruchomej są podstawowym narzędziem dla ***służb porządku publicznego i ratownictwa.*** Obecnie w kraju funkcjonuje ponad 2000 sieci dyspozytorskich analogowych systemów łączności ruchomej.

Od początku lat dziewięćdziesiątych w Warszawie i Krakowie eksploatowany jest przez Policję cyfrowy system ruchomej łączności radiowej firmy Ericsson pod nazwą EDAX. Są ta zamknięte regionalne systemy łączności radiowej składające się ze stacji bazowych pracujących w przyznanych częstotliwościach wykorzystywane przez dane służby. Natomiast w Warszawie, Łodzi, Krakowie i Szczecinie uruchomiono w jednostkach Policji pilotażowe instalacje systemu łączności TETRA[163] współpracujące z Systemem Wspomagania Dowodzenia (SWD). System zapewnia połączenia głosowe i transmisji danych dla potrzeb zdalnego dostępu do baz danych Policji oraz przekazywania lokalizacji radiowozów do stanowiska dowodzenia.

Używane powszechnie przez służby systemy ruchomej łączności radiowej pracują w niechronionych kanałach radiowych i narażone są na podsłuch. Organizacja systemu łączności wynika z przydziału kanałów radiowych dla poszczególnych służb, co utrudnia łączność współdziałania między nimi. Z reguły

---

[162]Dowolna topologia sieci fizycznej wybrana i przeznaczona do tworzenia do tworzenia struktury sieciowej ATM przez organizację wirtualnych połączeń logicznych, charakterystycznych dla tej technologii.
[163]TETRA – standard systemu trankingowego umożliwiający usługę telefoniczną jak i teledacyjną.

w sąsiedztwie większości urzędów. Dzięki temu kablowe łącza dostępowe są krótkie, nie przekraczając zazwyczaj od kilkuset metrów do kilku kilometrów. Możliwe jest, więc stworzenie na poziomie lokalnym sieci dostępowej o dużej przepustowości. Sieć transmisyjna TP S.A. pozwala na dalszy rozwój sieci PESEL-NET przez zastosowanie kanałów cyfrowych o większej przepustowości oraz zapewnienie dostępu nawet na poziomie poszczególnych gmin.

Sieć transmisji danych Policji POLWAN jest budowana w oparciu o łącza cyfrowe o przepływności 2 Mb/s (protokół Frame Relay[166]) pomiędzy komendami wojewódzkimi Komendą Główną Policji. Tworzy szyfrowaną cyfrową Policyjną Sieć Transmisji Danych (PSTD)[167], łączącą 17 węzłów wojewódzkich PSTD z węzłem centralnym zlokalizowanym w KGP udostępniającą użytkownikom z komend powiatowych (miejskich) policji i komisariatów centralne bazy danych (m.in. POSIGRAF, Krajowy System Informacyjny Policji KSIP).

Sieć teleinformatyczna Policji POLWAN budowana jest do poziomu Komend Powiatowych Policji. Jest budowana w oparciu o kanały cyfrowe 2Mbit/s dzierżawione od różnych operatorów telekomunikacyjnych. Z kanałów cyfrowych 2Mbit/s mogą być wydzielane kanały o przepływności n x 64 kbit/s. Do podłączania pozostałych jednostek, będą stosowane dzierżawione kanały cyfrowe n x 64Kbit/s.

Sieć telekomunikacyjna Straży Granicznej oprócz ruchomej sieci łączności radiowej obejmuje sieć telekomunikacyjną, której podstawą jest sieć z komutacją pakietów POLPAK z protokołem Frame Relay. Sieć zapewnia połączenia informatyczne i telefoniczne w ramach struktury organizacyjnej SG. Transmisje telefoniczne realizowane są w sieci transmisji danych w technologii VoIP[168]. Usługa jest świadczona w formie outsourcingu[169].

---

[166]Protokoł Frame Relay jest stosowany w technologii sieci rozległych - protokół transportowy w trybie pakietowym – podobnie jak protokoł X.25 tylko, że wykorzystuje prostszy mechanizm korekcji błędów i wykrywa błędy nagłówka, formatu oraz cyklicznego kodu nadmiarowego.

[167]*Internet w Policji,* TELEINFO nr 40/2000, 2 października 2000 r.

[168]Przekaz głosu w pakietach (ang. VoIP – Voice over Internet Protocol). Jest to aplikacja telefonii komputerowej, która pozwala na przekazywanie głosu przez sieci pakietowe jako dane cyfrowe.

[169]Outsourcing telekomunikacyjny jest metodą prowadzenia biznesu z wykorzystaniem technologii implementowanych w systemach usługowych contact center (telecentra informacyjne). Polega on na dostarczaniu klientom poszukiwanych funkcji sieciowych i przetwarzaniu informacji wraz z gwarancją odpowiednich parametrów transmisji i niezawodności działania na podstawie zawartej odrębnej umowy.

telekomunikacyjnej;

- opiniowanie programów i koncepcji rozwoju systemów telekomunikacyjnych sporządzanych przez eksploatatorów;
- monitorowanie wykorzystania sieci telekomunikacyjnej zintegrowanej, przygotowywanie corocznych informacji właściwemu ministrowi spraw wewnętrznych w tym zakresie wraz z oceną działań inwestycyjnych;
- ewidencjonowanie eksploatowanych zintegrowanych sieci i infrastruktury telekomunikacyjnej.

Sieć teleinformatyczna MSWiA (sieć PESEL-NET) powstała w 1996 roku w wyniku modernizacji sieci analogowych łączy dzierżawionych zbudowanej specjalnie dla użytkowników systemu CBD PESEL. Początkowy obszar działania sieci PESEL-NET ograniczony był do użytkowników korzystających wcześniej z zasobów Centralnej Bazy Danych PESEL. Sieć realizowała dostęp z terminali lub stacji roboczych użytkowników do systemów centralnych.

Sieć PESEL-NET była projektowana dla potrzeb eksploatacji centralnych systemów informatycznych przez użytkowników zlokalizowanych na terenie dawnych miast wojewódzkich, pracujących w trybie transakcyjnym i małymi wymaganiami na przepustowość. Dobór sprzętu komutacyjnego oraz przepustowość łączy zostały zwymiarowane zgodnie występującymi w tym czasie potrzebami. Sieć PESEL-NET obejmuje obszar całego kraju funkcjonując na kanałach cyfrowych dzierżawionych od TP S.A.. Realizuje usługi transmisji danych z komutacją pakietów. Węzły sieci funkcjonują głównie w miastach będących siedzibami dawnych województw oraz niektórych powiatów. Można w niej tworzyć tzw. sieci wirtualne prywatne (VPN)[165]. Obecnie sieć wykorzystywana jest także dla potrzeb centralnych systemów informatycznych. Użytkownikami są głównie instytucje zlokalizowane w miastach -siedzibach dawnych województw.

Zaletą jest to, że obiekty, w których zainstalowane są węzły sieci, połączone są siecią kablową i znajdują się zwykle w centrum miasta lub miejscowości

---

[165]Wirtualna sieć prywatna (ang. VPN – Virtual Private Network) – pojęcie to do sieci logicznej funkcjonującej zwykle w publicznej rozległej sieci fizycznej. Sieć ta działa w sposób zbliżony do rzeczywistej sieci prywatnej, zapewniając jednak redukcję kosztów związanych z dzierżawą łączy.

Systemy alarmowania i ostrzegania Obrony Cywilnej są jednym z elementów systemu telekomunikacyjnego dla potrzeb bezpieczeństwa państwa. Organizacja systemów alarmowych jest jednym z przedsięwzięć obrony cywilnej, które mają ostrzegać ludność przed grożącym niebezpieczeństwem napadu z powietrza oraz skażeniem promieniotwórczym i chemicznym, a także o klęskach żywiołowych i zagrożeniu środowiska w celu umożliwienia jej odpowiedniego zareagowania. Do ogłaszania i odwoływania alarmów wykorzystuje się:

- syreny wchodzące w skład centralnych systemów alarmowych miast sterowane radiowo i przewodowo;
- rozgłośnie radiowe i ośrodki telewizyjne;
- autonomiczne systemy alarmowe: syreny nie włączone do miejskich systemów alarmowych (zakładów pracy, ochotniczych straży pożarnych);
- zastępcze środki alarmowania: syreny ręczne, gongi, pojazdy z urządzeniami nagłaśniającymi.

Systemy alarmowania zapewniają zaalarmowanie ok. 60% ludności w czasie do 1 minuty zamieszkałej w mieście i 5-7 minut zamieszkałej na terenach wiejskich. Do roku 1992 funkcjonował scentralizowany system alarmowania oparty na sieci telekomunikacyjnej będącej obecnie w posiadaniu Telekomunikacji Polskiej S.A. System ten obejmował 520 miast z liczbą ludności przekraczającą 10 tysięcy. Podstawowe elementy scentralizowanych systemów obejmowały:

- nadajnik dyspozytora;
- centralka alarmowa typu AM4 lub AM5;
- telefoniczne łącza sterujące- ogółem 20 tys. km;
- urządzenia włączające;
- silnik trójfazowy;
- syrena powietrzna.

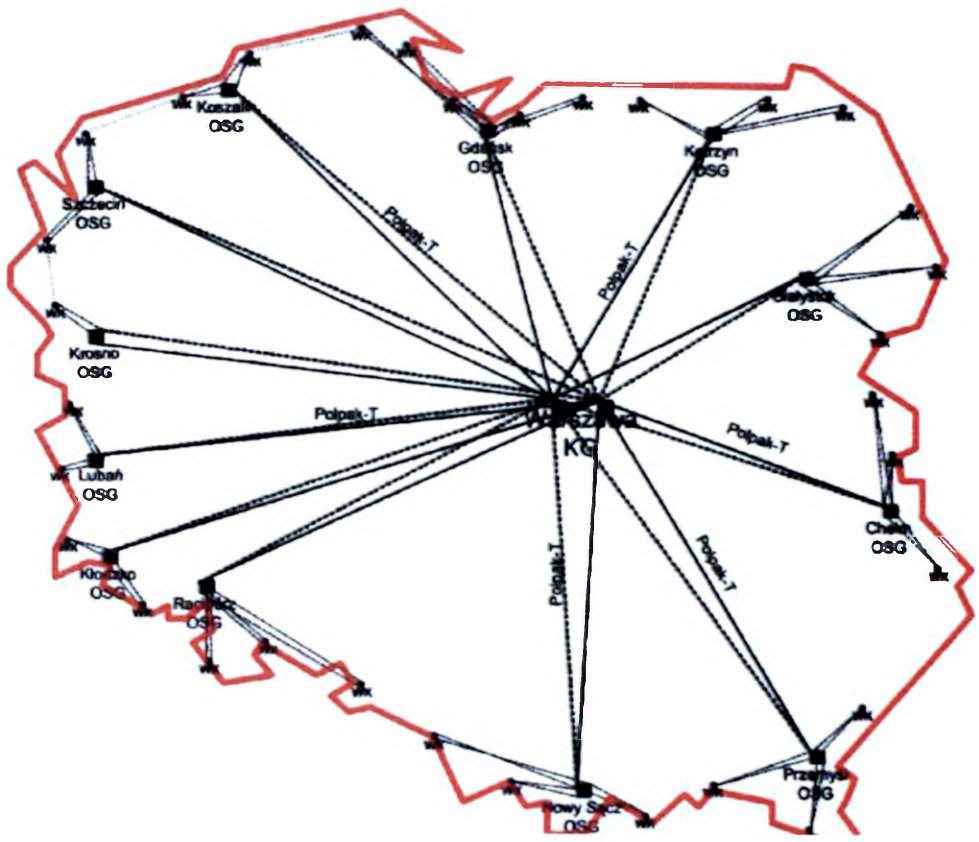
System ten był budowany w latach 50 i 60 w oparciu o istniejące analogowe systemy teletransmisyjne. Wadą tego systemu była konieczność utrzymywania dużej liczby łączy oraz dużej liczby operatorów systemu. W latach 1989-1992 łącza w większości miast zostały rozłączone, pozostawiono tylko dla zakładów stanowiących zagrożenia dla ludzi i środowiska. Na wypadek nadzwyczajnych

Sieć obejmuje następujące jednostki[170]:

- Komendą Główną Straży Granicznej - 2 lokalizacje;
- oddziały Straży Granicznej - 12 lokalizacji;
- placówki graniczne - 268 lokalizacji.

Architektura sieci dostosowana jest do struktury organizacyjnej Straży Granicznej. Współpraca z innymi sieciami w tym telefoniczną siecią resortową MSWiA odbywa się przez punkty styku w Warszawie (Mapa 2.4.).

Mapa 2.4. Sieć telekomunikacyjna transmisji danych
na potrzeby Straży Garnicznej



Źródło: Materiały prezentacyjne firmy NextiraOne, www.nextira.pl

Niniejsze rozwiązanie jest przykładem integracji usług w oparciu o sieć z komutacją pakietów i odpowiada obecnym trendom rozwojowym. Natomiast rozwiązanie to pokazuje, niekorzystne zjawisko wyodrębnienia sieci łączności dla jednej służby porządku publicznego, która to wymaga współdziałania z innymi służbami. Jest to przykład braku koordynacji w ramach resortu spraw wewnętrznych.

---

[170]W. Garbacz, *Projekt ogólnopolskiej sieci IP na przykładzie Straży Granicznej*, Prezentacja NextiraOne, www.nextiraone.pl.

narady i konferencje na, których są omawiane różne formy działalności organizacji przydatne dla wsparcia obronności będące przedmiotem działań Ligi Obrony Kraju, Związku Harcerstwa Polskiego, Polskiego Czerwonego Krzyża, Polskiego Związku Krótkofalowców. Uzgodniono wymianę doświadczeń i informacji na temat udziału organizacji pozarządowych w przedsięwzięciach związanych z obroną terytorialną Polski[174].

Nowym aspektem aktywności proobronnej jest tworzenie sieci wczesnego ostrzegania o zagrożeniach takich jak pożary, powodzie, karambole na drogach czy zagrożenie atakami terrorystycznymi. Została przyjęta propozycja współpracy w tworzeniu równoległej do państwowej sieci łączności na wypadek zagrożeń i katastrof. Sieć ta jest w trakcie tworzenia na bazie lokalnych porozumień pomiędzy sztabami zarządzania kryzysowego, a oddziałami i klubami Polskiego Związku Krótkofalowców.

Na uwagę zasługuje zniesienie obowiązku posiadania pozwolenia radiowego na używanie urządzeń nadawczych lub nadawczo-odbiorczych Radia Obywatelskiego w związku z wejściem w życie rozporządzenia Ministra Infrastruktury z dnia 26 lipca 2004 r. zmieniającego rozporządzenie w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, co może przyczynić się do rozwoju sieci obywatelskich.

W sytuacji kryzysowej istnieje potrzeba połączeń telekomunikacyjnych pomiędzy władzami rządowymi, wojskowymi i cywilnymi oraz innymi ważnymi użytkownikami z pomocą sieci telekomunikacyjnej, takiej jak publiczna sieć komutowana. Połączenia w sieci telekomunikacyjnej są i powinny być traktowane jako podstawowe, zapewniające zwiększoną ilość połączeń, gdy usługi publiczne telekomunikacyjne mogą zostać ograniczone ze względu na uszkodzenia, zatory lub usterki.

Staje się więc koniecznością zaplanowanie adaptacyjnej i elastycznej struktury sieci teleinformatycznej na potrzeby zaistniałych sytuacji podczas realizacji zadań w stanach nadzwyczajnych, aby ograniczyć skutki możliwych uszkodzeń wynikające z występujących zagrożeń do minimalnego poziomu. Jeżeli

---

[174]Zob. Świat Radio, maj 2004 s., 45-46.

zagrożeń TP S.A. opracowała instrukcję przyłączeniową w celu możliwości ponownego zestawienia łączy w czasie 6 do 12 godzin.

Cyfryzacja sieci telekomunikacyjnej spowodowała trudności w eksploatacji sieci telegraficznej, która były podstawą funkcjonowania sieci alarmowania. W 2002 roku TP S.A. wyłączyła sieć teleksową, a wraz z nią sieć teletransmisji telegraficznej. TP S.A, której jednym z udziałowców jest France Telecom, kieruje się osiągnięciem zysku i nie wykazuje zainteresowania utrzymywaniem systemów związanych z bezpieczeństwem narodowym. Przykładem jest sieć radiotelefoniczna 160 MHz i morskie stacje brzegowe. Wobec powyższego stanu wdrożono w latach 1992- 96 system alarmowy ze sterowaniem radiowym[171].

Obecnie eksploatowane przez Państwową Straż Pożarną są systemy kilku producentów[172]. Radiowy System Włączania Syren RSWS-2000[173] jest dedykowanym systemem tylko do sterowania syrenami alarmowymi przeznaczonym dla:

- obrony cywilnej;
- straży pożarnej;
- zakładów przemysłowych;
- zbiorników wodnych.

System ma budowę hierarchiczną i obejmuje: centralę wojewódzką, centrale lokalne i urządzenie włączające syrenę. Realizuje on tylko funkcje sterowania. Przesyłanie krótkich wiadomości tekstowych nie jest możliwe.

Sieci organizacji pozarządowych w czasie zaniedbanej infrastruktury telekomunikacyjnej stanowiły jedyny środek łączności będący w dyspozycji obywateli. Do lat dziewięćdziesiątych organizacje np. LOK, ZHP i PZK miały wyznaczone zadania obronne, były dotowane i wyposażane w demobilowy sprzęt łączności. W dobie Internetu i dostępności telefonów komórkowych spowodowany został spadek zainteresowania społeczeństwa krótkofalarstwem.

Ostatnio podejmowane są próby reaktywowania organizacji pozarządowych w działaniach na rzecz bezpieczeństwa państwa. Zostają przeprowadzane spotkania,

---

[171]Por. W. Michalak, *Ostrzeganie i alarmowanie ludności*, AON, Warszawa 1998, s., 5.
[172]Zob. www.platan.pl.
[173]Zob. Świat Radio, 01/2004, s., 21.

wiele technik sterowania siecią w sposób automatyczny lub ręczny. Techniki sterowania mogą być zastosowane do zarządzania ruchem różnego typu lub nawet poszczególnymi połączeniami tego samego typu w zależności od miejsca do którego są kierowane i prawdopodobieństwa prawidłowego zestawienia połączenia.

Techniki sterowania mogą być ekspansywne lub restrykcyjne w zależności od zastosowanej metody sterowania, miejsca wykorzystania i wybranego do sterowania parametru ruchu. Przykładem sterowania ekspansywnego może być zabezpieczenie większej liczby dróg obejściowych na potrzeby najważniejszych połączeń. Przykładem sterowania restrykcyjnego może być odciążenie sprzętu komutacyjnego poprzez ograniczenie komutowanego ruchu.

Dotychczasowe doświadczenia wskazują, że w czasie kryzysu wzrasta zapotrzebowanie na usługi i obsługę zwiększonego ruchu w publicznej sieci komutowanej. Jeżeli nie są zastosowane techniki zarządzania siecią, wówczas liczba niezrealizowanych połączeń może być mniejsza można zastosować następujące techniki sterowania:

- wyłączenie najważniejszych połączeń spod kontroli technik zarządzania siecią w taki sposób, że połączenia te będą zestawione w czasie kryzysów;
- zastosowanie specjalnych technik zarządzania siecią, które zapewniają obsługę oznakowanych połączeń i specjalne przywileje w rodzaju uprzywilejowanego dostępu do sieci;
- zarządzanie ruchem w łączach w celu kontrolowania liczby połączeń wychodzących lub przychodzących;
- eliminowanie użytkowników nieuprawnionych, stacji abonenckich i łączy poprzez blokowanie prób uzyskania połączenia z numerami kierunkowymi kraju, strefowymi i numerami określonych central (tj. blokowanie numerów);
- rekonfigurację sieci w celu przekierowania połączeń poprzez inne węzły komutacyjne w kraju lub poprzez kraj tranzytowy;
- zapewnienie abonentom specjalnym dodatkowych usług lub łączy na wypadek sytuacji szczególnych zagrożeń.

nie zostaną podjęte natychmiastowe działania w celu kontrolowania i usuwania skutków zagrożeń, przeciążenie lub natłok może rozprzestrzenić się i zakłócić funkcjonowanie systemu telekomunikacyjnego w krajowych lub międzynarodowych częściach sieci teleinformatycznej. Degradacja ruchu telefonicznego spowoduje wzrost liczby niezrealizowanych połączeń.

W czasie szczególnych zagrożeń, sytuacji kryzysowych i wojny, publiczne sieci telekomunikacyjne muszą sprostać gwałtownym zmianom natężenia ruchu i zwiększonym potrzebom komunikacyjnym w zakresie wsparcia działań sojuszu. W czasie wojny, nawet po usunięciu skutków rozległych awarii, uwarunkowania na terenie kraju mogą być bardzo różne tak, że na niektórych obszarach nie ma wcale łączności, podczas gdy na innych łączność funkcjonuje normalnie. W takich okolicznościach działania cywilnej administracji łączności polegają zasadniczo na zapewnieniu ciągłości świadczenia najważniejszych usług telekomunikacyjnych, zarówno krajowych, jak i międzynarodowych we współpracy, o ile jest to konieczne, z innymi administracjami. W sieci może wystąpić przeciążenie i natłok z powodu wielu przyczyn, na przykład:

- uszkodzeń i awarii elementów sieci;
- uwarunkowań zewnętrznych, które powodują natłok w sieci (np. klęski żywiołowe i lub inne sytuacje kryzysowe);
- natłoku w sieciach wzajemnie połączonych.

W celu zapewnienia maksymalnego wykorzystania usług świadczonych przez tą sieć we wszystkich sytuacjach organizuje się zarządzanie siecią, czyli zbiór działań jakie są potrzebne do monitorowania stanu i sterowania wszystkimi elementami sieci. O ile nie zostaną podjęte natychmiastowe działania w celu kontrolowania, skutków takich wydarzeń, przeciążenie lub natłok może rozprzestrzenić się i spowodować degradację ruchu telekomunikacyjnego w innych częściach sieci krajowych lub międzynarodowych. Działania z zakresu zarządzania siecią są ciągle rozwijane pod kątem ograniczenia skutków tych wydarzeń.

Techniki zarządzania siecią zapewniają sposoby przekierowania ruchu w sieciach, a sposób ich wykorzystania powinien uwzględniać parametry jakościowe sieci, które określają jakie działania są potrzebne. Współczesne systemy telekomunikacyjne są zaprojektowane w taki sposób, że wykorzystywanych jest

zagwarantowany ciągły dostęp do publicznych sieci komutowanych dzięki właściwym porozumieniom z operatorami telekomunikacyjnymi.

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

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

2.2. Analiza i ocena bezpieczeństwa ekonomicznego Polski na przełomie wieku

2.2.1. Analiza uwarunkowań bezpieczeństwa ekonomicznego Polski

Na kształtowanie bezpieczeństwa ekonomicznego Polski mają istotny wpływ uwarunkowania zewnętrzne i wewnętrzne. Obecna sytuacja międzynarodowa, obejmująca zewnętrzne bliższe i dalsze otoczenie Polski jest istotnym czynnikiem oddziaływującym pośrednio i bezpośrednio na stan bezpieczeństwa naszego kraju.

W takich warunkach istnieją i mogą pojawić się źródła i zagrożenia, również dla bezpieczeństwa ekonomicznego kraju. Relacje z otoczeniem międzynarodowym, mogą niejednokrotnie stwarzać sytuacje, wymagające podejmowania decyzji strategicznych w celu koniecznego dostosowania się do zaistniałych warunków międzynarodowych. Można wyróżnić różne formy dostosowania, w tym takie jak:

- sprostanie nowym wymaganiom;
- wykorzystanie szans stwarzanych przez okoliczności i partnerów;

Techniki zarządzania i sterowania siecią przynoszą operatorom korzyści handlowe w czasie pokoju, ale podczas wojny i w sytuacjach kryzysowych będą miały zasadnicze znaczenie dla zachowania ciągłości świadczenia usług telekomunikacyjnych. z powodu takiego znaczenia należy wymagać od operatorów sieci publicznych, aby ich Centra Zarządzania Siecią NMC (ang. – Network Management Centre) były czynne bez przerwy i pożądane jest umiejscowienie ich w chronionych obiektach oddalonych od potencjalnych obszarów ataków. Łącza pomiędzy NMC i węzłami sieci powinny być uodpornione, bardzo niezawodne i zdublowane, o ile jest to możliwe lub powinna istnieć możliwość przejęcia ich funkcji lokalnie albo na poziomie regionalnym lub też w Centrach Komutacji. Dla zapewnienia możliwości zarządzania kryzysowego w sytuacji degradacji ruchu telekomunikacyjnego konieczne jest opracowanie i wdrożenie narodowego programu uprzywilejowanego dostępu do sieci.

Wnioski z ćwiczeń wskazują, że w czasie kryzysu zapotrzebowanie klientów na publiczne usługi komutowane wzrośnie. Powinny zostać wprowadzone funkcje sterowania w obrębie zarządzania siecią, to wtedy liczba zrealizowanych połączeń będzie niższa niż normalnie. Zarządzanie ma na celu zapewnienie maksymalnego wykorzystania usług świadczonych w sieci, w każdej sytuacji. W sytuacjach, kiedy zastosowanie technik zarządzania siecią nie jest możliwe, należy zastosować metody blokowania prób uzyskania połączenia poprzez przeciążone węzły komutacyjne. Zablokowanie możliwości uzyskania połączenia przez grupę abonentów i zapewnienie dostępu abonentom specjalnym może być jedynym rozwiązaniem skutecznym.

Należy wymagać od operatorów telekomunikacyjnych planowania i przygotowania odpowiednich środków na potrzeby restrykcyjnego korzystania z publicznych sieci komutowanych w sytuacjach rozległych katastrof w czasie pokoju oraz w sytuacjach kryzysowych i podczas wojny. Działania te powinny być realizowane pod nadzorem administracji państwa, która może zażądać od operatorów telekomunikacyjnych ograniczenia świadczenia usług i przekazania łączy na potrzeby obronności kraju. Istotne jest, aby abonenci specjalni pełniący ważne funkcje na rzecz prawidłowego funkcjonowania państwa mieli

w tym zapewne widzi swoją szansę realnego współdziałania z USA i będzie się starała szeroko ją wykorzystywać dla odbudowywania regionalnie samodzielnej i mocarstwowej pozycji.

W Azji Środkowej i Wschodniej dominującą pozycje zajmują Chiny i Japonia. Zawarte sojusze i rozlokowanie sił zbrojnych USA w tym regionie zapewniają stabilność. Bardzo ważny jest sojusz USA z Japonią. Chiny rozporządzają stale zwiększającym się zapleczem politycznym, ekonomicznym i wojskowym. Mogą więc w przyszłości samodzielnie oddziaływać na sytuację międzynarodową, przynajmniej w skali kontynentu. Państwo to jest też stałym członkiem Rady Bezpieczeństwa ONZ i uczestniczy w rozstrzyganiu problemów o znaczeniu globalnym. Stąd też od współdziałania Chin z innymi mocarstwami w dużym stopniu zależy utrzymanie ładu międzynarodowego i rozwiązywanie globalnych problemów ludzkości[177].

Szybki rozwój ekonomiczny Japonii prowadzi do uznania jej za supermocarstwo gospodarcze. Japonia jest również wielką potęgą finansową i pierwszym kredytodawcą na świecie. Daje to jej drugie miejsce po Stanach Zjednoczonych. Jedną z cech polityki Japonii od dłuższego już czasu jest dążenie do odgrywania większej niż dotychczas roli w stosunkach międzynarodowych „na miarę swojej potęgi ekonomicznej"[178], m.in. poprzez zwiększenie pomocy krajom regionu i rozwijającym się.

Dla Europy - a zwłaszcza dla Polski - wielkim wyzwaniem jest problem zjednoczonych Niemiec. Niemcy dominując pod względem ekonomicznym, z czasem osiągają przewagę militarną. Struktura NATO bez militarnego zaangażowania USA traci swoje znaczenie. Francja i Wielka Brytania nie będą w stanie stworzyć równowagi w Europie Zachodniej, zagrożonej dominacją niemiecką. Szczególna rola w tym zadaniu spoczywa na USA. Pozytywne rozwiązanie tej kwestii wymaga także pełnej integracji zjednoczonych Niemiec z Zachodem oraz przyjaznych stosunków Sojuszu Północnoatlantyckiego z Rosją.

Pomimo wejścia Polski do NATO i UE nie może być porównywana z Rosją i Niemcami pod względem absolutnych wielkości militarnych, oraz potencjałów

---

[177]Por. J. Kaczmarek , A. Słowiński, Bezpieczeństwo, Świat - Europa - Polska, Warszawa 1998, s. 72-74.
[178]W. Góralski, Japonia, działalność na rzecz osiągnięcia pozycji supermocarstwa. Warszawa 1992, s. 35.

- brak reakcji na pojawiające się wyzwanie i poddanie się możliwości destrukcyjnego (obezwładniającego, zakłócającego) oddziaływania, co może prowadzić do powstania szeregu zagrożeń ze strony środowiska międzynarodowego[175].

Istnieje szereg niekorzystnych uwarunkowań ekonomicznych, politycznych i militarnych bezpieczeństwa Polski, niosących ze sobą wyzwania dla sfery gospodarczej. Ze względu na szeroki zakres problematyki, tylko niektóre z nich zostaną przedstawione.

W sferze politycznej współczesny system stosunków międzynarodowych określający warunki bezpieczeństwa globalnego i regionalnego charakteryzuje się niezbyt pewną stabilnością. Nowy światowy układ sił jest w trakcie powstawania, a jego przyszła struktura podmiotowa - poza dominującą pozycją USA jest trudna do określenia.

Stany Zjednoczone są obecnie największą polityczną, gospodarczą i militarną potęgą, jedynym mocarstwem światowym prowadzącym politykę globalną. Wielkość amerykańskiego rynku wewnętrznego i jego zdolności produkcyjne, a także potencjał naukowy tego mocarstwa, zapewniają mu dominację nad pozostałymi państwami[176], lecz mimo to nie są jednak w stanie angażować się wszędzie jednakowo. Uwzględniając różne zagrożenia swoich interesów muszą dokonywać selekcji priorytetów.

Rosja jest nadal mocarstwem militarnym wywierającym wpływ nie tylko na europejskie, lecz i światowe bezpieczeństwo. Pomimo wielu zastrzeżeń, Rosja będzie jednym z głównych czynników wpływających na kształt i funkcjonowanie światowego systemu bezpieczeństwa, chociaż nie będzie to rola hegemona. Rosja jest dalej potęgą militarną - głównie nuklearną. Mimo całej złożoności stosunków między Rosją a USA, oba państwa potrzebują się wzajemnie. Wiadomo bowiem, że samych Stanów Zjednoczonych nie wystarcza aby ukształtować i utrzymać dalszy porządek światowy. Stąd Amerykanie gotowi są dzielić się z Rosją strefami wpływów, zwłaszcza w przestrzeni postradzieckiej i na jej południowych obrzeżach (tak jak dzielą się z Francją w międzyzwrotnikowych regionach Afryki). A Rosja

---

[175]Por. *Podstawy, mechanizmy*...wyd. cyt., s.222.
[176]Narodowa strategia Stanów Zjednoczonych Ameryki Północnej, AON, Warszawa 1992, s. 4.

Wskazane zjawiska nie wyczerpują całej gamy działań czy też sytuacji, które mogą wystąpić w rozpatrywanych obszarach. Współczesna polityka i ekonomia charakteryzują się wielopłaszczyznowymi powiązaniami międzynarodowymi. Ekonomia jest też doskonałym instrumentem realizacji celów przez kraje dominujące gospodarczo w swoim otoczeniu. Spektrum celowych działań, jakie w tym obszarze mogą być podjęte, stając się narzędziem presji, faworyzowania bądź wymuszania jest bardzo szerokie i trudne do precyzyjnego zidentyfikowania. Takich działań można obawiać się zarówno ze strony najsilniejszych krajów jak i podporządkowanych im organizacji międzynarodowych.

Zewnętrzne ekonomiczne uwarunkowania bezpieczeństwa gospodarczego Polski można sprowadzić do określonych obszarów takich jak:

- nasilające się procesy globalizacji życia gospodarczego i związane z tym narastanie współzależności rozwoju i funkcjonowania gospodarek narodowych;
- zjawiska i procesy gospodarcze w różnych regionach świata i ich wpływ na wymianę międzynarodową, koniunkturę różnych regionów, ugrupowań gospodarczych poszczególnych krajów;
- umiędzynarodowienie rynków finansowych i globalna kontrola przepływów pieniężnych;
- pogłębiające i rozszerzające się procesy regionalnej integracji gospodarczej.

Po rozpadzie „bloku wschodniego" stan stosunków międzynarodowych determinowany jest w większym stopniu przez czynniki natury ekonomicznej niż militarnej, a stabilizacja nie jest już osiągana wyłącznie za pomocą równowagi sił wojskowych. Nasila się rywalizacja gospodarcza o strefy wpływów, rynki zbytów i o panowanie nad źródłami bogactw naturalnych. Potęgi i główne ośrodki gospodarcze starają się kształtować stosunki polityczne i gospodarcze zgodnie ze swoimi interesami. Sama rywalizacja o bogactwa surowcowe znajdujące się na terytorium państw nie rozwiniętych nie ustała, a przede wszystkim o dostęp do zasobów o znaczeniu podstawowym: wody, ziemi uprawnej, żywności, energii i wszelkich kopalin.

gospodarczych. Nadal pozostawać będzie między dwoma wielkimi sąsiadami, narażona na rozgrywanie przez Rosję i Niemcy swoich interesów naszym kosztem. Rozpatrując uwarunkowania bezpieczeństwa ekonomicznego Polski na płaszczyźnie polityczno - militarnej narzuca się wniosek, że świat po zimnej wojnie nie jest miejscem bezpiecznym. Pogłębiają się napięcia lokalne. Po zakończeniu zimnej wojny nasiliły się, konflikty regionalne wynikające z różnic etnicznych, plemiennych, religijnych i narodowych. Poszukiwanie bezpieczeństwa zewnętrznego poprzez zwiększenie zbrojeń stworzyło warunki do braku stabilizacji i do zmniejszonego bezpieczeństwa międzynarodowego.

W świecie mamy do czynienia z krajami i regionami biednymi i bogatymi, słabo i wysoko rozwiniętymi, stabilnymi i wewnętrznie skonfliktowanymi na płaszczyźnie etnicznej, religijnej i ekonomicznej. Konflikty te mogą występować na obszarze jednego lub kilku krajów. Europa w perspektywie najbliższych lat narażona jest bardziej na lokalne konflikty zbrojne niż na konflikt o dużej skali. Przykłady potwierdzające taką tezę, też mają miejsce już dziś w południowych obszarach Europy (np.: rozpad Jugosławii). W perspektywie nie można wykluczyć takich zagrożeń również w innych częściach Europy.

Obserwuje się również:

- postępującą utratę kontroli nad produkcją i dystrybucją broni konwencjonalnej oraz masowej zagłady, a także nowoczesnymi technologiami jej produkowania;
- powstawanie ponadpaństwowych organizacji o charakterze politycznym lub gospodarczym, a także przestępczym bądź wyznaniowym;
- postępującą degradację środowiska naturalnego;
- brak znaczącego wzrostu świadomości (wykształcenia) ludności świata adekwatnie do postępującego rozwoju technicznego, dostępu do technologii oraz wyżu demograficznego;
- mnożenie się konfliktów i czystek etnicznych, odrodzenie ruchów nacjonalistycznych i neofaszystowskich oraz intensyfikację religijnego fundamentalizmu jako zarzewia terroryzmu;
- stosowanie wybiórczej i siłowej polityki „wymuszania pokoju" przez mocarstwa.

swobodne przepływy siły roboczej w skali całej gospodarki światowej a nawet w skali poszczególnych regionów.

Przyrost ludności w krajach biednych stwarza ogromne problemy: brakuje żywności, występuje stagnacja w systemie edukacji podstawowej i zawodowej, załamują się struktury państwowe, brakuje mieszkań, miejsc pracy oraz zaplecza socjalnego. w rezultacie niezwykle niski jest standard życia, nierównomierny podział dóbr konsumpcyjnych. Pogłębiają się konflikty na tle terytorialnym, etnicznym i religijnym. Tak duże zróżnicowanie w gospodarce światowej stwarza zagrożenia dla jej funkcjonowania i rozwoju, pogłębia zależność między gospodarkami słabo i wysoko rozwiniętymi. Pojawia się groźba masowych migracji, także na obszary krajów średnio rozwiniętych.

Wiele państw Europy postrzega zagrożenia z racji swobodnego przepływu ludności przez granice, które często prowadzą do nielegalnej migracji, przemytu, przestępczości zorganizowanej, nieefektywnej działalności policji, korupcji urzędników państwowych oraz sporów etnicznych. Tworzone są bariery aby w ten sposób zwiększyć dochody ludności danego kraju i zapewnić zatrudnienie istniejącym no obszarze tego kraju niemobilnym czynnikom produkcji. Te kwestie wymagają szerszej dyskusji społecznej i konsensusu w celu rozwiązywania tych problemów. Ma to niewątpliwie wpływ na procesy hamowania przyjmowania nowych członków w skład Unii Europejskiej.

Współcześnie obok działalności międzynarodowej państw występuje szereg innych podmiotów. Uczestnicy stosunków międzynarodowych są zbiorowością bardzo liczną i niejednorodną. Różnią się między sobą wieloma istotnymi cechami. Okazuje się bowiem, że obok dyplomaty i żołnierza, symbolizującego tradycyjnie aktywność zewnętrzną państw, na arenie międzynarodowej działają także liczne podmioty pozapaństwowe[180]. Są wśród nich m.in. przedsiębiorstwa ponadnarodowe, osoby prywatne (np. turyści), partie polityczne, kościoły, fundacje, organizacje mniejszości narodowych, tajne związki terrorystyczne, a także bardzo zróżnicowana grupa organizacji międzynarodowych. Podmioty te niejednokrotnie w tak dużym stopniu oddziaływały na życie międzynarodowe, że bez uwzględnienia ich

---

[180]Por. J. Stefanowicz, *Ład międzynarodowy*. Warszawa 1996, s. 100.

Przez całe wieki, handel międzynarodowy był najstarszą oraz najważniejszą formą więzi ekonomicznych między państwami, obecnie jest na równi z wojnami głównym czynnikiem kształtującym stosunki między narodami i państwami. Współczesny handel międzynarodowy jest odbiciem daleko posuniętej specjalizacji międzynarodowej, w ramach której ma miejsce wymiana części i podzespołów wchodzących w skład finalnego produktu.

Postęp technologiczny sprawił więc, że gospodarki poszczególnych państw osiągnęły niespotykany do tej pory poziom umiędzynarodowienia i wzajemnej zależności od siebie. Jednocześnie zjawiska w dobie kształtowania się społeczności międzynarodowej „trzeciej fali", z charakterystycznymi dla niej globalizacją, rewolucją informacyjną i wszechogarniającą ekspansją technologiczną, staną się najprawdopodobniej źródłem zagrożeń dla istnienia współcześnie rozumianych państw i narodów.

Pod pojęciem globalizacji często rozumie się najbardziej zaawansowaną formę umiędzynarodowienia działalności gospodarczej, realizowanej na płaszczyźnie rynków, sektorów (branż) i przedsiębiorstw. Pod pojęciem tym rozumie się często określony stan gospodarki światowej (liberalizację handlu i przepływów kapitału), jak również nasilające się procesy integracji światowej i umiędzynarodowienia życia gospodarczego. Pojęcie globalizacji oznacza także wzrost różnego rodzaju powiązań między różnymi podmiotami życia międzynarodowego oraz wzajemne, najczęściej asymetryczne oddziaływania we wszystkich sferach życia społeczeństwa, od umiędzynarodowienia rynków i kapitału po kulturę masową, migracje, finanse i zapewnienie pokoju[179]. Najbardziej widocznymi efektami globalizacji było znaczne zwiększenie handlu światowego i przepływów kapitału.

W gospodarce światowej mamy obecnie do czynienia z globalizacją rynków, która odnosi się do integracji produktu oraz z globalizacją rynków kapitałowych. Utrzymuje się natomiast nadal duża segmentacja rynków pracy, ponieważ większość państw prowadzi dosyć restrykcyjną politykę emigracyjną utrudniającą

---

[179]Por. A. Gwiazda, Globalizacją i regionalizacja gospodarki światowej, Wyd. Adam Marszałek, Toruń 1998, s. 9-10.

Ekonomiczna dematerializacja polega m.in. na tym, że „niepomiernie wzrasta rola transakcji czysto finansowych. Mniej ważą w gospodarce światowej takie elementy materialne, jak grunty, surowce czy maszyny. Nabierają zaś znaczenia jej elementy nie związane z przetwarzaniem materialnego substraktu: wiedza naukowa, dostęp do informacji, reklama, cała sfera usług czy właśnie sfera finansów"[182].

Szczególnie trudna jest liberalizacja transakcji finansowych. Jednocześnie międzynarodowe transakcje finansowych, jak dotąd nie podlegają żadnym regulacjom. Bardzo duża mobilność na współczesnych rynkach finansowych powoduje, że rządom coraz trudniej przychodzi prowadzić „racjonalną" z punktu widzenia interesów ich kraju, politykę monetarną. Natomiast zwiększyło się znacznie ryzyko przemknięcia danego kryzysu finansowego do innych krajów, co potwierdziły kryzysy w Azji. Okazuje się, że globalne rynki kapitałowe determinują w pewnym stopniu posługiwanie się stopą procentową i kursami walutowymi dla regulacji sytuacji gospodarczej w danym kraju. Polityka ta może być używana w celu regulacji gospodarki krajowej lub też w celu regulacji kursu walutowego, ale nie może ona wpłynąć na osiągnięcie obu tych celów naraz[183].

Rozwój społeczeństw wiąże się także z wyraźnym wzrostem zagrożeń o charakterze niemilitarnym. Są to głównie zagrożenia środowiska naturalnego spowodowane przez klęski żywiołowe i katastrofy przemysłowe lub komunikacyjne. Te, a także nie ujęte tu uwarunkowania w istotny sposób rzutują na kształt bezpieczeństwa ogólnego i ekonomicznego Polski. Są one przedmiotem współcześnie prowadzonych ocen i analiz.

Coraz większe otwarcie polskiej gospodarki niesie ze sobą szereg zagrożeń dla dziedzin dotychczas ochranianych przez państwo. Proces ten jest powiązany z trendem globalizacji gospodarki światowej. Odnosi się to do takich obszarów jak rynek finansowy, hutnictwo, przemysł paliwowy, transport samochodowy i kolejowy, telekomunikacja, energetyka, rolnictwo wraz z szeroko rozumianym sektorem żywnościowym. Efektem otwarcia polskiej gospodarki jest już widoczny wzrost konkurencji na naszym rynku.

---

[182]Por. C. Porębski, *O globalizacji brzydkich stówek kilkanaście*, w „Znak" 1998 nr 7, s. 42.
[183]Por. A. Gwiazda, *Globalizacja*...wyd. cyt., s. 25.

aktywności nie można w pełni wyjaśnić wielu zjawisk i procesów międzynarodowych.

Można jednak uważać, że najbardziej dynamicznymi uczestnikami stosunków międzynarodowych są państwa, posługujące się najszerszym i najbogatszym zbiorem środków i metod działania. Mają one do swojej dyspozycji środki i metody polityczne, gospodarcze, wojskowe, psychospołeczne i wywiadowcze. Wykorzystują ponadto środki normatywne (normy międzynarodowe) oraz posługują się instrumentalnie innymi uczestnikami stosunków międzynarodowych, w tym obcymi rządami, organizacjami społecznymi, partiami politycznymi czy ruchami międzynarodowymi.

Instytucje międzynarodowe wywierają wpływ na procesy rozwoju i funkcjonowania stosunków międzynarodowych. Pluralizm uczestników stosunków międzynarodowych komplikuje życie międzynarodowe także dlatego, że różne podmioty przenoszą na płaszczyznę międzynarodową wiele spraw i problemów wewnętrznych. W ten sposób przemieszcza się położenie wielu konfliktów, sporów, napięć, sojuszy i solidarności.

Proces globalizacji wywiera istotny wpływ na reformowanie gospodarek, a zwłaszcza na gospodarki przechodzące transformację ustrojową, takie jak Polska. Rozpoczynając procesy reform gospodarczych rządy poszczególnych państw zostały z mniejszą władzą w rękach niż w okresie przed rozpoczęciem tych reform. Okazało się też, że rządy te nie mają obecnie już pełnej kontroli nad procesem reform w skali własnego kraju (ani tym bardziej nad postępującą globalizacją w skali regionalnej i całej gospodarki światowej). Staje się to często podstawą usprawiedliwiania błędów popełnianych w polityce rządu i zarządzaniu państwem nie dającym się rzekomo kontrolować procesem globalizacji, który „wymusza" na rządzie takie, czy inne kroki[181].

Współczesny przepływ kapitału w skali globalnej jest oderwany od rzeczywistych inwestycji i to stanowi poważne zagrożenie dla funkcjonowania gospodarki wielu państw (w tym jak się wydaje także dla Polski). Niektórzy określają ten efekt globalizacji mianem „dematerializacji" gospodarki światowej.

---

[181]Por. A. Gwiazda, *Globalizacją i regionalizacja gospodarki światowej,* Adam Marszałek, Toruń 1998, s. 18.

niekorzystnym zachowaniem się kapitału międzynarodowego w stosunku do polskiej gospodarki.

Przede wszystkim może pogłębić się penetracja gospodarki polskiej przez międzynarodowy kapitał spekulacyjny, który może napływać i odpływać w rytm zmian sytuacji na międzynarodowych rynkach finansowych (kapitałowych). Niewątpliwym skutkiem będzie rozchwianie kursów walutowych, kursów złotego do innych walut, stopy procentowej, które będą prowadzić do destabilizacji systemu finansowego gospodarki polskiej. Ze względu na wynikającą stąd niepewność, efektem będzie ograniczenie transakcji w obrotach handlowych z zagranicą (zarówno przez eksporterów i importerów krajowych i zagranicznych).

Jednym z elementów tych działań będzie zrównoważenie deficytu handlowego. Jego utrzymywanie się jest główną przyczyną deficytu obrotów bieżących handlu zagranicznego, a utrzymywania się takiej sytuacji w dłuższym okresie oznacza narastanie zadłużenia zagranicznego.

Procesy transformacji ustrojowej, trwające w Polsce od kilkunastu lat, tj. budowy demokracji i rynkowej gospodarki oprócz wielu pozytywnych zjawisk generują także zjawiska będące wyrazem wewnętrznej destabilizacji społeczno – politycznej między innymi takie jak:

- ubożenie społeczeństwa, spadek płac realnych;
- utrzymujące się bezrobocie, utratę praw wcześniej nabytych;
- brak stabilnych unormowań prawnych i sprawnego wymiaru sprawiedliwości;
- wzrastającą przestępczość pospolitą i zorganizowaną;
- ograniczanie praw i swobód obywatelskich;
- złe gospodarowanie mieniem publicznym;
- recesję gospodarczą;
- wzrastające zadłużenie państwa;
- piractwo i nieposzanowanie praw autorskich;
- wzrost korupcji urzędników;
- bezkarność aferowych „rekinów" i „trucicieli" środowiska naturalnego;
- demagogiczną retorykę polityków i spadek ich wiarygodności;
- dążenia rewindykacyjne byłych właścicieli;

Wszelkie prognozy dotyczące przyszłego rozwoju gospodarczego Polski mogą ujawniać pewne odchylenia od rzeczywistości, co jest wynikiem tego, iż dzisiaj także perspektywy rozwojowe gospodarki światowej obarczone są dużym współczynnikiem niepewności. Jest to z jednej strony wynikiem trwałości trendu wzrostu gospodarczego w Stanach Zjednoczonych, który w znacznym stopniu jest oparty na rosnącym popycie wewnętrznym oraz zdolności państw Europy Zachodniej do przezwyciężenia tendencji stagnacyjnych w gospodarkach narodowych.

Na przyszłość gospodarki światowej znacząco rzutuje także sytuacja gospodarek państw Dalekiego Wschodu, przede wszystkim przezwyciężenie trendów kryzysowych przez gospodarkę japońską oraz utrzymanie wysokiego tempa wzrostu przez gospodarkę Chin. Kształtująca się tam sytuacja ma bezpośredni i pośredni wpływ na polską gospodarkę.

Duży wpływ na rozwój naszej gospodarki będzie miał rozwój sytuacji w krajach powstałych po rozpadzie ZSRR, ponieważ większość z krajów należących do Wspólnoty Niepodległych Państw jest naszymi naturalnymi rynkami zbytu. Poza republikami bałtyckimi gospodarki tych państw znajdują się w stanie zapaści gospodarczej i dlatego znacznie bardziej żywiołowo reagują na wszelkiego rodzaju zachwiania. W tej sytuacji trudno obecnie oprzeć na nich trwały rozwój naszej gospodarki bez odpowiedniej interwencji państwa np. w formie wspierania eksportu poprzez udzielanie rządowych gwarancji.

Wielką niewiadomą bieżących i przyszłych uwarunkowań rozwoju gospodarczego Polski jest sytuacja na międzynarodowych rynkach finansowych. Trzeba na wstępie podkreślić, iż dotychczas nie stworzono sprawnych mechanizmów, które pozwalałyby średniemu państwu o otwartej gospodarce rynkowej na efektywne ingerowanie w te rynki. Z tych powodów Polska jest narażona na „wahnięcia gospodarcze" związane z nagłym napływem lub odpływem kapitałów. W dużej części są to kapitały spekulacyjne, na działanie których jesteśmy szczególnie narażeni, gdyż pojawienie się ich grozi destabilizacją gospodarki. Sytuacja rozchwiania na międzynarodowych rynkach finansowych powoduje, iż gospodarkę światową cechuje duża niepewność. Może to skutkować

- główne partie polityczne (rządzące i opozycyjne) po wejściu Polski do NATO i UE są zgodne co do strategicznych celów polityki zagranicznej. Pomimo, że negocjacje związane z przystąpieniem do UE napotykały na szereg przeszkód ze strony ugrupowań politycznych preferujących narodowo - chrześcijańskie wartości. Ugrupowania te, dzisiaj nie stanowią aż tak znaczącej siły politycznej, a przypadku załamania gospodarczego lub kryzysu społecznego, nie będą mogły w krótkim czasie pozyskać wielu zwolenników i stać się trudną przeszkodą uczestniczenia Polski w UE;
- kluczowe reformy zamykające proces transformacji ustrojowej tj. reforma samorządowa, ubezpieczeń społecznych, przemysłu ciężkiego, rolnictwa, służby zdrowia i edukacji będą zapewne wdrażane, wewnętrzny opór „materii" i konieczność uwzględniania wielu sprzecznych interesów różnych środowisk najprawdopodobniej sprawi, że kształt ww. reform będzie odbiegał od oczekiwań społecznych co będzie zapewne źródłem napięć wewnętrznych;
- liberalna polityka ekonomiczna będzie jednym ze źródeł postępu gospodarczego ale będzie również prowadziła do zubożenia dużej części społeczeństwa, która może stać się zapleczem dla tych wszystkich ugrupowań, które preferują inna wizję rozwoju kraju, jak również inną wizję zjednoczonej Europy.

2.2.2. Analiza stanu bezpieczeństwa ekonomicznego Polski w latach 1989÷2003

Najważniejszymi potrzebami ludzkości zawsze były potrzeby fizjologiczne i bezpieczeństwa, to w swojej istocie nie zmieniło się do dzisiaj. Różnice w odczuwaniu potrzeb fizjologicznych i bezpieczeństwa na przestrzeni dziejów ludzkości uwidaczniają się w ciągłym poszerzeniu się tych obszarów. Jeżeli człowiek pierwotny, aby zaspokoić swoje podstawowe potrzeby dążył jedynie do przedłużenia gatunku, zaspokojenia głodu, a życie w grupie dawało mu większe poczucie bezpieczeństwa.

Istniejące potrzeby i nakładające się na ich realizację możliwości rozwojowe są przyczyną hierarchii potrzeb, z której to w pierwszym rzędzie wypływają

- klerykalizację życia społeczno – politycznego;
- próby ograniczenia tożsamości narodowej i wyznaniowej, uprzedmiotowianie społeczeństwa, arogancję władzy itp.[184]

Należy stwierdzić, że niezadowolenie społeczeństwa zmienia się w czasie w zależności od rozwoju jego sytuacji (poczucia bezpieczeństwa egzystencjalnego). Przy czym przyzwolenie na wszelkiego rodzaju manipulacje uzdrawiające sytuację wewnętrzną maleje. Wynika to przede wszystkim z rozbieżności między realiami dnia codziennego (rzeczywistością) a oczekiwaniami wynikającymi z obietnic przedwyborczych.

Zagrożenie dla stabilności wewnętrznej państwa stanowią, oczywiście, tylko te formy niezadowolenia (protestu), które obejmują szerszy krąg społeczeństwa lub są wyrażane przez grupy zawodowe mające znaczenie strategiczne. Do tych ostatnich należą m.in.: górnicy, hutnicy, energetycy, kolejarze itp. Strajk tych grup zawodowych, podobnie jak strajk generalny, może sparaliżować cały kraj i doprowadzić do destabilizacji (sparaliżowania) życia wewnętrznego. W takiej sytuacji trudno podejmować racjonalne decyzje, a każde dyletanctwo może spowodować zaognienie sytuacji i nie kontrolowany jej rozwój.

Dokonana analiza czynników wpływających na stan stabilności wewnętrznej upoważnia do sprecyzowania następujących stwierdzeń:

- ograniczenia w zaspokajaniu potrzeb egzystencjalnych grup zawodowych lub szerszych zbiorowości, tzw. środowiskowych grup społecznych, może być traktowane jako potencjalne źródło zagrożeń bezpieczeństwa ekonomicznego państwa. Można przyjąć, iż w przyszłości niezadowolenie społeczeństwa na tle poziomu zaspokajania potrzeb nie przybierze jednak charakteru konfliktotwórczego, zagrażającego stabilności wewnętrznej państwa do tego stopnia, aby skutkowało to zagrożeniem militarnym;
- na tle sprzeczności interesów grup społecznych i etnicznych lub wyznaniowych, może powstać zagrożenie stabilności wewnętrznej państwa, a w skrajnym wypadku - nawet zagrożenie militarne;

---

[184]Por. S. Dworecki, *Od konfliktu do wojny*, Wyd. BUWIK, Warszawa 1996, s. 31-33.

trendach globalizacyjnych we wszelkich wymiarach ludzkiej jest zjawiskiem nieodłącznym.

Polska, tak jak na początku lat dziewięćdziesiątych, również na przełomie XX i XXI wieku stanęła przed ogromnymi zagrożeniami wobec zaistniałego rozwoju gospodarczego kraju. Mimo ogromnego wysiłku całego społeczeństwa w okresie poprzedniej dekady polska gospodarka nie stworzyła podstaw do podjęcia równorzędnej walki, choćby w wybranych dziedzinach życia gospodarczego, z wysoce konkurencyjnymi gospodarkami krajów rozwiniętych np.: Francji, Stanów Zjednoczonych, Niemiec i innych państw.

Przez całą dekadę lat dziewięćdziesiątych liczono, iż prywatyzacja i wolny rynek rozwiążą wszelkie bolączki polskiej gospodarki. Państwo w coraz to większym stopniu odżegnywało się od wszelkich form interwencjonizmu państwowego. Jednak jak dowodzi rzeczywistość nasza gospodarka posiada jeszcze nazbyt słabe podstawy, aby poradzić sobie samodzielnie, bez intensywnego wsparcia ze strony instytucji państwowych, z wymogami stawianymi przez wolny rynek. Warto przy tym zauważyć, iż silne i dynamicznie się rozwijające gospodarki np. amerykańska posiadają nad sobą rozwinięty przez państwo parasol ochronny. Dotyczy on może nie wszystkich, ale wielu wybranych dziedzin i aspektów gospodarki.

Koniecznym było określenie przez państwo kierunków rozwoju polskiej gospodarki, a co z tym jest związane określenie dziedzin, które będą motorem napędowym rozwoju gospodarczego kraju. To z kolei wymusiło podjęcie kolejnych wyzwań, których realizacja była niezbędna dla dynamicznego i płynnego rozwoju kraju. Należało stworzyć w pierwszej kolejności stabilne ramy prawne dla działalności gospodarczej. Taki postulat został skierowany do takich obszarów jak prawo podatkowe, prawo celne, prawo handlowe, czy też administracyjne. Ponadto przy ich tworzeniu powinno się dbać o zgodność z normami międzynarodowymi, a przede wszystkim powinny być trwałe oraz pozwalające na planowanie działalności przez przedsiębiorstwa przynajmniej w perspektywie średniookresowej, czyli trzy - pięcioletniej.

By umożliwić rozwój gospodarczy kraju należy ponieść odpowiednie nakłady na infrastrukturę kraju. Kwestią rozwiązań szczegółowych jest sposób

podstawowe potrzeby tj. egzystencjalne, tak rozumiane z punktu widzenia jednostki, jak i kraju. W pierwszej kolejności istnieje potrzeba zapewnienia spełnienia podstawowych potrzeb bezpieczeństwa, choć trudno w rzeczywistości oddzielić oba obszary. Obie kategorie potrzeb można zaliczyć do potrzeb niedostatku, czyli takich, które rodzą się w wyniku braku określonego elementu. Jest to składnik wynikający z obszaru potrzeb biologicznych, psychologicznych, czy nawet środowiskowych. Jednak należy zaznaczyć, iż aby zaistniało poczucie danej potrzeby musi być ona uświadomiona.

To człowiek współczesny nie uważa jako takiego zaspokojenia odczucia głodu za potrzebę podstawową, a poszerzył ją o sposób i formę uczynienia tego. Potrzeby egzystencjonalne poszczególnych ludzi przekładają się na potrzeby grup społecznych, a następnie potrzeby państwa. Jednym z obszarów o bardzo dużym znaczeniu dla zaspokojenia potrzeb egzystencjonalnych państwa jest obszar bezpieczeństwa ekonomicznego. Bywa bowiem rzadko aby potrzeby bilansowały się z posiadanymi możliwościami. Odnosi się to także do potrzeb i możliwości kształtowania bezpieczeństwa ekonomicznego Polski.

Pomimo kilkunastu lat przemian społeczno-gospodarczych Polska jest nadal krajem o formującym się obliczu gospodarczym. Procesy transformacji zapoczątkowanej w 1989 r. zaskoczyły wszystkich, tak rządzących, jak i opozycję, która nie była przygotowana i nie spodziewała się przejęcia rządów w Polsce. Wraz z przemianami politycznymi Polski. W obszarze politycznym istniały pewne koncepcje przebudowy państwa i były one opracowane ramowo, to program gospodarczy był tworzony na bieżąco. Wraz z objęciem władzy przez nowy nie socjalistyczny rząd, została nakreślona droga rozwoju polskiej gospodarki. Stała się nią przemiana z systemu gospodarki planowej w kierunku gospodarki rynkowej.

Gospodarka przełomu lat osiemdziesiątych i dziewięćdziesiątych była niedostosowana do wymogów wysoce konkurencyjnych rynków światowych. Odnosiło się to zwłaszcza do poziomu jej zaawansowania technologicznego, jak i sposobów zarządzania nią. Jej przebudowa poszła w kierunku przemian systemowych - zwłaszcza strukturalnych i własnościowych. Celem podjętych przemian było dostosowanie polskiej gospodarki do wymogów stawianych przez międzynarodowe rynki, na których ostra walka konkurencyjna przy narastających

Patrząc na przykłady krajów azjatyckich można pokusić się o stwierdzenie, iż pierwsze społecznie oczekiwane efekty byłyby widoczne jako trwały trend po kilkunastu latach, zaś z punktu widzenia czysto gospodarczego mogłyby być zauważalne po kilku latach. Aby uzyskać stały trend wzrostowy na poziomie przynajmniej 5% produktu krajowego brutto (PKB) w skali rocznej, należy odpowiednią część dochodu narodowego przeznaczyć na określone cele rozwojowe. Jego wysokość może być tylko przewidywana, ponieważ jego poziom zależy od szeregu wypadkowych wypływających z wewnątrz, jaki i z otoczenia gospodarki. W sytuacji gospodarczej Polski można przyjąć, że przy nakładach inwestycyjnych 25÷30% produktu krajowego brutto następuje ożywienie gospodarcze, którego efektem jest trwały trend wzrostu gospodarczego na poziomie 5÷7% w ciągu kilku lat. Uzyskanie tak wysokich nakładów wymaga skorelowania działań sektora państwowego, samorządowego i prywatnego. Wraz z określeniem wysokości potrzebnych nakładów ważną kwestią jest określenie zdolności absorpcyjnych polskiej gospodarki w obszarze inwestycji.

Potencjalnymi źródłami, z których mogłyby być zaspakajane potrzeby inwestycyjne są zarówno źródła pochodzenia krajowego jak i zagranicznego. Krajowe źródła to: inwestycje państwowe, w tym i samorządowe oraz inwestycje kapitału prywatnego. Kapitał krajowy w przypadku inwestycji państwowych (samorządowych) pochodzi z akumulowania przychodów podatkowych, prywatyzacyjnych, czy też pożyczek z krajowego systemu bankowego lub z międzynarodowych rynków finansowych, w tym z funduszy celowych pochodzących z różnych organizacji międzynarodowych lub od innych państw np. zamiana polskiego długu wobec rządu szwedzkiego na inwestycje proekologiczne na obszarze Pomorza. Natomiast źródeł rentowności dotychczas funkcjonujących przedsięwzięć gospodarczych, a co z tym jest związane otwartości systemu bankowego na udzielanie kredytów na nowe inwestycje. Niestety pierwsze dwa elementy tego układu wykazują pewną słabość, gdyż nakłady inwestycyjne państwa oraz sytuacja na rynku wewnętrznym, jak i zewnętrznym nie sprzyja wzrostowi nakładów na inwestycje.

Poziom inwestycji w gospodarce uwidacznia się we wzroście wartości środków trwałych. Poprzez inwestycje przedsiębiorstwa zwiększają swój majątek,

finansowania przedsięwzięć z tego zakresu. Może to być kapitał państwowy, samorządowy, inwestorzy krajowi lub zagraniczni, którzy będą wspierani finansowo przez polski system bankowy, czy też poprzez pożyczki celowe z funduszy międzynarodowych np. PHARE.

Inwestycje w infrastrukturę, czyli system łączności, system komunikacyjny, czy też w system ochrony środowiska jest nieodzownym elementem przyciągającym kapitał inwestycyjny do określonych regionów. Z tego powodu wydaje się niezbędnym położenie nacisku przez państwo na dokończenie telefonizacji kraju, w standardzie umożliwiającym zapewnienie łączności zgodnie z wymogami inwestorów. Ponadto należy położyć odpowiedni nacisk na budowę autostrad, dróg ekspresowych oraz zapewnienie odpowiedniej jakości dróg lokalnych oraz ich przejezdności o każdej porze roku. W planach powinno się uwzględniać odpowiednie uzupełnienie systemu drogowego połączeniami kolejowymi.

Ważną kwestią z perspektywy rozwoju kraju jest godne uczestnictwo Polski w Unii Europejskiej, a także przyciągnięcie przedsiębiorców do rozbudowy infrastruktury proekologicznej, czyli oczyszczalni ścieków, wysypisk śmieci o odpowiednim standardzie itd. Obecnie wiele regionów oczekujących na inwestorów liczy także, iż poniosą oni odpowiednie nakłady na tę infrastrukturę. Podnosi to koszt potencjalnej inwestycji i jednocześnie stwarza barierę dla mniejszych przedsięwzięć, które mogłyby zaistnieć jedynie w regionach o przygotowanej infrastrukturze ekologicznej.

Polską gospodarkę można nazwać gospodarką rozwijającą się, która z początkiem trzeciego tysiąclecia stoi na nowo obranej drodze rozwoju. Wymaga to podniesienia aktywności gospodarczej kraju i określenia, które dziedziny będą napędzały wzrost gospodarczy. Wyselekcjonowanie w nich odpowiednich nakładów i właściwej ich alokacji oraz stworzenia dla nich przyjaznego środowiska, w którym będą działały. Im szybciej zostaną podjęte działania w tym kierunku, tym szybciej można się spodziewać oczekiwanych efektów. Jednak jest to bardzo długa droga, która będzie wymagała podjęcia dużego wysiłku i cierpliwości ze strony społeczeństwa.

gospodarczej. Walka, która toczy się o docelowy system gospodarczy Polski przebiega na linii dwóch przeciwstawnych poglądów etatyzmu - liberalizmu. Do dzisiaj nie udzielono odpowiedzi w kwestii kierunków i głębokości interwencjonizmu państwa w życie gospodarcze kraju.

Polska jest oceniana, jako kraj średniej wielkości, tak pod względem ludności, powierzchni, jak i znaczenia gospodarczego. Jednak w ekonomii, tak jak w wielu dziedzinach trudno jest jednoznacznie oceniać badane obiekty, gdyż wiele elementów jest niejednorodnych i niejednoznacznych. Z jednej strony Polska jest krajem średniej wielkości, jednak patrząc na nią z perspektywy rynku zbytu okazuje się, iż jest jednocześnie krajem dość perspektywicznym ze względu na ilość ludności. Nadal jest to obszar rodzący dla producentów, czy usługodawców szerokie możliwości, dlatego w wielu dziedzinach należy oczekiwać skoku jakościowego, który dążył do osiągnięcia standardów krajów rozwiniętych.

Polska jako kraj położony w Europie Środkowej znajduje się na skrzyżowaniu naturalnych tras tranzytowych ze wschodu na zachód i z południa na północ. Mimo dużego skoku technologicznego w XX wieku położenie i jej ukształtowanie terenu nie straciło na znaczeniu tak gospodarczym, politycznym, jak i militarnym. Możliwości Polski przełomu XX i XXI wieku zostały ukształtowane na przestrzeni jej dziejów.

Pod względem powierzchni wśród wybranych krajów zajmuje 12. miejsce. Wśród krajów NATO pod względem powierzchni Polska zajmuje 7. miejsce; wśród krajów bezpośredniego otoczenia spoza NATO zajmuje 3. miejsce po Rosji i Ukrainie; wśród krajów dalszego otoczenia znajduje się na 3. miejscu po Szwecji i Finlandii.Pod względem gęstości zaludnienia podobnie, jak pod względem liczby ludności i powierzchni Polska należy do krajów o średniej gęstości zaludnienia w grupie omawianych państw. Jednak odnosząc porównanie gęstości zaludnienia o podobnej liczbie ludności np. Hiszpanii, czy Ukrainie okazuje się, iż jest krajem o znacznie większej gęstości zaludnienia[186].

Dokonując oceny możliwości Polski wynikających z porównania dwóch podstawowych wielkości, czyli powierzchni kraju i liczby ludności oraz

---

[186]Tamże, s. 122.

a w konsekwencji rośnie również realna wartość środków trwałych przez nie wykorzystywanych. Mimo załamania gospodarczego lat osiemdziesiątych i recesji gospodarczej na początku lat dziewięćdziesiątych widoczny jest stały przyrost wartości nakładów na środki trwałe[185]. Niestety nie jest to poziom, który pozwoliłby na przełamanie jakościowe i ilościowe oraz nadgonienie różnic technicznych i technologicznych pomiędzy polską gospodarką, a gospodarkami krajów Unii Europejskiej.

Na poziomie centralnym możliwe jest przyciąganie kapitału do inwestowania w obszarze ekologii, szczególnie z państw sąsiednich oraz pozyskiwanie środków na inwestycje z Banku Światowego, Międzynarodowego Funduszu Walutowego, czy też Unii Europejskiej na restrukturyzacje infrastruktury gospodarczej. Możliwe jest to także poprzez działania podejmowane przez działania samorządów od strony technicznej i merytorycznej. Do regionów odpowiednio przygotowanych łatwiej napływają nowe inwestycje. Należy w tym momencie podkreślić, iż inwestorzy zagraniczni oczekują od władz centralnych danego państwa przyjęcia długofalowej, stabilnej polityki gospodarczej zapewniającej możliwość prowadzenia przedsięwzięć, które rokowałyby osiągnięcie zakładanych celów. Można stwierdzić, że taki model gospodarki jest bardzo drapieżny, a przez to trudno akceptowany przez społeczeństwo posiadające przyzwyczajenia z epoki gospodarki planowej, gdzie większość społeczeństwa miała zapewnione bezpieczeństwo socjalne – choć nie na najwyższym poziomie. Różnice w dochodach nie były tak drastyczne jak w latach dziewięćdziesiątych i przy zapewnieniu minimum socjalnego słabiej odczuwalne. Ponadto praca nie była tylko środkiem do realizacji potrzeb, ale także obowiązkiem każdego obywatela. Częstokroć ludzie bez pracy znajdowali się pod silnym pręgierzem nie tylko państwa, ale i często ze strony środowiska. W szczególności odnosiło się to do obszarów o wiekowych tradycjach przemysłowych np. Dolny czy Górny Śląsk.

Polska na początku XXI wieku nadal stoi na rozdrożu i przed podjęciem ostatecznych decyzji, które wprowadziłyby najkorzystniejsze rozwiązania najbliższe polskiej tradycji, mentalności i odpowiadałby wymogom współczesnej

---

[185]Por. *Rocznik statystyczny Polski 2003,* GUS, Warszawa 2003. s. 436.

tendencję odchodzenia od węgla kamiennego w procesie pozyskiwania energii w Polsce. Wynika to z ograniczenia w popycie na węgiel kamienny, co w rezultacie spowodowało spadek jego wydobycia. Przewidywane obniżenie wydobycia, wynikające z restrukturyzacji branży, nie zostało jeszcze osiągnięte. Ograniczenia te pociągają za sobą konieczność restrukturyzacji całego przemysłu wydobywczego, który jest zaangażowany w eksploatację zasobów węgla kamiennego. Do procesu restrukturyzacji przemysłu węgla kamiennego przymierzano się od początku lat dziewięćdziesiątych, jednak proces ten nabrał rozmachu dopiero na przełomie 1998 i 1999 r. Wówczas to przystąpiono do ostatecznej likwidacji Górnośląskiego Zagłębia Węglowego (GZW) oraz ograniczenia wydobycia w Dolnośląskim Zagłębiu Węglowym (DZW), w którym to rozpoczęto likwidację nierentownych kopalni. Do początku 2002 r. nie został jednak stworzony docelowy model polskiego górnictwa węgla kamiennego. Stworzenie realnego modelu będzie wymagało rozstrzygnięcie szeregu kwestii. Przede wszystkim nie jest znana przyszła struktura odbiorców węgla kamiennego w Polsce tj. kształt polskiej energetyki oraz docelowy model polskiej gospodarki, z której będzie wynikał stopień zapotrzebowania na ten nośnik energii pierwotnej - nie jest jeszcze ostatecznie rozstrzygnięta.

Na przestrzeni dekady lat dziewięćdziesiątych wzrosła produkcja energii elektrycznej w Polsce i w pełni są zaspakajane potrzeby rynku wewnętrznego, przy jednoczesnym marginalnym eksporcie i imporcie tego nośnika. Jednak korzystna jest tendencja utrzymywania się nadwyżki eksportowej w przypadku energii elektrycznej, choć ten fakt traktować jedynie jako posiadający niewielkie znaczenie prestiżowe[187]. Obecnie stoimy przed perspektywicznym otwarciem się rynku całej branży dla producentów z Unii Europejskiej.

Dokonując ocen wszystkich nośników energetycznych należy jednak podkreślić, iż węgiel kamienny i brunatny stanowią podstawę bazy paliwowej polskiej energetyki, zaś pozostałe nośniki energii pierwotnej jak olej opałowy i gaz ziemny stosowane są głównie do rozpalania kotłów, jak i podtrzymywania procesu spalania. Nadal jednak z węgla kamiennego wytwarza się ponad połowę energii

---

[187]Por. *Rocznik statystyczny*...wyd. cyt., s. 350.

wynikającej kombinacji obu wielkości gęstości zaludnienia zauważyć trzeba, iż Polska:

- jest krajem średniej wielkości pod względem zajmowanego obszaru, jak i liczby ludności;
- pod względem liczby ludności i powierzchni kraju zajmuje podobną pozycje w gronie porównywanych krajów;
- biorąc pod uwagę obszar europejski z wyłączeniem Rosji, po skorelowaniu wielkości liczby ludności i powierzchni jest krajem, które potencjał pozwala na konkurowanie z największymi państwami europejskimi;
- mając status kraju średniej wielkości pod względem liczby ludności, jak i zajmowanej powierzchni, dysponuje również mocnymi podstawami do uzyskania znaczącej pozycji w Europie pod względem gospodarczym, politycznym, jak i militarnym, a w szczególności na obszarze Europy Środkowej, Wschodniej i Południowej.

Możliwości rozwojowe Polski można również ocenić poprzez syntetyczny wskaźnik PKB. Ten wskaźnik w sposób syntetyczny pozwala określić możliwości trwania i rozwoju oraz utrzymania bezpieczeństwa Polski. PKB Polski jest na średnim poziomie w porównaniu do omawianych państw. Jednak jeżeli porównać PKB Polski do PKB krajów, które są podobnej wielkości pod względem ludności i powierzchni, wówczas okazuje się, wskaźnik nie jest tak korzystny dla naszego kraju. Z grona wymienionych państw jedynie Hiszpanię, Portugalię i Grecję można przyjąć za kraje do pewnego stopnia adekwatne, i które może wykorzystać w celach porównawczych dla Polski, jako wyznacznik kierunków rozwojowych. Natomiast porównanie PKB Polski, Rumunii i Ukrainy potwierdza, Polska nadal zajmuje pozycję lidera przemian w Europie Środkowo-Wschodniej. Jeżeli porównywać PKB Polski do PKB Czech i Węgier wynika, iż Polska posiada trzykrotnie większy PKB niż porównywane kraje. Jednak porównując PKB per capita omawianych państw okazuje iż Polska posiada omawianą wielkość porównywalną do Węgier i prawie dwukrotnie mniejsza niż Czechy.

Z punktu widzenia możliwości rozwojowych ważnym obszarem jest dziedzina energetyki. Można zauważyć od początku lat dziewięćdziesiątych

trochę innymi prawami niż pozostałe. Na obszarze Polski jest widoczny wzrost ruchu środków transportu chodowego, lecz jest to związane w znacznym stopniu z ruchem tranzytowym, go do tej pory nie potrafimy wykorzystać dla uzyskania określonych korzyści, czy choćby pokrycia strat wynikłych ze zwiększonego ruchu samochodowego. Ponadto nie ma programów wspierania krajowych przewoźników w konkurowaniu z ich odpowiednikami z innych krajów na rynkach europejskich.

Przez ostatnie dziesięciolecie nastąpił gwałtowny przyrost liczby samochodów osobowych i ciężarowych, ponadto uległa zmianie struktura ich własności. Na rynku użytkowników, jak i odbiorców dominującą rolę zdobyli użytkownicy indywidualni i firmy prywatne, w przeciwieństwie do poprzednich lat. Motoryzacja kraju odbywała się jakby kosztem transportu kolejowego i śródlądowego, a także kosztem zbiorowego transportu samochodowego. Głód motoryzacyjny jaki miał miejsce w okresie istnienia PRL stał się bodźcem szybkiej motoryzacji kraju.

Jednym z najdynamiczniej rozwijających się działów polskiej gospodarki jest telekomunikacja i informatyka a szczególnie telefoniczna - stacjonarna i bezprzewodowa. Na przestrzeni ostatnich lat wyraźnie widoczny jest postęp technologiczny i ilościowy, choć nadal są regiony, w których jest utrudniony dostęp do telefonów stacjonarnych. Wydaje się, iż przyszłość telefonii jest w znacznym stopniu zdeterminowana rozwojem telefonii komórkowej[188].

Nowym zjawiskiem z tego obszaru jest pojawienie na rynku telefonii stacjonarnej firm prywatnych, które podjęły walkę z dotychczasowym monopolistą Telekomunikacją Polską S.A. Przewiduje się w najbliższych latach uruchomienie telefonii UMTS oraz sieci szerokopasmowych z protokołem IP. Należy się spodziewać, iż presja konkurencji pomiędzy dotychczasowym monopolistą a firmami prywatnymi z jednej strony, a z drugiej pomiędzy sieciami stacjonarnymi i komórkowymi, przyczyni się do powstania rozwiązań jakościowo nowych w obszarze technologicznym, a przede wszystkim świadczenia szerokiej gamy tanich usług.

Bardzo ważnym działem, który ma znaczący wpływ na możliwości rozwoju

---

[188]Por. *Rocznik statystyczny*...wyd. cyt., s. 366.

elektrycznej w Polsce. Spadek wytworzonej energii elektrycznej zwęgla kamiennego w latach dziewięćdziesiątych w stosunku do lat osiemdziesiątych należy wiązać z powolnym procesem dywersyfikacji nośników energii pierwotnej w Polsce, który jest także widoczny w innych krajach.

Zakłada się, iż w 2010 r. będzie następująca struktura pozyskiwania energii elektrycznej z nośników pierwotnych:

- 60 % energii elektrycznej będzie uzyskiwane z węgla kamiennego;
- 21 % energii elektrycznej będzie uzyskiwane z węgla brunatnego;
- 7 % energii elektrycznej będzie uzyskiwane z gazu ziemnego;
- 2 % energii elektrycznej będzie uzyskiwane z elektrowni wodnych.

Innym obszarem rzutującym na możliwości rozwojowe kraju jest stan przemysłu budowlanego. W tym obszarze miały miejsca największe i wyraźne przekształcenia własnościowe. Po regresie początku lat dziewięćdziesiątych nastąpił wzrost dynamiki budowlanej, która wyraźnie osłabła po 1998 roku. Problemy gospodarcze uwidoczniły się także w budownictwie mieszkaniowym. Kurczy się budownictwo powszechne, a przedsiębiorstwa ukierunkowują się na odbiorców osiągających duże dochody. Nadal brakuje działań mających na celu pobudzenie budownictwa socjalnego, bez którego nie rozwiąże się szeregu problemów społecznych i gospodarczych.

We wszystkich obszarach sieci komunikacyjnej zauważalne jest jej kurczenie się lub stagnacja. Szczególnie jest to widoczne w obszarach zabudowanych i trasach tranzytowych. Jedynie pewien wzrost na przestrzeni lat 1999÷2003 został odnotowany w obszarze dróg publicznych o nawierzchni utwardzonej. Zauważalna jest tendencja kurczenia się rynku przewozów transportu samochodowego. Regres przeżywa także transport kolejowy oraz wodny.

Kondycja każdego rodzaju transportu jest wypadkową aktualnego stanu gospodarki. Natomiast w początkowych latach XXI wieku pomimo trudności gospodarczych widoczny jest wzrost przewozu pasażerów i towarów we wszystkich rodzajach transportu oprócz kolei. Tendencje wzrostowe w omawianym okresie utrzymały się jedynie transporcie lotniczym - w szczególności odnosi się to do liczby przewiezionych pasażerów i transporcie rurociągowym. Jednak transport lotniczy i rurociągowy są specyficznymi obszarami transportu, które rządzą się

rozwojowe rolnictwa jest jednocześnie jego siłą, bowiem można wykorzystać rosnące zapotrzebowanie na zdrową żywność, która jest produkowana metodami naturalnymi. Znaczącym wskaźnikiem określającym możliwości rozwojowe kraju jest dynamika eksportu i importu oraz saldo tych dwóch wielkości.

Na początku lat dziewięćdziesiątych dynamika eksportu w Polsce była ujemna, dopiero w 1994 r. osiągnęła dodatni współczynnik. Był jeden z najlepszych wyników do 1998 r. Jednak i w następnych latach został odnotowany spadek dynamiki eksportu, aby od 2000 r. zacząć stopniowo wzrastać.

Przyczyn dużego wzrostu można doszukiwać się w spadku zapotrzebowania rynku wewnętrznego i poszukiwaniu przez producentów innych rynków zbytu, nawet na granicy opłacalności. Odwzorowuje to tendencje, które zaistniały w polskiej gospodarce po 1997 r. Jest to początek niekorzystnego trendu, będzie objawiał się spadającą dynamiką eksportu. Należy jednak zauważyć, że na tle innych krajów dynamika polskiego eksportu kształtowała się korzystnie, jednak porównując wysokość eksportu krajów zachodnich (np. Niemiec, czy Hiszpanii) widać jak gospodarki tych krajów dynamicznie się rozwijają.

W latach 1992-2003 utrzymywała się wysoka dynamika importu. Ponadto należy zauważyć, iż dynamika importu w omawianym okresie nie przewyższała dynamiki przyrostu eksportu. Jest to zjawisko niekorzystne w skali gospodarki, gdyż może prowadzić do zjawisk kryzysowych w gospodarce narodowej, między innymi może być przyczynkiem do ujemnego rozwoju gospodarczego.

Z grona porównywanych krajów Polska jest państwem o jednym z największych ujemnych sald eksportu do importu. O poziomie kondycji gospodarki danego kraju w pewnym wymiarze może świadczyć: jaki udział procentowy posiada ujemne saldo handlu zagranicznego i importu w stosunku do eksportu?

Z analizy potrzeb i możliwości kształtowania bezpieczeństwa ekonomicznego wynika, że Polska posiada duży potencjał, który w znacznym stopniu jest wypełniać stawiane przed nim wymogi. Jednak bez systemowych rozwiązań, o charakterze długofalowym nie jest możliwe zbilansowanie potrzeb i możliwości na takim poziomie, aby osiągnąć pożądany stan bezpieczeństwa państwa.

kraju jest rolnictwo. Rozwój, struktura i dynamika rozwoju gospodarczego są w tle z tym obszarem, który w znacznym stopniu decyduje o poziomie bezpieczeństwa żywnościowego kraju. Po okresie ciągłego niedoboru żywności na rynku, ujawniło się w polskich warunkach całkowicie nowe zjawisko nadprodukcji żywności i coraz bardziej selektywnego zapotrzebowania na produkty rolne. Zwiększone zapotrzebowanie odnosi się, zarówno do obszaru indywidualnej konsumpcji, jak i zapotrzebowania ze strony przemysłu przetwórczego.

W okresie transformacji ustrojowej w naszym kraju widocznym stały się znaczne skoki wysokości dynamiki produkcji rolnej. Można się dopatrywać w tym obszarze działania niczym nieskrępowanych praw rynku. Producenci rolni napotykają szereg barier i trudności, które wynikają z zasad wolnego rynku.

Sytuacja taka uniemożliwia podejmowania planowych działań wieloletnich w obszarze rolnictwa. Przyczyn falowania dynamiki produkcji rolnej można się doszukiwać w wielu aspektach. Może to wynikać bezpośrednio obszaru problematyki rolniczej, jak i poza rolniczej.

Ważkim problemem z obszaru produkcji rolnej jest produkcja zwierzęca. Jest bezpośrednio powiązana w Polsce z produkcją roślinną. Można zauważyć w rolnictwie niekorzystne trendy polegające na masowym odchodzeniu od produkcji zwierzęcej na rzecz produkcji roślinnej i odwrotnie. Wynika to w znacznym stopniu z faktu poszukiwania przez rolników produkcji o największej stopie zwrotu w jak najkrótszym czasie, na czym cierpi jakość produkcji. Takie falowanie wynika z faktu rozdrobnienia polskich gospodarstw rolnych z małej ich specjalizacji, a także niskiego poziomu wykształcenia rolników. Niekorzystnym efektem tego typu sytuacji jest powstawanie ogromnej nadprodukcji w określonym rodzaju działalności i związanych z nią trudności ze zbytem towarów po cenie zapewniającej zysk.

Potencjał rolny Polski jest jej silną i jednocześnie słabą stroną. Polska posiada możliwości rozwinięcia produkcji rolnej, której wielkość i w perspektywie kilku najbliższych lat wysoka jakość umożliwiłaby zajęcie polskiemu rolnictwu jednego czołowych miejsc w Europie. Jednak, aby to było możliwe należy je doinwestować, wesprzeć procesy scalania gospodarstw oraz wspomagać procesy wdrażania nowszych metod produkcyjnych. Paradoksalnie pewne opóźnienie

zjawisk"[191]. Również bariery są zaliczane do tak wartościowanych zjawisk. Dlatego też biorąc pod uwagę istotę pojęcia barier i ich skutki dla procesów gospodarczych i realizacji celów ekonomicznych i obronnych, można kategorie barier i zagrożeń stosować zamiennie.

W bardziej skonkretyzowanej formie „zagrożenie" najczęściej definiowane jest jako sytuacja, w której naruszone mogą być istotne dla danego podmiotu wartości. Inna dokładniejsza definicja podaje, że „Zagrożenie, sytuacja w której istnieje zwiększone prawdopodobieństwo utraty życia, zdrowia, wolności albo dóbr materialnych". Zagrożenie wywołuje u człowieka niepokój lub strach o różnym stopniu natężenia, do przerażenia lub obezwładnienia włącznie, bądź odruch lub świadomą chęć przeciwdziałania. Zagrożenie może wynikać z przyczyn naturalnych (np. oddziaływanie żywiołów) i spowodowanych przez innego człowieka (np. nieprzyjaciela)[192]. Zagrożenia kojarzone są z możliwością wystąpienia takich oddziaływań, które uniemożliwiają lub utrudniają realizację np. egzystencji, rozwoju (wartości) eksponowanych w naukach społecznych, albo wykonywanie zadań i funkcji (korzystanie z wartości użytkowych), jak jest to rozumiane np. w odniesieniu do urządzeń technicznych.

W naukach społecznych zagrożenia definiowane są między innymi jako niekorzystne i niebezpieczne dla żywotnych interesów i podstawowych wartości danego podmiotu (jednostkowego lub zbiorowego) działania innych uczestników życia społecznego[193]. W odniesieniu do państwa i narodu zagrożenie definiowane jest „...jako możliwość powstania sytuacji, w której dane społeczeństwo nie ma warunków dla swego bytu i rozwoju lub są one w sposób istotny ograniczone"[194].

Natomiast „zagrożenie bezpieczeństwa państwa to splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych w którym z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju wewnętrznego bądź naruszenie lub utrata

---

[191]Por. R. Zięba, *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych*, w: D. Bobrów, E. Haliżak, R. Zięba, *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku*, Warszawa 1997, s. 4.

[192]Por. *Leksykon Wiedzy Wojskowej*, MON, Warszawa 1979, s. 512.

[193]Por: M. Cieślarczyk, *Niektóre psychospołeczne aspekty bezpieczeństwa, wyzwań, szans i zagrożeń*, w: „Zeszyty Naukowe AON" 1999 nr 2(35), s. 233.

[194]R. Wróblewski, *Wybrane problemy diagnozy bezpieczeństwa narodowego*, w: „Zeszyty Naukowe AON" 1991 nr 3/4 , s. 69.

2.2.3. Bariery i zagrożenia w procesie kształtowania bezpieczeństwa ekonomicznego Polski

Bezpieczeństwo państwa w jego różnych wymiarach, obecnie coraz częściej postrzegane jest w kategoriach zagrożeń wartości chronionych przez państwo oraz przeciwdziałań zmierzających do redukcji zagrożeń lub ograniczenia skutków destrukcyjnych oddziaływań. Dlatego też można stwierdzić, że zagrożenia są nieodłącznym elementem, zarówno negatywnej jak i pozytywnej interpretacji bezpieczeństwa, a stan bezpieczeństwa państwa jest zawsze albo wypadkową albo kompromisem pomiędzy potrzebami związanymi z ukształtowaniem pożądanego stanu a możliwościami ich zaspokojenia.

Określenie barier i zagrożeń ze strony procesów rozwojowych w obecnych uwarunkowaniach współczesnego świata dla gospodarczych podstaw bezpieczeństwa kraju, ukierunkowuje je przede wszystkim na płaszczyznę ekonomiczno - obronną, jako część zagrożeń bezpieczeństwa ekonomicznego państwa. Aby określić zagrożenia ze strony procesów rozwojowych współczesnego świata dla gospodarczych podstaw bezpieczeństwa państwa, należy uprzednio zidentyfikować pojęcie zagrożeń w jego ekonomicznej treści. Jednoznaczne określenie kategorii zagrożeń i bezpieczeństwa państwa jest trudne do przeprowadzenia - co wynika ze złożoności i wielowymiarowości ekonomicznego bezpieczeństwa państwa. Dostępne definicje zagrożeń nie ułatwiają wykonania zadania określenia ich istoty. W definicjach leksykalnych zagrożenie ma bezpośredni związek ze słowem bezpieczeństwo i najczęściej jest wyjaśniane odwrotnością bezpieczeństwa[189]. Najczęściej zagrożenia konkretyzowane są poprzez wartości, które mogą być utracone, a także poprzez przedmiot destrukcyjnych oddziaływań lub cechy źródeł zagrożeń[190]. Konkretyzację umożliwia także wskazanie podmiotu lub przedmiotu bezpieczeństwa. Ponadto zagrożenia mogą być skonkretyzowane np. poprzez przedmiot destrukcyjnych oddziaływań lub cechy źródeł zagrożeń.

Ogólne przedstawienie istoty tej kategorii, jak np. przez stwierdzenie, że „Zagrożenie to możliwość wystąpienia jednego z negatywnie wartościowanych

---

[189]Por. S. Korycki, *System*...wyd. cyt., s. 54.
[190]Por. S. Dworecki, *Zagrożenia*... wyd. cyt., s. 65.

Drugie nakazuje badanie ich wpływu na możliwości realizacji wartości a także poszukiwanie sposobów eliminowania, unikania lub ograniczania zagrożeń, a w sytuacji ich przekształcenia w destrukcyjne oddziaływania, ograniczenia ich skutków.

Analizując zagrożenia gospodarczych podstaw bezpieczeństwa państwa z treści pojęć bezpieczeństwa państwa i bezpieczeństwa ekonomicznego, wskazać trzeba na dwa stanowiska w tej kwestii:

- pierwsze, koncentrujące się na określaniu zagrożeń poprzez negatywne skutki różnych oddziaływań na możliwość realizacji przez dany obiekt lub podmiot istotnych dla niego wartości;
- drugie, polegające na lokalizowaniu zagrożeń pośród konfliktów (określanie zagrożeń poprzez konflikty daje możliwość operacjonalizacji tych zagrożeń).

Zgodnie z pierwszym stanowiskiem zagrożenia gospodarczych podstaw bezpieczeństwa państwa (tożsamych w praktyce z bezpieczeństwem ekonomicznym kraju) prezentowane są jako możliwość utraty chronionych wartości rozpatrywanych na różnych płaszczyznach i jako odwrotność bezpieczeństwa. Różnica w definiowaniu polega głównie na przedstawieniu innych obiektów zagrożeń (lub płaszczyzn), jak np. system społeczno-gospodarczy lub potencjał obronno-ekonomiczny. Należy przy tym podkreślić, że kategoria potencjału gospodarczo-obronnego poprzedzała kategorię gospodarczych podstaw bezpieczeństwa państwa, a współcześnie ta pierwsza została wchłonięta przez tę szerszą drugą.

Na płaszczyźnie obronno - ekonomicznej, odnoszącej się do gospodarczych podstaw bezpieczeństwa państwa, Z. Kołodziejak zagrożenia gospodarcze ujmuje jako „..zespół czynników o charakterze wewnętrznym i zewnętrznym, uruchomienie których może doprowadzić do zaburzeń w rozwoju potencjału obronno - ekonomicznego"[199].

Podobne w treści jest stanowisko W. Stankiewicza, który w języku ekonomiki obrony pojęcie „zagrożenie" definiuje „...jako rodzaj możliwych

---

[199]Por. S. Michałowski, *Bezpieczeństwo ekonomiczne w stosunkach wschód - zachód*, PISM, Warszawa 1990, s. 23.

suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych w wyniku zastosowania przemocy politycznej, psychologicznej, ekonomicznej, militarnej itp."[195]. Takie stanowisko w kwestiach rozumienia istoty i treści zagrożeń upowszechnia się coraz bardziej. Jako reprezentatywną dla określania zagrożeń bezpieczeństwa państwa poprzez wartości, można przytoczyć następującą definicję: „zagrożenie dla bezpieczeństwa narodowego stanowi działanie lub ciąg wydarzeń, które:

- zagrażają drastycznie i w stosunkowo krótkim okresie jakości życia mieszkańców danego państwa lub
- niosą ze sobą istotne zagrożenie ograniczenia możliwości dokonywania wyborów politycznych przez rząd państwa lub prywatne instytucje pozarządowe (osoby prywatne, grupy, korporacje) w ramach danego państwa"[196].

W ramach ogólnych zagrożeń bezpieczeństwa narodowego (państwa) wyróżnia się także zagrożenia dla jego różnych dziedzin (segmentów), na których jest ono realizowane. Można zatem wyróżnić ich odpowiednie rodzaje. „Przyjmując za podstawę dziedziny, w których może wystąpić zagrożenie, wyróżnia się zagrożenia militarne i niemilitarne. Wśród zagrożeń niemilitarnych można z kolei wyróżnić zagrożenie polityczne, zagrożenie gospodarcze, zagrożenie ekologiczne, zagrożenie wewnętrzne i inne"[197].

Zagrożenia gospodarcze wyróżniane są jako „rodzaj zagrożenia bezpieczeństwa, w wyniku którego może nastąpić osłabienie potencjału gospodarczego"[198]. Zagrożenia bezpieczeństwa państwa, jak wynika z definicji, jest rozpatrywane w dwóch opcjach: w jednej jest określane przez pryzmat zagrożeń, ich struktury i warunków zaistnienia, możliwości likwidacji lub ograniczenia, w drugiej przez pryzmat ich wpływu na przetrwanie i rozwój kraju. Ze sposobu podejść do zagrożeń reprezentowanych w obu opcjach wynikają istotne wnioski do rozpatrywania barier i zagrożeń bezpieczeństwa ekonomicznego państwa.

Pierwsze nakazuje rozpoznać istotę, źródła i warunki zaistnienia zagrożeń.

---

[195]S. Dworecki, *Zagrożenia*...wyd., cyt., s. 61.
[196]Por. J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa,* ISP PAN, Warszawa 1996, s. 24.
[197]Por. *Słownik terminów z zakresu*...wyd., cyt., s. 163.
[198]Tamże, s. 163.

niebezpieczeństwa kiedy występuje regres gospodarczy lub zbyt niski w stosunku do potrzeb stopień zaspokojenia potrzeb związanych z bezpieczeństwem. Można też stwierdzić, że jest to taka forma istnienia, która nie zapewnia trwania, przetrwania, nie mówiąc o rozwoju.

Dla określenia specyfiki zagrożeń gospodarczych podstaw bezpieczeństwa państwa istotne znaczenie ma także przywołane wcześniej rozumienie zagrożeń w kategoriach „umierania dla innych" lub „życia dzięki śmierci innych". Ten sposób postrzegania zagrożeń jest niezwykle cenny z punktu widzenia ekonomii, ponieważ istotą rynków są właśnie zagrożenia tego typu, a odpowiadającą im formą jest konkurencja. Pozwala to wybrnąć ze sprzeczności pomiędzy stabilizacją, jako jednej i istotnych cech bezpieczeństwa ogólnego i państwa, a konieczną destabilizacją wynikającą z rynkowej konkurencji, wymuszającą przestrzeganie reguł efektywnościowych stanowiących o rozwoju, a więc o bezpieczeństwie ekonomicznym.

Jednak z całą mocą należy podkreślić, że taki sposób postrzegania zagrożeń dla gospodarczych podstaw bezpieczeństwa państwa, może mieć tylko ograniczone zastosowanie. Wynika to z faktu, że kształtowanie tej sfery opiera się głównie na decyzjach politycznych. Dopuszczenie mechanizmu rynkowej alokacji zasobów w obszarze służącym tylko bezpieczeństwu gospodarczych podstaw bezpieczeństwa stanowi tylko np. przetargi na dostarczanie dóbr i usług organizowane przez jednostki wojskowe. Znacznie szerzej wykorzystanie rynkowych mechanizmów jest dopuszczane do obszaru podwójnego zastosowania. Warunkiem tego jest w pewnym zakresie stabilność reguł gry rynkowej (określanych w procesie politycznym), a więc stabilność polityczna (wewnętrzna i zewnętrzna) lub szerzej bezpieczeństwo polityczne państwa.

Zagrożeniem będzie, więc niedostosowanie podmiotów do funkcjonowania i realizacji celów, pod naciskiem konkurencji. Drugą stroną tego stanowiska będzie identyfikowanie zagrożeń z brakiem zmian strukturalnych. Można wręcz stwierdzić, ze nie rzecz w zagrożeniach albo w ich braku, lecz w takim stosunku do nich, który optymalizuje szansę (i pewność) istnienia i prolongowania. Zagrożeniem jest hamowanie wymiany struktur, zarówno sfery realnej, jak i sfery regulacji przestarzałych i nieefektywnych na struktury nowe, sprawniejsze.

i prawdopodobnych działań przeciwnika, skierowanych na osłabienie potencjału obronno – gospodarczego"[200]. Dodaje przy tym ważną uwagę w kwestii identyfikacji zagrożeń mówiąc, że stan bezpieczny cechuje brak zagrożenia lub niski stan napięcia polityczno - militarnego uznany za normalny w dłuższym okresie. Wynika z tego wniosek, że do zagrożeń nie należy zaliczać wszystkich niekorzystnych oddziaływań a jedynie te, które wyraźnie odbiegają od stanu „normalnego". Ten autor nie wyjaśnia czym się charakteryzuje i jaki jest to „normalny stan" napięcia. Można wstępnie oprzeć się na intuicyjnym rozumieniu, tego czym są zagrożenia o niskiej intensywności.

W związku z fragmentarycznym ujęciem zagrożeń bezpieczeństwa ekonomicznego, podejmowane były próby zbudowania definicji całościowej. Taki zamierzony rezultat wydaje się zawierać następująca definicja: „Zagrożenie gospodarcze - stan, w którym państwo nie może przeciwstawić się takim oddziaływaniom zewnętrznym i wewnętrznym, które uniemożliwiają rozwój ekonomiczny zgodny z określonymi kierunkami i tempem, a przez to osłabiają potencjał gospodarczo - obronny"[201]. Jak łatwo zauważyć treść cytowanej definicji odnosi się do zagrożeń wartości, zarówno na płaszczyźnie ogólnoekonomicznej, jak i na płaszczyźnie gospodarczo - obronnej. Ponadto akcentuje, że zagrożenia mogą pochodzić zarówno ze źródeł zewnętrznych jak i wewnętrznych.

Wydaje się zatem, że jest to w miarę pełne, chociaż ogólne określenie istoty zagrożeń bezpieczeństwa ekonomicznego. Łącząc przedstawione stanowiska należy stwierdzić, że zagrożenia gospodarczych podstaw bezpieczeństwa państwa (bezpieczeństwa ekonomicznego państwa) identyfikowane będą z takimi zewnętrznymi i wewnętrznymi procesami, które mogą skutkować brakiem zdolności gospodarki do zaspokajania uzasadnionych potrzeb, lub utratą adekwatności albo pogłębianiem niedopasowania gospodarczych podstaw bezpieczeństwa do sprostania wymogom konfliktów

Opierając się na takim sposobie rozumowania można stwierdzić, że gospodarka i gospodarcze podstawy bezpieczeństwa państwa znajdują się w stanie

---

[200]Por. W. Stankiewicz, *Zagadnienia bezpieczeństwa ekonomicznego a gospodarka obronna*, w: *Bezpieczeństwo ekonomiczne, teoria i praktyka*, Łódź 1986, s. 29.
[201]*Bezpieczeństwo gospodarcze*, Opracowanie zbiorowe, AON, Warszawa 1994, s. 57.

- utraty zdolności do dostarczania wystarczającej ilości dóbr i usług;
- utraty możliwości utrzymania pożądanego poziomu potencjału militarnego i rezerw gospodarczych w czasie pokoju;
- utraty szeroko rozumianego zaplecza w czasie wojny dla wojsk walczących.

Sformułowane kryteria identyfikacji zagrożeń odnoszą się do pewnych dających się przewidywać progów krytycznych w gospodarce i gospodarczych podstawach bezpieczeństwa państwa (w tym jej powiązań z zagranicą), poniżej których naczelne wartości stanowiące o bezpieczeństwie kraju nie będą mogły być realizowane i chronione.

Zaznaczyć jednak należy, że nie wszystkie zjawiska wyrażone ujemnymi wskaźnikami (np. wyrażone spadkiem wydobycia węgla) należy wiązać z kategorią zagrożeń gospodarczych podstaw bezpieczeństwa państwa. Zagrożeniami nie będą te zjawiska i procesy, które przywracają ich adekwatność do zadań i funkcji wynikających ze zmian sposobów realizacji bezpieczeństwa państwa lub oczyszczają ze zbędnych mocy wytwórczych i produktów, pomimo że statystyka odnotuje związany z tym spadek produkcji. Inaczej mówiąc do zagrożeń nie zalicza się tej części zjawisk, dzięki którym dokonują się zmiany jakościowo - strukturalne, podnoszące efektywność i zdolności gospodarczych podstaw bezpieczeństwa do dostarczania odpowiednich dóbr. Warunkiem jest jednak płynne zastępowanie elementów struktury przestarzałej elementami nowoczesnymi. Do zagrożeń ograniczenia swobody nie należy zaliczać decyzji w podejmowaniu decyzji gospodarczo-obronnych wynikających np. umów handlowych czy wchodzenia w skład ugrupowań integracyjnych, jeżeli są one zgodne własnymi preferencjami kraju i suwerennie dokonanego wyboru.

Kształtowanie gospodarczych podstaw bezpieczeństwa kraju - jak wcześniej wskazano jest uwarunkowane, zarówno czynnikami zewnętrznymi jak i wewnętrznymi. Stąd też w zależności od miejsca położenia źródła zagrożenia oddziaływujące na ten podsystem można podzielić na dwie zasadnicze i równorzędne grupy, tj.:

- zagrożenia zewnętrzne;
- zagrożenia wewnętrzne.

Przedstawione sposoby rozumienia zagrożeń gospodarczych podstaw bezpieczeństwa państwa (lub inaczej zwanego - bezpieczeństwa ekonomicznego), za podstawę ich określenia przyjmują zakres czy też poziom realizacji chronionych wartości[202]. Stąd też możliwość utraty tych wartości lub ich niepełna realizacja są łączone z występowaniem zagrożeń, rozumianych jako oddziaływania niosące niepożądane skutki. Istnieje w związku z tym potrzeba określenia tych skutków, aby na tej podstawie stwierdzić czy pojawiły się zagrożenia.

Selekcji zagrożeń z pośród różnorodnych oddziaływań można dokonać tylko na podstawie przyjęcia odpowiednich kryteriów. Dlatego do zagrożeń gospodarczych podstaw bezpieczeństwa państwa (bezpieczeństwa ekonomicznego państwa) przyjęto kryteria zbudowane na podstawie przewidywanych skutków negatywnych oddziaływań, jeżeli kryteria te mają spełniać, funkcję osadnika, w którym w odpowiednim czasie istnieje możliwość pojawienia się destrukcyjnych oddziaływań na gospodarkę. Ponadto określone kryteria są niezbędną podstawą obiektywizacji ocen w analizach bezpieczeństwa państwa. Należy ustalić, przed czym powinno się bronić, a w konsekwencji zdecydować jakie przeciwdziałania podjąć i jakie do tego użyć środki. Trafne decyzje można podjąć tylko na podstawie poprawnie zidentyfikowanych zagrożeń.

Kryteria rozumiane jako zasady wyznaczające sposób osądzania skutków destrukcyjnych oddziaływań na gospodarcze podstawy bezpieczeństwa państwa, wyprowadzane powinny być z nadrzędnego systemu wartości[203]. Zagrożeniami gospodarczego bezpieczeństwa państwa będą te oddziaływania (zjawiska i procesy), które mogą doprowadzić do:

- zahamowania rozwoju gospodarczego lub utraty zdolności rozwojowych;
- pogorszenie pozycji kraju mierzonej udziałem w tworzeniu dochodu narodowego i międzynarodowym nalezytym podziale pracy w stosunku do gospodarek otoczenia zagranicznego;
- utraty swobody (suwerenności) podejmowania decyzji w sprawach gospodarczych i gospodarczo-obronnych oraz ich optymalizacji;

---

[202]Por. J. Świniarski, *O naturze bezpieczeństwa, Prolegomena do zagadnień ogólnych*, Warszawa - Pruszków, 1997, s. 174.

[203]Por. Wł. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych,* Muza S.A. Warszawa 2001, s. 282.

Na płaszczyźnie ekonomiczno - obronnej przedmiotem zainteresowań są zagrożenia gospodarczych podstaw bezpieczeństwa. Można je podzielić - podobnie jak na płaszczyźnie ogólnoekonomicznej na dwie zasadnicze grupy:

- □ zewnętrzne zagrożenia ekonomiczno-obronne;
- □ wewnętrzne zagrożenia ekonomiczno-obronne.

W zależności od położenia źródeł (miejsca) potencjału zagrożeń ekonomiczno-obronnych, można wyróżnić:

- zewnętrzny potencjał zagrożeń ekonomiczno-obronnych;
- wewnętrzny potencjał zagrożeń ekonomiczno-obronnych.

Potencjał zagrożeń ekonomiczno-obronnych może istnieć w różnych formach. Jako przykładowe można wymienić:

- brak alternatywnych źródeł zaopatrzenia gospodarki w surowce lub produkty strategiczne pozyskiwane z zewnątrz;
- brak trwałej współpracy (powiązań) o odpowiedniej skali z przemysłem obronnym krajów w ramach sojuszniczych ugrupowań;
- eliminacja z międzynarodowych rynków uzbrojenia i sprzętu wojskowego;
- struktura i charakter zagranicznych inwestycji w sektory gospodarki, które mają istotne znaczenie dla zapewnienia bezpieczeństwa państwa;
- ograniczenia dostępu do nowoczesnych technologii produkcji i wykorzystania dóbr służących bezpieczeństwu itp.

Obok porządkowania zagrożeń według źródeł i przedmiotu oddziaływań można stosować także inne kryteria klasyfikacji. Dla przykładu - w zależności od charakteru źródeł (impulsu) możliwych destrukcyjnych oddziaływań, czyli sfer z której pochodzą destrukcyjne oddziaływania - wyróżnić można zagrożenia:

- rzeczowe, które mogą powodować negatywne skutki w rozmiarach i strukturze gospodarczych podstaw bezpieczeństwa;
- informacyjne, wywołujące dezorganizację funkcjonowania bądź nietrafne kierunki rozwoju gospodarczych podstaw bezpieczeństwa.

Wewnętrzne zagrożenia i bariery kształtowania bezpieczeństwa państwa w sposób najbardziej syntetyczny znajdują odzwierciedlenie w ograniczeniach tworzenia produktu krajowego brutto. Znajdują one swoją pierwotną przyczynę

Opierając na takim podziale gospodarczy potencjał zagrożeń gospodarczych podstaw bezpieczeństwa, w zależności od położenia (miejsca), można podzielić na dwie grupy:

- zewnętrzny potencjał zagrożeń;
- wewnętrzny potencjał zagrożeń.

Ten potencjał może oddziaływać kanałami powiązań gospodarczych z zagranicą w zakresie przepływów rzeczowych i informacyjnych. Miarą tego potencjału może być wielkość środków możliwych do zaangażowania w celach destrukcyjnych lub wielkość i ważność przepływów środków ekonomicznych, które mogą zostać przerwane. Najważniejsze spośród nich grupują się w przepływach:

- towarów i usług;
- ludzi i kapitałów;
- technologii i sztuki zarządzania.

Z listy istniejących i możliwych do określenia przykładów tego potencjału w odniesieniu do Polski, warto wymienić kilka, takie jak:

- nierównorzędność znaczenia dla siebie partnerów w stosunkach ekonomicznych, co może przejawiać się w formie zależności handlu zagranicznego, technologicznej, kapitałowej, itp.;
- zależność od dostaw (pozyskiwania) istotnych dla funkcjonowania i rozwoju gospodarki czynników, jak np. zależność surowcowo -
- energetyczna od jednego partnera;
- zależność kredytowo-płatnicza, wyrażona brakiem zdolności kraju do obsługi i redukcji zadłużenia zagranicznego bez istotnego obniżenia rozwoju i konsumpcji;
- wymuszone uzależnienie sfery regulacji gospodarki, wyrażone np. koniecznością uzgadniania polityki gospodarczej i gospodarczo-obronnej z międzynarodowymi instytucjami finansowymi;
- wymuszone ograniczenie udziału w międzynarodowej wymianie (eliminacja z rynków) produktów uznanych za „wrażliwe" przez
- najsilniejszych partnerów itp.

zmianami warunków popytu i podaży, spowodowanymi reformą deflacyjną i liberalizacyjną początkujących przekształcenia systemowe, które zmieniały logikę alokacji zasobów. Dlatego ten etap transformacji można określić jako okres urealnienia się podstawowych wielkości ekonomicznych pod wpływem racjonalizacji struktury rzeczowej popytu, a w stosunku do okresu socjalizmu poważnie zmieniła się sektorowa struktura cen. Zmalały względne ceny produkcji rolnej i przemysłu, wzrosty zaś ceny usług. Efektem programu deflacyjnego było natomiast osiągnięcie w latach 1990-91, po raz pierwszy od 40 lat, trwałego zrównoważenia rynku dóbr konsumpcyjnych, zaopatrzeniowych i inwestycyjnych, a dzięki temu wyeliminowanie chronicznych niedoborów towarów. W tym czasie zmieniła się logika kształtowania struktury gospodarki, w której o decyzjach alokacyjnych przesądzały funkcjonalne sprzężenia między preferencjami konsumentów i efektywnym popytem a podażą. Porównując tendencje zmian zaobserwowanych w Polsce i w większości badanych krajów Europy Zachodniej należy stwierdzić, że ukształtowana w naszej gospodarce struktura tworzenia produktu krajowego brutto w 1997 r. charakteryzuje się bardziej korzystnymi proporcjami, o czym świadczą dodatnie odchylenia udziału przemysłu, handlu i usług finansowo-biznesowych.

W 1998 r. doszło do pierwszego, poważniejszego (od 1992 r.) obniżenie tempa wzrostu produktu krajowego brutto. To osłabienie jego dynamiki należy wiązać przede wszystkim z kryzysem finansowym w Rosji, który rozpoczął się w sierpniu 1998 r. i spowodował załamanie się eksportu polskiego na tamten rynek. Świadczy o tym silna zbieżność czasowa między kryzysem rosyjskim a początkiem załamania się polskiego eksportu, zaś wtórnie - także popytu krajowego, w następstwie tego łamania.

W drugim etapie transformacji w Polsce wyraźna była dezagraryzacja i industrializacja, podobnie jak w krajach zachodnich. Trudna jest natomiast interpretacja relatywnego wzrostu usług. Ich wzrost był uwarunkowany niską podstawą wyjściową. w 1998 roku doszło do zahamowania zaobserwowanej od roku 1992 tendencji wzrostowej udziału przemysłu w produkcie krajowym brutto. Jednak istotne odchylenia dodatnie na rzecz udziału usług w tworzeniu produktu

w opóźnieniach rozwojowych polskiej gospodarki w stosunku do gospodarek krajów rozwiniętych, a wyrażają się w dysproporcjach struktury tworzenia produktu krajowego brutto. Jako takie mogą być one jednym z istotnych źródeł zagrożeń bezpieczeństwa ekonomicznego Polski współtworząc gospodarczy potencjał zagrożeń[204] przez, który należy rozumieć skalę (poziom, rozmiary) odstępstw makrostruktury produkcji polskiej gospodarki w okresie transformacji od przyjętej za normę makrostruktury typowej dla gospodarki rynkowej.

Istnienie dużego dystansu i zbyt powolne zbliżanie się do struktury tworzenia produktu krajowego brutto charakterystycznej dla gospodarek rozwiniętych, wyczerpuje znamiona ujęte w kryteriach identyfikacji zagrożeń bezpieczeństwa ekonomicznego, ponieważ skutkują utratą zdolności rozwojowych (w pożądanym tempie) i pogorszeniem pozycji polskiej gospodarki w międzynarodowym podziale pracy.

Współczesna struktura polskiej gospodarki, pomimo dokonujących się zmian, wzrosła ze struktury odziedziczonej po PRL i jest w pewnym zakresie posiada jej wady. Jednak ocena jej struktury według porównywalnych kryteriów napotyka poważne trudności metodologiczne i statystyczne. Była to typowa gospodarka ograniczona przez wielkość zasobów, pomimo istnienia dość znacznego obszaru własności prywatnej w porównaniu do innych krajów realnego socjalizmu. Do cech charakterystycznych poprzedniego systemu gospodarczego należał brak funkcjonalnych sprzężeń między trzema kluczowymi kategoriami ekonomicznymi: preferencjami konsumentów, efektywnym popytem a podażą. Tak więc struktura rzeczowa popytu była dwojako zdeformowana: bezpośrednio w strukturze wewnętrznej popytu oraz pośrednio - wskutek nadmiernych jego rozmiarów globalnych[205]. Ponadto struktura rzeczowa podaży nie była dostosowana nawet do zniekształconej już struktury popytu efektywnego, ponieważ istniała chroniczna nierównowaga w sferze produkcji i nie było barier popytu finalnego.

W pierwszym etapie transformacji w strukturze wewnętrznej produktu krajowego brutto zaszły istotne przekształcenia. Były one wywołane zasadniczymi

---

[204]Zob. A. Lipowski, *Zmiany w strukturze tworzenia PKB w Polsce w okresie transformacji 1990-97/98. Analiza i ocena,* w: *„Ekonomista"* 1999 nr 5, s. 565.
[205]Por. A. Lipowski, *Zmiany w strukturze*...wyd. cyt., s. 568.

Serwicyzacja to przesuwanie działalności gospodarczej firm, zakładów przemysłowych, koncernów na świadczenie usług. Serwicyzacja dotyczy zwykle: zarządzania, przemysłu teleinformatycznego, nowych technologii, ochrony środowiska itp. To właśnie serwicyzacja gospodarki najczęściej powoduje początkową stabilizację udziału przemysłu w produkcie krajowym brutto, a później jego względny spadek.

Z przedstawionych zmian strukturalnych wynika, że tendencję do dezindustrializacji i serwicyzacji gospodarki wykazały relatywnie później rozwinięte kraje Europy Zachodniej. W związku z tym można przypuszczać, że gdyby gospodarka Polski miała dalej iść śladem krajów Europy Zachodniej w procesie przemian makrostrukturalnych, to powinna rozpocząć dezindustrializację i autentyczną serwicyzację jeszcze szybciej niż później rozwinięte gospodarki zachodnioeuropejskie. Proces transformacji z istoty swej polega bowiem na przyspieszonym, w porównaniu z krajami zachodnimi, przekształceniu się gospodarki w całkowicie rynkową.

Relatywna dynamika przemysłu w Polsce w drugim etapie transformacji przebiega nieco szybciej niż kilkadziesiąt lat temu w Europie Zachodniej. Zdaje się to potwierdzać przypuszczenie, że punkt nasycenia gospodarki przemysłem na rzecz serwicyzacji może być w Polsce osiągnięty przy relatywnie niższym produkcie krajowym brutto na jednego mieszkańca niż to było w Europie Zachodniej. W tym celu musi się rozpocząć ekspansja takich usług, jak: transport, telekomunikacja, informatyka wraz z ponowną ekspansją pośrednictwa finansowego w miarę szybkiego wzrostu produktu krajowego brutto na jednego mieszkańca.

Wiodącymi przyczynami dokonujących się zmian w strukturze polskiej gospodarki, były przede wszystkim skutki reform deflacyjnej i liberalizacyjnej. Natomiast po to, ażeby widoczne były owoce zmian w postaci ekspansji produkcji konkurencyjnej w skali międzynarodowej, muszą być przyspieszone reformy instytucjonalne - systemowe. Dotychczasowe efekty produkcyjne ciągle stanowią bowiem w większym stopniu skutki historycznie pierwszych dwóch reform niż

---

[208]Proces ten jest dodatkowo pobudzany przez przerzucanie przez kraje rozwinięte części przemysłu do krajów rozwijających się.

krajowego brutto w Polsce, w porównaniu do odpowiedniego stadium rozwoju Europy Zachodniej, oznacza, że nasza gospodarka weszła na ścieżkę serwicyzacji.

Na podstawie analizy dostępnej literatury i argumentów empirycznych można stwierdzić, że w miarę rozwoju gospodarczego najpierw obniżają się udziały rolnictwa i rosną udziały przemysłu w gospodarce, później spadają udziały przemysłu, zwiększają się natomiast relatywnie usługi rynkowe. Powstały koncepcje tzw. społeczeństwa postindustrialnego, które wykorzystywano m.in. w formułowaniu długoterminowych prognoz rozwoju gospodarki zachodniej. W makrostrukturze produkcyjnej wielu krajów Europy Zachodniej wystąpiły następujące zjawiska[206]: ***dezagraryzacja, industrializacja, stabilizacja udziału przemysłu w tworzeniu produktu krajowego brutto, dezindustrializacja oraz serwicyzacja.***

Dezagraryzacja stanowi uniwersalną, ponadustrojową prawidłowość strukturalną każdej gospodarki. Wynika to:

- z rolniczego charakteru każdej gospodarki w punkcie startu do rozwoju;
- z naturalnych barier ekspansji produkcji rolniczej (ziemia), która w przeciwieństwie do działów pozarolniczych może w dłuższym czasie wzrastać wyłącznie przez intensyfikację;
- w miarę wzrostu zamożności społeczeństwa - ze stopniowego przesuwania się popytu z dóbr żywnościowych na dobra przemysłowe, a następnie na usługi (rynkowe).

Industrializacja oznacza wypieranie z gospodarki sektora rolniczego. Można zatem powiedzieć, że w punkcie startu każda gospodarka ma niewielki przemysł, który w przeciwieństwie do rolnictwa może ekstensywnie, wzrastać[207].

Stabilizacja udziału przemysłu w produkcie krajowym brutto oznacza, że gospodarka osiągnęła pułap swego nasycenia przemysłem.

Dezindustrializacja oznacza to, że nasycenie przemysłem zaczyna się zmniejszać wtedy gdy wypierają go inne bardziej dynamicznie rozwijające się sektory (pozarolnicze)[208].

---

[206]Tamże, s. 590.

[207]Przykładem wykorzystania ekstensywnego wzrostu przemysłu była gospodarka PRL, która nasyciła kraj przemysłem znacznie ponad rynkowe standardy zachodnioeuropejskie, to jednak z poważnym naruszeniem makroproporcji produkcyjnych.

nieskutecznego kształtowania stosunków gospodarczych z zagranicą. Przyczyny mogą tkwić także w kształtowaniu się uwarunkowań zewnętrznych, a zwłaszcza w przebiegu koniunktury gospodarczej w krajach zewnętrznego otoczenia gospodarczego a także w pojawianiu się ograniczeń i barier wymiany na rynkach zagranicznych.

2.3. Analiza i ocena wpływu infrastruktury telekomunikacyjnej na kształtowanie bezpieczeństwa ekonomicznego na przełomie wieku

2.3.1. Analiza wpływu infrastruktury telekomunikacyjnej na kształtowanie bezpieczeństwa ekonomicznego Polski

Wielu obserwatorów opisuje dzisiejszą globalną gospodarkę jako przekształcającą się w gospodarkę opartą na wiedzy, bazującą na produkcji i dystrybucji jej produktów. Naczelną cechą nowej gospodarki jest - będzie w najbliższej przyszłości - kluczowa rola wiedzy jako zasobu wytwórczego. Waga wiedzy wynika z faktu, że to jej potencjał decyduje o zdolności do absorpcji innowacji zarówno w odniesieniu do przedsiębiorstw, jak i całych społeczeństw. Nie bez przyczyny zamiennie do określenia gospodarka oparta na wiedzy stosuje się również określenie *społeczeństwo informacyjne,* aby wyrazić charakter dokonujących się zmian. Rozpatrywane w skali globalnej przesunięcie od społeczeństwa przemysłowego do informacyjnego, dokonuje się bowiem głównie w wyniku oddziaływania technologii związanych z przetwarzaniem informacji, które rozumiane jest jako materialna konkretyzacja wiedzy (mikroelektronika, komputery, robotyka, telekomunikacja, biotechnologia) radykalnie zmieniają gospodarkę trzeciego millennium.

Początkiem nowego etapu na drodze do społeczeństwa informacyjnego i elektronicznej gospodarki było pojawienie się i rozwój transportu morskiego oraz kolejowego. Nowe możliwości ułatwiły transport coraz istotniejszych dla rozwoju cywilizacji dóbr, takich jak ropa naftowa, węgiel czy rudy metali. Znaczenie żywności jako towaru podstawowego zmalało na rzecz surowców naturalnych. Wynalezienie telefonu zmieniło sposób organizacji procesów biznesowych umożliwiając dokonywanie działań bez opóźnienia czasowego i konieczności bezpośredniego kontaktu. Zmiany, które zaszły w tym okresie były tak poważne, że określa się je mianem rewolucji przemysłowej. Kolejną fazę społeczno-ekonomiczną zawdzięczamy rozwojowi transportu samochodowego, pojawienia się

zaawansowanych reform instytucjonalno - systemowych. Te reformy powinny także przyczynić się do intensywniejszego rozwoju sfery usług edukacyjno – naukowych, finansowo - ubezpieczeniowych, informacyjnych i telekomunikacyjnych[209]. Może to spowodować w przyszłości ustabilizowanie udziału przemysłu, a następnie rozpoczęcie procesu dezindustrializacji. Byłby to dowód, że gospodarka Polski osiągnęła już strukturalną dojrzałość podobną do rozwiniętych krajów Europy Zachodniej. Podsumowując dokonane rozważania wewnętrznych zagrożeń gospodarczych podstaw bezpieczeństwa państwa, należy stwierdzić, że dokonujące się w tej dziedzinie zmiany prowadzą do ich pomniejszenia. Ta korzystna tendencja przejawia się poprzez procesy prowadzące do upodobniania się struktury tworzenia produktu krajowego brutto do analogicznej struktury krajów Europy Zachodniej. Bezwzględne pomniejszenie gospodarczego potencjału zagrożeń w strukturze gospodarki, ograniczy zagrożenia bezpieczeństwa gospodarczego Polski, polegające na możliwości utraty zdolności gospodarki do rozwoju.

Zagrożenia dla bezpieczeństwa ekonomicznego Polski wynikają również z międzynarodowych stosunków gospodarczych, które to oprócz korzyści płynących z międzynarodowego podziału pracy i międzynarodowego obrotu gospodarczego, kreują także zewnętrzny potencjał zagrożeń gospodarczych. Może być on określany na różnych poziomach, a także w różnych układach podmiotowych i przedmiotowych. Najbardziej ogólnym sygnałem pojawienia się źródeł i potencjału istotnych zagrożeń bezpieczeństwa ekonomicznego Polski jest brak równowagi w wymianie gospodarczej z zagranicą (deficyt), a także jej struktura.

Przejawem powstania zewnętrznego potencjału zagrożeń bezpieczeństwa ekonomicznego kraju, jak uprzednio wspomniano, jest deficyt obrotów bieżących bilansu płatniczego kraju na poziomie uznanym za niebezpieczny. Powstanie i utrzymywanie się tego deficytu na poziomie uznanym za niebezpieczny najczęściej jest rezultatem nieodpowiedniego przebiegu wewnętrznych procesów rozwojowych i sytuacji gospodarczej, a także przejawem niewłaściwego bądź

---

[209]Por. A. Lipowski: *Zmiany w strukturze...*, wyd. cyt., s. 594.

Zdobywanie informacji do momentu upowszechnienia się Internetu sprowadzało się do zapoznawania się z publikacjami tradycyjnymi oraz do przekazów ustnych. Te opcje w poważny sposób ograniczają możliwości poszerzania swojej wiedzy.

Internet nie tylko w sposób znaczny ułatwia zdobycie konkretnej publikacji z księgozbiorów największych księgarni na całym świecie, lecz również poprzez usługę WWW pozwala na poszerzanie wiedzy o tematy nie poruszane w literaturze. Może to być spowodowane np. małą popularnością poszukiwanych informacji. Oprócz tych udogodnień Internet pozwala na otrzymywanie odpowiedzi na konkretne zapytania, gdy potencjalnemu użytkownikowi potrzebny jest fragment informacji nie wymagający zagłębiania się w dany temat. Do takich działań jesteśmy w Internecie niejednokrotnie zachęcani poprzez umieszczanie na stronach adresów ich autorów z dodatkowym tekstem np. : „Jeśli masz jakieś pytania napisz do nas".

Wymienione możliwości zdobywania informacji powodują większą indywidualizację wśród członków społeczeństwa informacyjnego, która wynika z różnorodności charakterów i zainteresowań ludzkich. Ludzie korzystający z Internetu są bogatsi o sobie tylko właściwą wiedzę. Nie bez znaczenia są również metody komunikacji poprzez tematyczne fora dyskusyjne, gdzie bez niepotrzebnych wstępów możemy przejść do interesujących nas kwestii i udzielić oraz otrzymać odpowiedzi od osób, które podobnie jak my zajmują się tematami dotyczącymi naszych zapytań.

Internet i poczta elektroniczna umożliwiają współpracę różnych grup roboczych zajmujących się problemami przemysłu i technologii, dzięki wykorzystaniu tych technologii, które już posiadają. Taka współpraca dostarcza możliwości zmiany nawet najbardziej krytycznych technologii o znaczeniu narodowym, poczynając od epizodycznego wykonywania sprawozdań w ramach prowadzonych przedsięwzięć, aż do precyzyjnych rozważań dotyczących zagadnień uzasadniających społeczne korzyści, jakie może przynieść określony projekt, dodając impetu jego wykonawcom.

Internet jest odpowiednim do tego narzędziem, niegdyś, na początku swego istnienia, zapewniał kontakt w sieci, łącząc naukowców zajmujących się rozwijaniem technologii. Dzisiaj może też służyć do rozwiązywania narodowych

samolotów oraz faksów, a co za tym idzie możliwości przesyłania dokumentów na odległość. Umożliwiło to tranzyt bardziej dostosowany do potrzeb odbiorców niż np. kolej. Gospodarka zaczęła koncentrować się na dobrach konsumpcyjnych i usługach. Rozważania te pozwalają na implikację, że nowe środki szeroko rozumianego przesyłu doprowadzają do zmian gospodarczych oraz społecznych.

Internet i inne media elektroniczne wprowadziły nas więc w nową epokę, nowy etap rozwoju. Po społeczeństwach agrarnym, industrialnym i postindustrialnym pojawia się społeczeństwo informacyjne. Podstawowym towarem jest tu produkt cyfrowy, czyli informacja (dokumenty, pieniądze, informacje o środkach finansowych, utwory autorskie oraz oprogramowanie), a cechami nowej rzeczywistości są: szeroki dostęp do informacji i usług, możliwość interakcji i swobodnego operowania danymi, w szczególności przeprowadzenia rozmaitych operacji na odległość w dowolnej chwili i z dowolnego punktu na Ziemi. Granice cywilizowanego świata wyznaczają dziś punkty funkcjonowania układu telekomunikacyjnego. Jakie są więc różnice pomiędzy społeczeństwem tradycyjnym, a społeczeństwem informacyjnym:

- kontakt bezpośredni i pokonywanie barier przestrzennych;
- możliwość zdobywania informacji oraz docierania z nią do niemal nieograniczonego grona osób.

W społeczeństwie informacyjnym człowiek ograniczony jest brakiem kontaktu fizycznego i wzrokowego ze swoim rozmówcą. Wyklucza to pozawerbalne możliwości kontaktu jak język ciała w postaci mimiki i gestów. W przestrzeni informacyjnej zostały one zastąpione przez słowa, znaki, symbole co wymusza na członku takiej społeczności nauczenia się nowych sposobów komunikacji. Osobowość tworzona jest na podstawie elektronicznych wypowiedzi. Taka sytuacja ma swoje oczywiste wady (ograniczenia w komunikacji, przyzwyczajenie do prowadzenia dyskusji bezpośredniej, twarzą w twarz), ale jednocześnie ma również zalety, a podstawą jest brak wzajemnych uprzedzeń, które są nie do uniknięcia w tradycyjnych społecznościach. Powoduje to, że grupy ludzi w społeczności informacyjnej są bardziej otwarte na nowe osoby i poglądy niezależnie od ich pochodzenia rasowego, kulturowego, religijnego itp. W społecznościach informacyjnych zanika w sposób realny zjawisko nietolerancji.

konkretnych projektów owocuje w postaci nabywanych doświadczeń, rozwoju cech przywódczych oraz uczy pracy w grupie. Interdyscyplinarne zespoły, złożone z osób których kompetencje nawzajem się uzupełniają rezonują dogłębnym zrozumieniem tematu, a w sferze kontaktów biznesowych pełnym, efektywnym zaprojektowaniem i realizacją zadania.

W szybko zmieniającej się rzeczywistości dotychczas uznawane zasady i praktyka działania dominujące w gospodarce przemysłowej ubiegłego wieku muszą zostać zweryfikowane. W świecie pojawiających się nowych, wzajemnych uwarunkowań gospodarczych, w którym zasoby typu know-how uzyskują coraz większe znaczenie w odniesieniu do innych zasobów gospodarczych, potrzebna jest nowa strategia funkcjonowania państwa, obejmująca różne sfery jego działania. Nowe wyzwania stawiają szczególne wymagania wobec teorii i praktyki kształtowania systemu bezpieczeństwa narodowego. Trudność w poszukiwaniu rozwiązań w tym zakresie, polega na konieczności jednoczesnego rozpatrywania wielu składowych podejmowanych działań społecznych: gospodarczych, politycznych i militarnych kierowanych interesem narodowym; ich wpływu na stan bezpieczeństwa państwa i uwzględniania wyzwań zmieniającej się rzeczywistości.

Wśród wielu rozpatrywanych czynników, gwałtowny rozwój technologii informacyjnych i wynikające z tego konsekwencje wymagają szczególnej uwagi, gdyż stanowią istotny obszar uwarunkowań, od których zależą możliwości kształtowania bezpieczeństwa narodowego. Przekonanie o zasadności tego stwierdzenia wynika chociażby z pobieżnej analizy obserwowanych kierunków rozwoju techniki teleinformatycznej i mediów, wyznaczających przyszłe zmiany struktury systemu społecznego działania.

Jednak niekwestionowanym pozostaje fakt, że w dobie społeczeństwa informacyjnego rozwój teleinformatyki a szczególnie infrastruktury telekomunikacyjnej powoduje określone skutki - zmiany w strukturach działania narodu, które pośrednio lub bezpośrednio wpływają na bezpieczeństwo państwa, gdyż przez szeroką wymianę informacji mają możliwości wrogich działań, tworząc zagrożenia jego ekonomicznego bezpieczeństwa oraz decydują o wielkości zasobów, jakimi może dysponować naród, aby przeciwstawić się temu niebezpieczeństwu.

problemów dotyczących stanu kondycji i kierunków rozwoju bazy technologicznej. Obecnie nawet najbogatsze państwa nie mogą pozwolić sobie na finansowanie wszystkich inicjatyw naukowych. Powstaje konieczność wyboru, a podejmowane decyzje wymagają czytelnego sformułowania priorytetów wynikających z polityki państwa w zakresie prowadzenia badań i rozwoju, które z kolei muszą być pochodną strategii gospodarczej i społecznej oraz współczesnego stanu nauki i techniki[210].

Społeczeństwo informacyjne, jako etap ewolucji sposobu istnienia jednostek w grupie, wykształca nowe horyzonty w świecie prowadzenia biznesu. Kwartalność - a więc przejście z epoki postindustrialnej do następnej, wyższej formy rozwoju społecznego, identyfikuje zmieniające się wymagania realizacji przedsięwzięć, w kluczowym punkcie stawiając osobowość profesjonalisty i jego wiedzę.

Serwicyzacja w segmencie dóbr wykształcanych przez rynek powoduje rewaloryzację posiadanych, stałych przez epoki, aktywów firmy. Wartościami nadrzędnymi stają się, wiedza zarówno w ujęciu przedmiotowym - bazy danych wraz z bazami klientów, jak podmiotowym, skupiająca się na człowieku - będącym członkiem organizacji i jego osobowości. Zapotrzebowanie na kreatywne postawy jak też zróżnicowanie życia na tym samym poziomie dochodów wykształca nowy rodzaj istnienia. Byt staje się wyraźniej zarysowany, jego największą zaletą jest teraz unikalny portfel umiejętności oraz możność wykorzystania nabytej wiedzy w praktyce. Zapotrzebowanie na usługi profesjonalne, a więc te ukierunkowane na obsługę biznesu wykreślają nowe płaszczyzny prestiżu, na najwyższych pozycjonując tzw. wolne zawody, a więc profesjonalistów.

Nowa filozofia prowadzenia biznesu staje się szansą dla ludzi. Poprzez zapał i chęć pomnażania wiedzy mają oni możliwość sprawdzenia swoich możliwości. Teoria w konfrontacji z codziennością zagadnień biznesowych pozwala na selekcję wiedzy oraz wczesną specjalizację. Z drugiej strony, łatwy dostęp do źródeł informacji jak też mnogość form, w której wiedza ta występuje, ze szczególnym uwzględnieniem nowego kanału – Internetu, pozwala na równomierne kształtowanie się osobowości w oparciu o rozwój intelektualny. Realizacja

---

[210]Por. T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne*...wyd. cyt., s. 71-75.

- uszkodzeń linii wysokiego napięcia, innych awarii zasilania itp.;
- fali uderzeniowej, impulsu elektromagnetycznego i promieniowania radioaktywnego będącego skutkiem katastrofy urządzeń jądrowych.

b) oddziaływań losowych w wyniku niecelowych działań ludzkich:

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

c) oddziaływań celowych:

- dywersji prowadzonej przez grupy zainteresowane zniszczeniem elementów systemu obronnego;
- próby programowego przekonfigurowania elementów sieci telekomunikacyjnych i komputerowych;
- próby ataku na system zabezpieczenia poufności informacji.

Elementy systemu telekomunikacyjnego państwa są rozmieszczone na całym terytorium Polski i w zależności od ich położenia może zaistnieć różne destrukcyjne oddziaływanie na nie w wyniku oddziaływań losowych, klęsk żywiołowych i ekologicznych. Natomiast oddziaływanie środków rażenia przeciwnika będzie uzależnione od wagi celu. W każdym wypadku najbardziej narażony jest system kierowania obronnością państwa, a w nim system łączności, szczególnie infrastruktura telekomunikacyjna, przeznaczona dla organów administracji państwowej odpowiedzialnych za funkcjonowanie państwa w czasie klęsk żywiołowych i ekologicznych, kryzysu oraz wojny. Z tego powodu należy uwzględnić odporność całego systemu łączności na uszkodzenia w wyniku oddziaływania różnorodnych zagrożeń zewnętrznych.

Podstawą działalności w zakresie przygotowania sieci telekomunikacyjnej użytku publicznego do wykonania zadań w okresie szczególnych zagrożeń są odpowiednie akty normatywne. W czasie pokoju na system telekomunikacyjny może zaistnieć destrukcyjne oddziaływanie (poza naturalnymi uszkodzeniami wynikającymi z niedoskonałości sprzętu) w wyniku :

a) oddziaływań niecelowych (np.: powodzi, pożarów, rozprzestrzeniania się przemysłowych środków trujących itp.);

2.3.2. Ocena wpływu infrastruktury telekomunikacyjnej na kształtowanie bezpieczeństwa ekonomicznego

Współczesny rozwój społeczeństw charakteryzuje się intensywnym postępem naukowo-technicznym, szybkim przyrostem ludności świata i coraz większą presją, wywieraną przez ludzkość na środowisko życia, w tym i na przyrodę. Każdy człowiek i każda społeczność żyje w otoczeniu i świadomości (lub nieświadomości) zagrożeń pochodzenia naturalnego i antropogenicznego. Otacza nas ogromna liczba różnego rodzaju zagrożeń o nieznanym, przeważnie jednak małym prawdopodobieństwie wystąpienia i trudnych do przewidzenia skutkach. O wielu z nich nie zdajemy sobie nawet sprawy. Nie ma w środowisku, zarówno cywilizacyjnym, jak i przyrodniczym sytuacji „ryzyka zerowego" i nic co związane jest z produkcją, przetwarzaniem, transportem i magazynowaniem nie dzieje się w stu procentach bezpiecznie. Postęp cywilizacyjny, nowe technologie, osiedlanie się ludzi w miejscach uznawanych dawniej za niebezpieczne (jak doliny zalewowe rzek) powoduje, że społeczeństwo staje się coraz bardziej narażone na różnego rodzaju nagłe zagrożenia.

Ochrona ludzi i mienia narodu oraz państwa przed zagrożeniami jest konstytucyjnym obowiązkiem wszystkich organów władzy, administracji państwowej i samorządowej, a także obowiązkiem organizacji społecznych i podmiotów gospodarczych. Zadania wynikające z tego obowiązku polegają głównie na rozpoznawaniu, zapobieganiu i zwalczaniu wszelkich form zagrożeń godzących w bezpieczeństwo narodu i państwa. W czasie pokoju elementy infrastruktury telekomunikacyjnej państwa mogą być niszczone (poza naturalnymi uszkodzeniami wynikającymi z niedoskonałości sprzętu) w wyniku:

a) oddziaływań losowych środowiskowych:

- powodzi;
- katastroficznych zatopień;
- pożarów;
- trzęsień i tąpnięć Ziemi (w Polsce występują rzadko i o słabej sile);
- rozprzestrzenienia się przemysłowych środków trujących;
- eksplozji gazów lub pyłów;
- wyładowań atmosferycznych;

Ze względu na przestrzenne rozmieszczenie elementów systemu telekomunikacyjnego, rozkład zagrożeń infrastruktury telekomunikacyjnej będzie bardzo nierównomierny, w tym przede wszystkim węzłów i linii sieci łączności, a to spowoduje wzrost uodpornienia. W trakcie zmian stanów gotowości obronnej państwa zacznie narastać stopień oddziaływań zewnętrznych dezorganizujących system łączności (np. niszczenie, rozpoznanie i obezwładnianie radioelektroniczne), który będzie maleć w czasie konfliktu wskutek wyczerpywania się potencjałów walczących stron. Rejony największych prawdopodobnych zagrożeń w konfliktach lokalnych lokują się przede wszystkim w rejonach przygranicznych szczególnie na wschodnich obszarach kraju (Mapa 2.5.).

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

a) oddziaływania niszczące - bronią konwencjonalną (w tym precyzyjną);
b) oddziaływania niszczące - bronią masowego rażenia:
   - bronią chemiczną;
   - bronią biologiczną;
   - bronią jądrową - zniszczenia fizyczne, promieniowanie radioaktywne i impuls elektromagnetyczny;
c) oddziaływanie radioelektroniczne.

Natężenie uszkodzeń systemu łączności, z wymienionych powodów można oszacować tylko za pomocą metod statystycznych. Uodpornienie na te zagrożenia będzie polegać na uruchomieniu określonych działań organizacyjno-technicznych. Można analizować skutki oddziaływania punktowego, skutki oddziaływania przestrzennego oraz prawdopodobieństwo - na jakim obszarze (rejonie) dane zagrożenia punktowe bądź przestrzenne mogą wystąpić najczęściej. Podstawą do analizy mogą być charakterystyki poszczególnych zagrożeń. W tym celu należy określić obszary, rejony o podwyższonym prawdopodobieństwie zaistnienia uszkodzeń i stopień możliwych zniszczeń od każdego z tych czynników. W sytuacjach szczególnych zagrożeń państwa mogą wystąpić zniszczenia fizyczne.

Największe prawdopodobieństwo zniszczeń może wystąpić w rejonach: przemysłu zbrojeniowego, węzłów i ważnych tras komunikacyjnych, ośrodków administracyjnych, węzłów telekomunikacyjnych, zgrupowań sił obronnych itd.

b) oddziaływań losowych w wyniku niecelowych działań ludzkich (np. błędów użytkowników i personelu powodujących awarie, uszkodzenia, skasowania zbiorów, przekonfigurowanie systemu itp.);

c) oddziaływań celowych (np. działań terrorystycznych, przestępstw kryminalnych; dywersji, próby nielegalnego wykorzystania danych itp.).

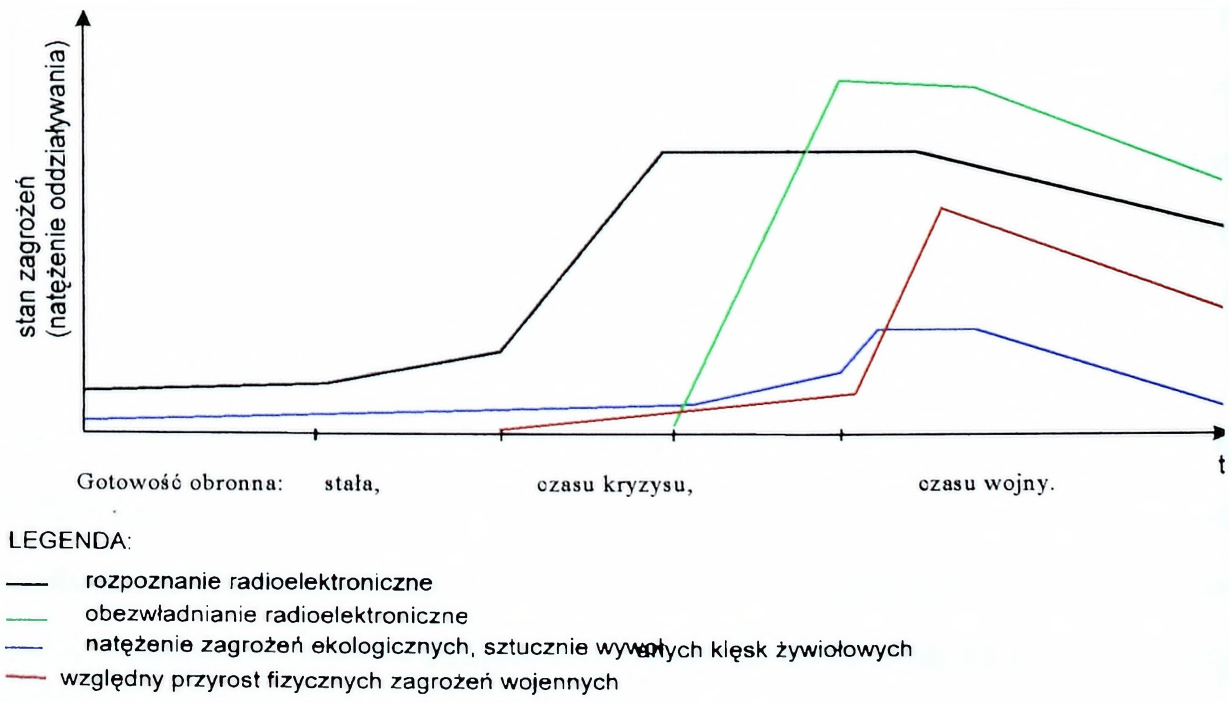
W czasie sytuacji kryzysowych i wojny zagrożenia już wymienione mogą się nasilić, a ponadto mogą wystąpić oddziaływania niszczące:

- bronią konwencjonalną (w tym precyzyjną);
- oddziaływania bronią masowego rażenia;
- wzmożone oddziaływanie radioelektroniczne.

Przygotowanie sieci telekomunikacyjnej przed zagrożeniami polega na zapewnieniu pożądanego stopnia jej żywotności w warunkach oddziaływania środków rażenia oraz zwiększonego prawdopodobieństwa wystąpienia klęsk ekologicznych. Żywotność tę osiąga się poprzez zabiegi uodporniające oraz sprawne odtwarzanie zniszczonego potencjału. Każdy z elementów systemu może być niszczony przez oddziaływanie zewnętrzne. Sieci telekomunikacyjne w okresie konfliktu zbrojnego mogą ulegać licznemu zbiorowi zagrożeń (Wykres 2.15.).

Wykres 2.15.

Zagrożenia sieci telekomunikacyjnej w okresie konfliktu zbrojnego



Źródło: W. Gawlikowski, M. Szaliłow, *Zagrożenia stacjonarnego systemu telekomunikacyjnego w czasie klęsk ekologicznych, katastrof i wojny.* w: „Zeszyty Naukowe AON" 1997 nr 3, s. 87.

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

Ścisłe określenie (przewidzenie) skutków jest trudne do określenia, zależne od wielu czynników tłumiących powodujących zmniejszenie zaindukowanego impulsu napięciowego. Wiadomo jednak, że wspomniany wybuch uszkodzi np. mikrokomputery nie zabezpieczone na odległość kilkuset kilometrów i więcej od epicentrum wybuchu. Na przykład wybuch jądrowy o sile 1Mt na wysokości 100 km spowoduje trwałe uszkodzenia aparatury elektronicznej w promieniu do 1000 km i drobne - w promieniu do 2000 km.

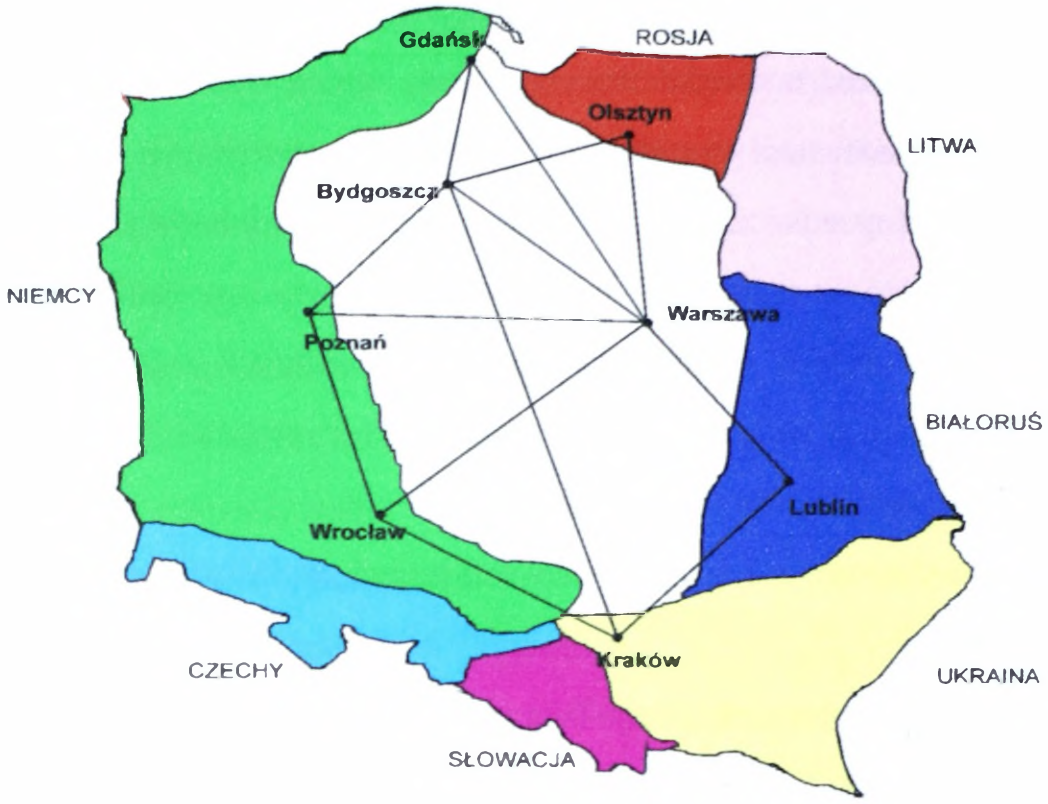
Oddziaływanie radioelektroniczne obejmie głównie najważniejsze dla systemu obronnego państwa węzły telekomunikacyjne oraz elementy łączności, rozpoznania i kierowania środkami walki sił zbrojnych.

W czasie pokoju, kryzysu i wojny może oddziaływać szereg czynników, z których najistotniejsze to oddziaływanie żywiołów lub klęsk żywiołowych:

a) powodzie, które nie występują nagle, można je wcześniej przewidzieć (od kilku godzin do kilku tygodni) i podjąć odpowiednie decyzje. Najczęściej występujące rodzaje powodzi:
   - opadowe (długotrwałe deszcze);
   - roztopowe (gwałtowne topienie śniegów);
   - zimowe (w wyniku zatorów lodowych);
   - sztormowe.

b) zatopienia katastroficzne występują w wyniku uszkodzenia (awarii) tam, zapór, wałów przeciwpowodziowych, śluz, stopni spiętrzających, jazów itp. Skutkiem tych awarii jest gwałtowne wylanie ogromnych ilości wody w bardzo krótkim czasie na tereny położone poniżej miejsca awarii.

Mapa 2.5. Tereny o największym prawdopodobnym zagrożeniu w konfliktach lokalnych



Legenda:

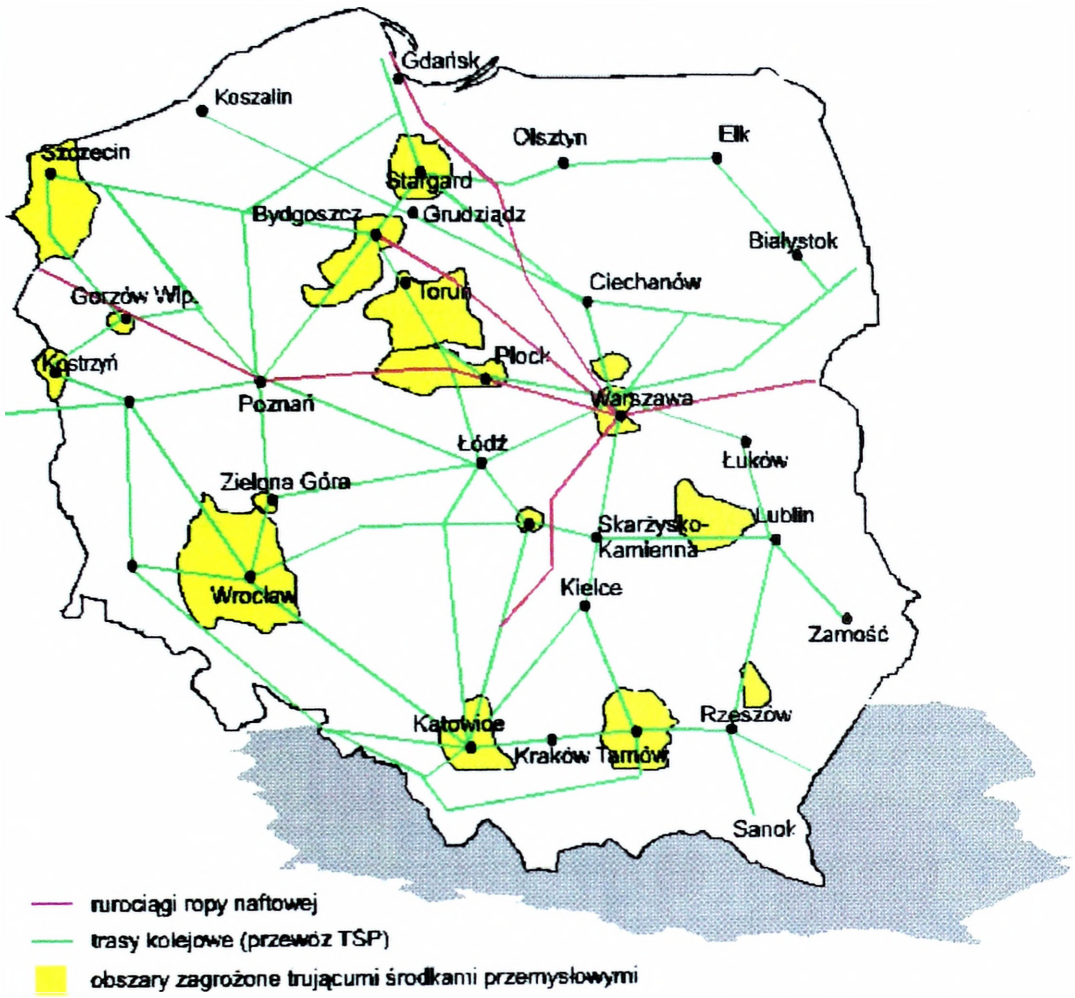
- obszar zagrożeń w konflikcie z Niemcami;
- obszar zagrożeń w konflikcie z Rosją;
- obszar zagrożeń w konflikcie z Litwą;
- obszar zagrożeń w konflikcie z Białorusią;
- obszar zagrożeń w konflikcie z Ukrainą;
- obszar zagrożeń w konflikcie z Słowacją;
- obszar zagrożeń w konflikcie z Czechami;
- linie łączności.

Źródło: W. Pokruszyński i inni. *System bezpieczeństwa publicznego Polski.* AON, Warszawa 1995, s. 23.

Jednym z możliwych zagrożeń wszelkich systemów wyposażonych w technikę elektroniczną jest impuls elektromagnetyczny wybuchu jądrowego. W wyniku wybuchu jądrowego powstaje promieniowanie gamma oraz rentgenowskie - X. Fale gamma oraz X powodują powstanie impulsowego pola elektromagnetycznego o bardzo dużych wartościach szczytowych, sięgających około 200A/m dla pola magnetycznego i 50 - 60 kV/m dla pola elektrycznego. Największy zasięg tego typu zjawiska występuje przy wybuchu powietrznym na wysokości rzędu 100 km, a impuls elektromagnetyczny trwa około 500 nanosekund.

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

Mapa 2.7. Obszary kraju zagrożone trującymi środkami przemysłowymi



Źródło: W. Pokruszyński i inni. *System bezpieczeństwa publicznego Polski.* AON, Warszawa 1995, s. 43.

W wyniku zestawienia najbardziej prawdopodobnego zaistnienia omawianych poprzednio poszczególnych zagrożeń sporządzona została ich mapa (Mapa 2.8.). Na jej tle rozmieszczono fragmenty elementów infrastruktury telekomunikacyjnej, niektóre linie i węzły łączności. Z obrazu, które one tworzą widać, że największe zagrożenia dla linii i węzłów łączności występują w wyniku oddziaływania klęsk żywiołowych i ekologicznych (z wyjątkiem Lublina i Olsztyna), natomiast tylko Poznań i Olsztyn są w strefie niewielkich zagrożeń spowodowanych zniszczeniami w wyniku lokalnego konfliktu zbrojnego.

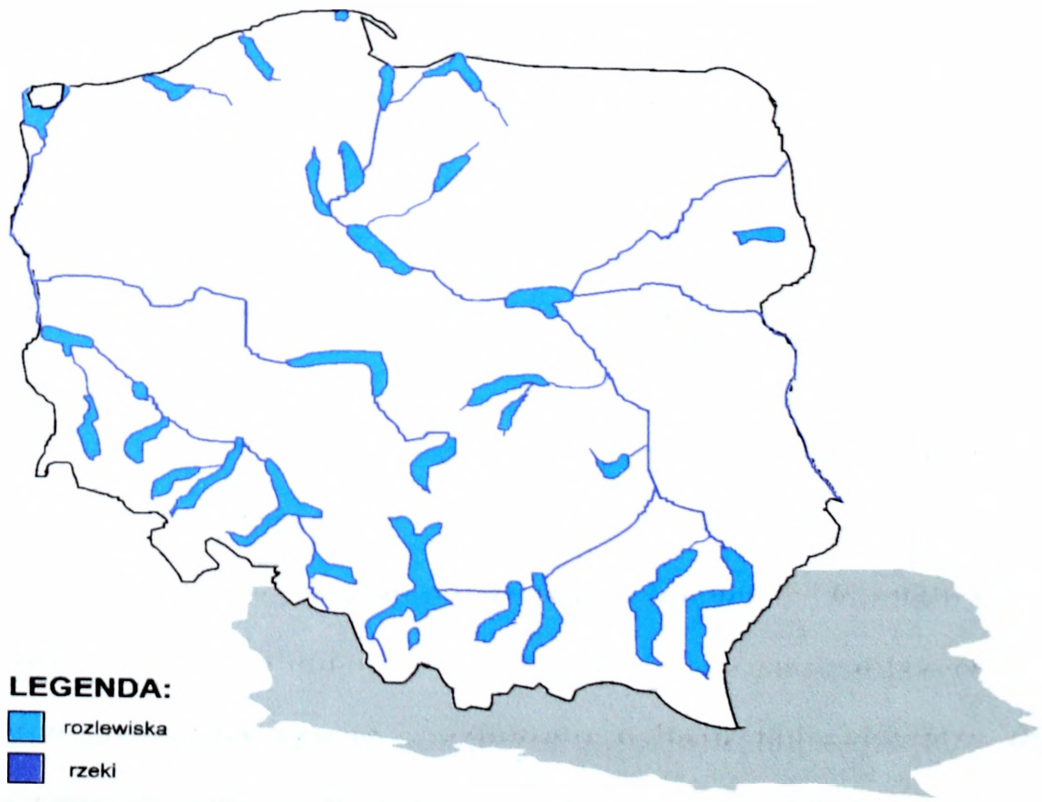
Natomiast w sytuacjach zagrożenia bezpieczeństwa państwa sieci i usługi telekomunikacyjne muszą sprostać nagłym zmianom natężenia ruchu oraz pilnej potrzebie wspomagania działań obronnych. Zakres zniszczeń w sieci może być różny w zależności od kraju oraz jego regionu. W powstałych warunkach działania operatorów w zakresie budowania, konserwacji i odtwarzania łączności krajowej i międzynarodowej nie będą możliwe bez odpowiedniej koordynacji. W wyniku

Cechą zatopień jest gwałtowność zdarzenia i często brak symptomów wskazujących na możliwość jego wystąpienia. Mogą być także wykonane sztucznie – w czasie kryzysu i wojny. Z pewnym prawdopodobieństwem można również wskazać miejsca wystąpienia powodzi i zatopień (Mapa 2.6.).

c) pożary najczęściej mogą wystąpić na obszarach zalesionych lub w zakładach przemysłowych, skupiskach ludzkich, gdzie zgromadzone są substancje i przedmioty łatwopalne. W wyniku pożarów mogą nastąpić zniszczenia bezpośrednie i wtórne - klęski ekologiczne np. pożar w rafinerii naftowej, składnicy gazów przemysłowych, pożar dużych obszarów leśnych.

d) katastrofy ekologiczne spowodowane:
   - uszkodzeniem reaktorów jądrowych - radiacja promieniotwórcza;
   - zagrożeniami chemicznymi - występującymi w pobliżu zakładów i składnic chemicznych oraz dróg transportu. Zagrożenia trującymi środkami dotyczą znacznych obszarów kraju (Mapa 2.7.).

Mapa 2.6. Prawdopodobne miejsca wystąpienia powodzi i zatopień



Źródło: W. Gawlikowski, M. Szaliłow, *Zagrożenia stacjonarnego systemu telekomunikacyjnego w czasie klęsk ekologicznych, katastrof i wojny.* w: „Zeszyty Naukowe AON" 1997 nr 3, s. 83.

335-3383i wojny. Operatorzy muszą opracować plany uwzględniające szereg czynników podanych poniżej.

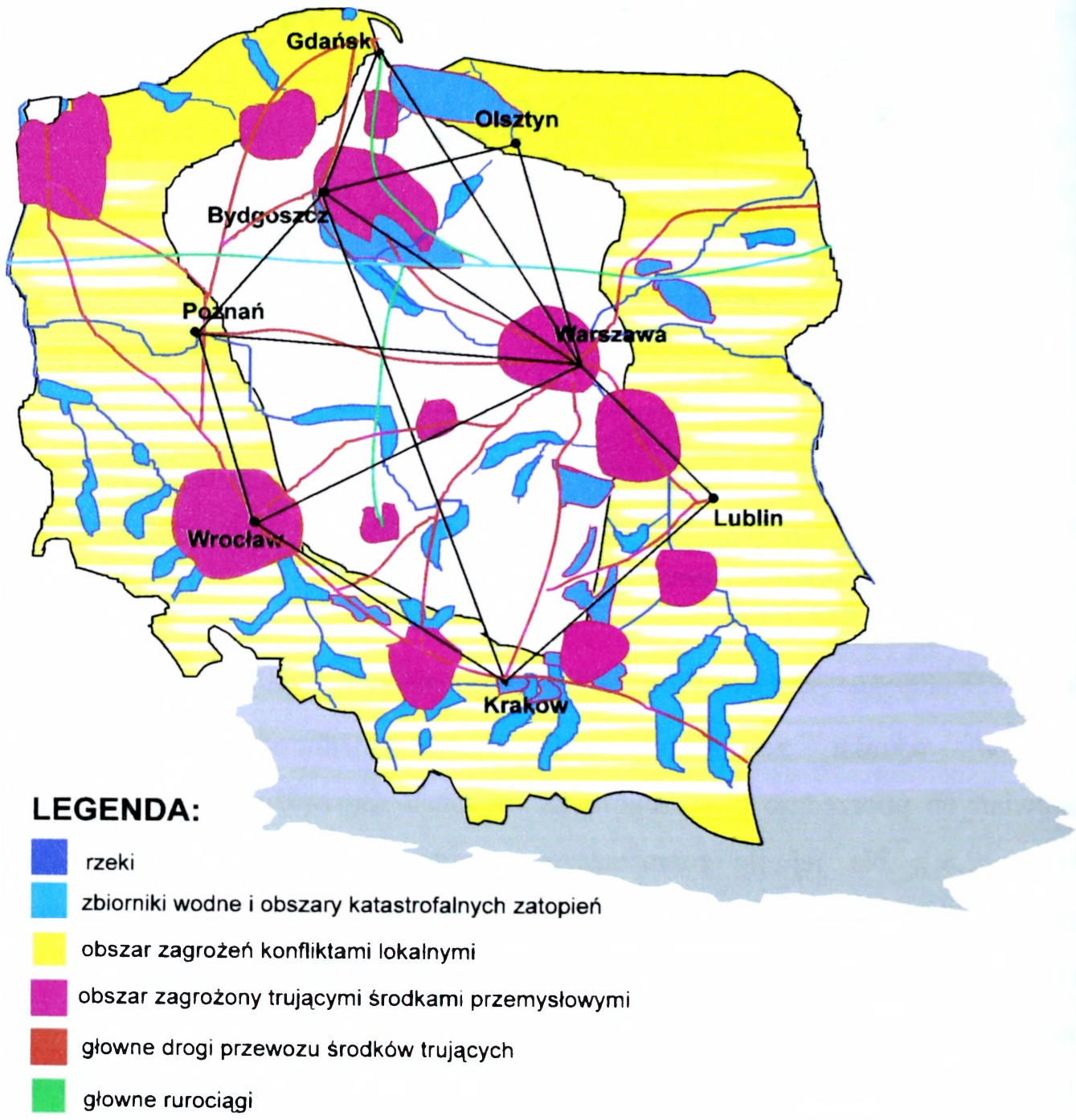
Planowanie budowy i eksploatacji sieci publicznych w czasie pokoju ma na celu nie tylko zapewnienie potrzeb komercyjno - usługowych, ale także wymagań okresu kryzysu i wojny, na przykład w zakresie jej żywotności i elastyczności. Biorąc pod uwagę wymagania obronne, możliwość technicznej realizacji oraz ograniczenia finansowe, należy w planowaniu uwzględnić następujące środki:

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

W sytuacji zagrożenia bezpieczeństwa państwa sieci telekomunikacyjne powinny podołać zmianom w modelach ruchu oraz pilnym potrzebom wspomagania działań wojsk sojuszu, nawet po zniszczeniach. Warunki w obrębie danego kraju mogą być bardzo zróżnicowane. Może zaistnieć sytuacja kiedy na wielu obszarach system świadczenia usług będzie w stanie kompletnego zniszczenia, w innych możliwe będzie normalne jego funkcjonowanie. w takich

decyzji władz krajowych operatorzy powinni przejść z działalności pokojowej na wojenną, zgodnie z wcześniej przygotowanymi planami.

Mapa 2.8. Obszary występowania z największym prawdopodobieństwem różnych typów zagrożeń



Źródło: Opracowanie własne na podstawie materiałów Obrony Cywilnej Kraju.

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

- w zbiorze dopuszczalnych struktur przeprowadzić badania analityczne niezawodności, trwałości i przepustowości. Na tej podstawie określić suboptymalną strukturę obiektu docelowego.

Należy prowadzić badania i działania w celu optymalizacji rozmieszczenia węzłów i podwęzłów w systemie łączności oraz zastosowanej przepływności traktów, uwzględniając przewidywane natężeniem ruchu rozmieszczenie abonentów i ich przemieszczanie - wymagane w sytuacjach stanów nadzwyczajnych. Realizacja organizowanego i docelowego systemu łączności powinna być poprzedzona badaniem modelu struktury powiązań jej węzłów.

Aktualnie w wielu krajach powszechna jest tendencja do wykorzystywania i adaptacji istniejących rozwiązań komercyjnych do zastosowań militarnych. Może się wydawać, że przyjęcie rozwiązań opartych na technologii wąskopasmowej, przy powszechnym już dziś dostępie do bardziej nowoczesnych rozwiązań, okazuje się mało przekonywujące, nie perspektywiczne, a tym samym nietrafne.

W niektórych państwach będących członkami NATO funkcjonują specjalne systemy łączności oparte o modulację delta. Fakt ten ma związek przede wszystkim z redukcją wydatków budżetowych np. na specjalne systemy łączności.

2.3.2.1. Bariery i zagrożenia dla bezpieczeństwa ekonomicznego Polski ze strony infrastruktury telekomunikacyjnej

We współczesnym świecie znacznie zmniejszyło się prawdopodobieństwo wybuchu wojny powszechnej, co nie oznacza jednak całkowitego uwolnienia się od konfliktów. Konflikty zbrojne nadal stanowią zagrożenie, ale o znacznie mniejszej skali i innym charakterze. Skutki takich konfliktów przenoszone się bezpośrednio na sąsiadujące państwa, wywołując kryzys natury politycznej, ekonomicznej, społecznej, militarnej itp. Obecnie bezpieczeństwo narodowe i jego zagrożenia w większości mają nie tylko, szeroko rozumiany charakter militarny czy ekologiczny, ale również społeczny a szczególnie ekonomiczny.

Równie niebezpieczne dla funkcjonowania państwa są zagrożenia spowodowane działaniami żywiołów, przede wszystkim zachowaniem się ludzi. W ustawodawstwie niektórych państw określa się je jako nadzwyczajne zagrożenia wewnętrzne, do których zalicza się: zagrożenia ustroju konstytucyjnego, zagrożenia

okolicznościach działania władz cywilnych polegać powinny na zapewnieniu nieprzerwanego świadczenia najważniejszych usług dla kraju i zagranicy.

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

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

W celu lepszego przystosowania systemu łączności do spełnienia zadań i wymagań systemu kierowania obronnością państwa należałoby:

- zrealizować podsystem utajniania;
- umożliwić dostęp radiowy dla abonentów będących w ruchu;
- rozważyć możliwość łączenia (między sobą) węzłów/podwęzłów za pośrednictwem łączy satelitarnych.

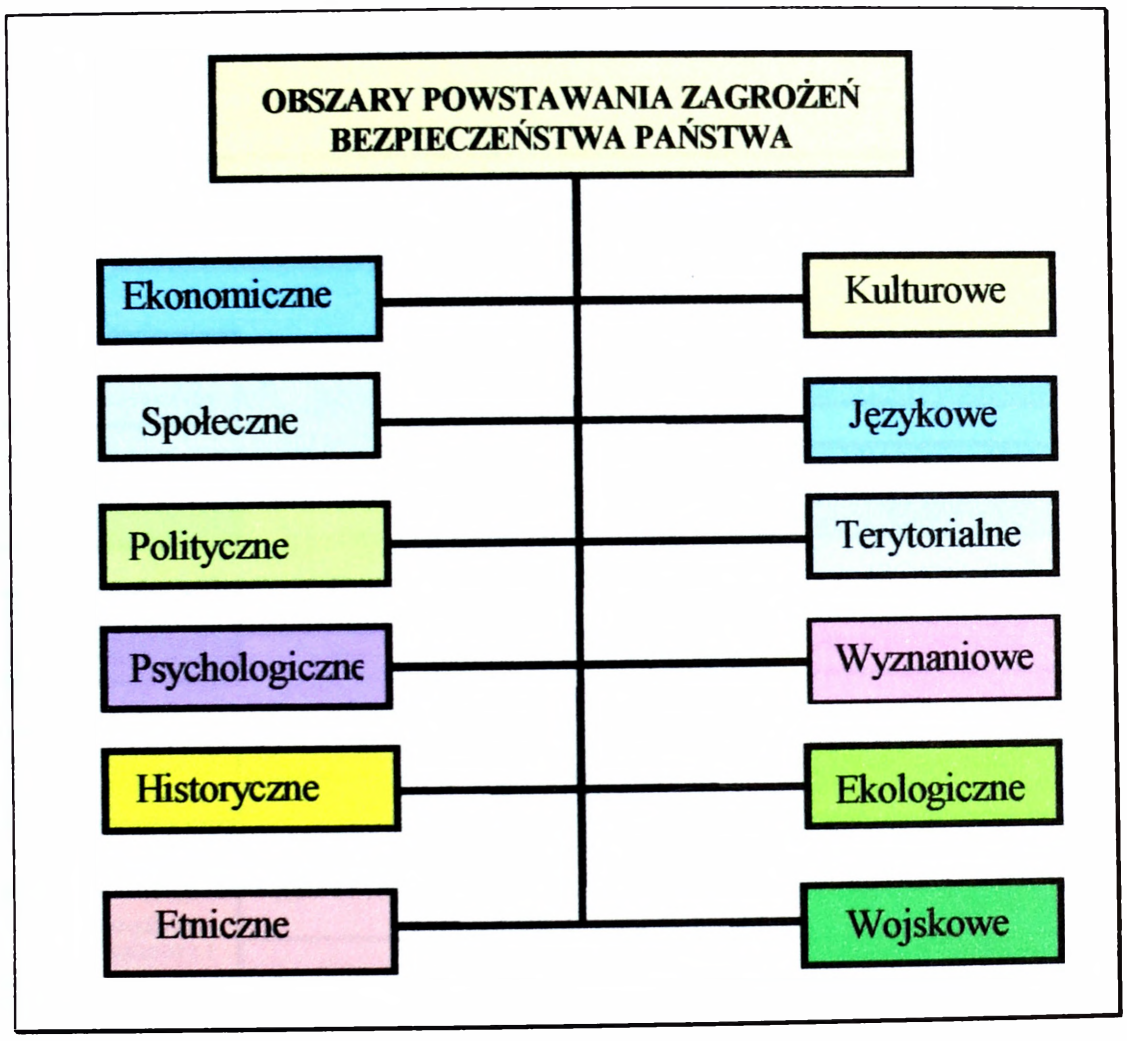
W celu określenia systemu łączności kierowania obronnością państwa należy się posłużyć następującym algorytmem postępowania:

- zweryfikować: zbiór użytkowników, ruch przez nich generowany (postacie wiadomości, ich priorytety, potrzeby w zakresie utajniania);
- zweryfikować i uzupełnić wymagania techniczne na obiekty;
- ustalić zasoby, które mogą być wykorzystywane z sieci TP S.A. i innych operatorów;
- opracować zasady rozpływu ruchu z uwzględnieniem właściwości elementów komutacyjnych i posiadanych zasobów sieci;
- zaprojektować dopuszczalną strukturę sieci z uwzględnieniem: zweryfikowanych wymagań, rozpływu ruchu, wskaźnika jakości obsługi;

mogą powstawać sytuacje konfliktogenne, zagrożenia militarne lub konflikty zbrojne.

Schemat 2.13.

Obszary powstawania zagrożeń bezpieczeństwa państwa



Źródło: S. Dworecki, *Od konfliktu do wojny*, BUWIK, Warszawa 1996, s. 19.

Zróżnicowany rozwój gospodarczy krajów powoduje, że obecnie stosunki międzynarodowe na wszystkich płaszczyznach charakteryzują się skomplikowanym systemem zależności i powiązań między regionami, społeczeństwami, religiami i ruchami politycznymi współpracującymi lub rywalizującymi ze sobą. Sieć powiązań gospodarczych sprawia, że stosunki ekonomiczne stają się ważnym instrumentem polityki, wpływającym na współczesne pojęcie bezpieczeństwa. Środki oddziaływania ekonomicznego mogą stać się skutecznym narzędziem wymuszeń, presji lub faworyzowania. Poziom rozwoju gospodarczego i sytuacja ekonomiczna państwa ma ścisły

bezpieczeństwa i porządku publicznego, klęski żywiołowe, nieszczęśliwe wypadki o znamionach klęski żywiołowej[211].

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

1. polityczno-militarne;
2. niemilitarne, w skład których wchodzą:
   - zagrożenia ustroju konstytucyjnego;
   - zagrożenie ładu i porządku publicznego;
   - nadzwyczajne zagrożenia środowiska.

Polityka jako sztuka rządzenia, jest uwarunkowana określonymi celami i interesami, a mająca za zadanie zdobycie lub utrzymanie władzy, może być źródłem powstawania konfliktów wewnętrznych, a także międzynarodowych. Zarówno jedna i druga płaszczyzna polityczna jest bardzo istotna, zwłaszcza do określenia potencjalnych źródeł zagrożeń militarnych. Przez przyczyny zagrożeń militarnych należy rozmieć takie dziedziny wewnętrznych i międzynarodowych stosunków, na tle których mogą się pojawić symptomy zjawisk konfliktotwórczych. Obszary, w których mogą powstawać zagrożenia bezpieczeństwa państwa są bardzo szerokie i złożone (Schemat 2.13.).

Przemiany społeczno-polityczne i wojskowe w latach dziewięćdziesiątych i dwutysięcznych spowodowały istotne zmiany geopolityczne w świecie i Europie. Zniknął podział na dwa przeciwstawne bloki, zostały zahamowane zbrojenia i odsunięte widmo wojny termojądrowej. Z Unią Europejską zintegrowane zostały państwa dawnego bloku wschodniego, co nie wyeliminowało jednak sprzeczności historycznych, narodowościowych, kulturowych, wyznaniowych itp., a tym samym źródeł napięć, sytuacji kryzysowych czy konfliktów.

W wyniku zmian geopolitycznych, państwa hegemonistyczne utraciły kontrolę nad tłumionymi dotychczas dążeniami i aspiracjami etnicznymi, narodowościowymi czy religijnymi. Jeżeli do tego dołączymy zróżnicowanie poziomu rozwoju: gospodarczego, nauki i techniki, technologii produkcji, społecznego oraz warunków socjalnych itp., to otrzymamy podłoże, na którym

---

[211] Zob. *Konstytucja Rzeczypospolitej Polskiej*, art. 228.

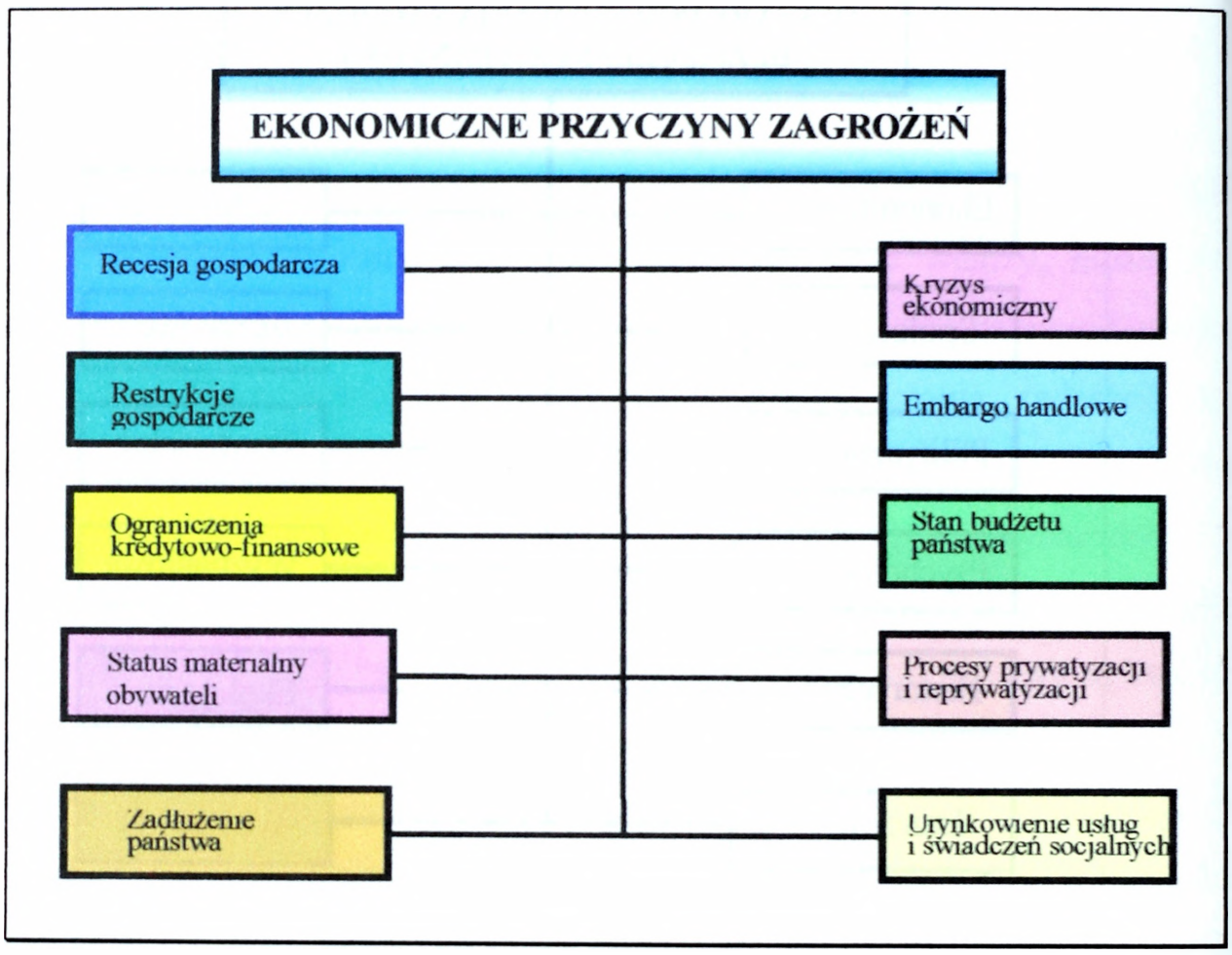
Wyzwania jakie stoją obecnie przed systemem obronności państwa znacznie różnią się od tych w przeszłości. Ze względu na członkostwo w NATO groźba ataku o dużej skali została skutecznie zlikwidowana i przez to nie musi determinować strategii obronnej kraju. W przeciwieństwie do sytuacji z przeszłości, obecne zagrożenia bezpieczeństwa państwa są wielokierunkowe i bardzo złożonej natury, co sprawia, że trudno jest je przewidzieć. Obecne zagrożenia w mniejszym stopniu są rezultatem zaplanowanych ataków na terytorium państwa i NATO, ale są przede wszystkim wynikiem destabilizacji wynikających z poważnych problemów ekonomicznych, społecznych i politycznych, obejmujących rywalizację etniczną oraz spory terytorialne, pojawiające się w wielu państwach centralnej i wschodniej Europy.

Istnienie dużych potencjałów jądrowych poza sojuszem jest również znaczącym czynnikiem, który musi być rozważany jeżeli bezpieczeństwo i stabilność w rejonie Europy i Oceanu Atlantyckiego ma zostać utrzymane. Bezpieczeństwo państwa a także NATO może zostać zakłócone przez inne zagrożenia szerszej natury łącznie z użyciem broni masowego rażenia, zakłóceniami przepływu podstawowych zasobów a przede wszystkim aktami terroryzmu i sabotażu. Szczegółowa natura tych zagrożeń jest trudna do przewidzenia, mimo to istnieje potrzeba opracowania planów oszacowania możliwych zagrożeń oraz usuwania i łagodzenia ich skutków. Z zagrożeniem życia i mienia spotykamy się od zarania dziejów. Początkowo źródłem zagrożenia były wyłącznie siły przyrody: pożary naturalne, uderzenia piorunów, powodzie, trzęsienia ziemi, wybuchy wulkanów i inne kataklizmy, wobec których i współczesny człowiek jest także w dużej mierze bezbronny. Tymczasem społeczność zagrożona jest znacznie szerszą gamą niebezpieczeństw wywołanych, zarówno przez klęski żywiołowe, jak i przez przemysł lub transport (wybuchy, uwolnienia toksycznych substancji, pożary). Wraz z rozwojem cywilizacji, a szczególnie przemysłu, pojawiły się zagrożenia, które człowiek sam generuje, na wskutek niedoskonałości swoich wytworów jak też niedoskonałości swego działania. Siłą rzeczy naruszany jest system funkcjonowania przyrody, którego zakłócenie porównywane jest do kataklizmu wojny nuklearnej. Różnica tkwi tylko w czasie występowania tych kataklizmów. Wojna nuklearna to zniszczenie życia

związek z nastrojami społecznymi i poczuciem jego bezpieczeństwa. Rozpatrując możliwe podłoża powstawania konfliktów, trudno pominąć cały obszar stosunków społecznych. Ekonomiczne przyczyny powstawania zagrożeń dają się sprowadzić do licznego ich zbioru (Schemat 2.14.).

Schemat 2.14.

Ekonomiczne przyczyny powstawania zagrożeń



Źródło: S. Dworecki, *Od konfliktu do wojny*, BUWIK, Warszawa 1996, s. 59.

W wyniku rozwoju ekonomicznego, postępu technicznego i technologicznego doszło do zachwiania równowagi w otaczającej nas przyrodzie, a zarazem do pogorszenia warunków życia ludzi (zatrucie środowiska naturalnego, zarówno w danym państwie, jak i w krajach sąsiednich). Z badań środowiska naturalnego wynika, że ludzkość przekroczyła graniczną wartość, poza którą wpływ ludzi na środowisko grozi jego zniszczeniem. Rozwój świadomości ekologicznej narodów w ostatnich latach, jej znaczenie i wpływ na życie jest tak duży, że ukształtowała się nowa płaszczyzna powstawania sprzeczności interesów czy konfliktów.

publicznego, klęski żywiołowe, nieszczęśliwe wypadki o znamionach klęski żywiołowej. Powstające sytuacje kryzysowe w wymiarze regionów czy też całego państwa powodują dodatkowy wzrost zapotrzebowania na aktualne informacje, ale również i na usługi telekomunikacyjne związane z przesyłaniem i przetwarzaniem danych.

Powodzenie każdej decyzji organów kierowniczych zależy od posiadania przez decydenta odpowiedniej jakości informacji o przedmiocie oceny, tj. obiektywnych, istotnych dla sprawy, a także w miarę kompletnych, porównywalnych i zwięzłych. Krajowe i międzynarodowe instytucje polityczne, gospodarcze, wojskowe, naukowe, a nawet osoby fizyczne coraz bardziej uzależniają się od stałej do niej dostępności. Jednym z głównych celów potencjalnego ataku przeciwnika może być system telekomunikacyjny kraju, gdyż jest intensywnie wykorzystywany do przekazywania informacji w czasie pokoju, a szczególnie podczas stanów kryzysowych oraz wojny, przez użytkowników wojskowych i cywilnych.

Funkcjonowanie systemu telekomunikacyjnego w tych warunkach może zostać zakłócone również przez szereg barier i czynników takich jak: terroryzm, sabotaż, broń konwencjonalna, jądrowa, chemiczna i biologiczna, walka elektroniczna, katastrofy naturalne i ekologiczne.

Pod pojęciem ***terroryzm*** – należy rozumieć różnie umotywowane ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup skutkujące naruszeniem istniejącego porządku prawnego, podjęte w celu wymuszenia od władz państw i społeczeństwa określonych zachowań i świadczeń, często naruszające dobra osób postronnych; działania te są realizowane z całą bezwzględnością, za pomocą różnych środków (naciski psychologiczne, przemoc fizyczna, użycie broni i ładunków wybuchowych), w warunkach specjalnie nadanego im rozgłosu i celowo wytworzonego w społeczeństwie lęku[212]. Należy odróżnić, mimo wspólnego źródłosłowu, terroryzm od terroru (aktów terroru); terror to gwałt i przemoc „silniejszych" organów państwa wobec „słabszych" obywateli, a terroryzm to gwałt i przemoc „słabszych" obywateli wobec

---

[212]Obecnie istnieje ponad 100 definicji tego zjawiska; kilkadziesiąt powstało w ramach prac ONZ, głównie przy próbach określenia terroryzmu międzynarodowego.

w krótkim okresie czasu, zaś wojna ekologiczna trwać może o wiele dłużej. Natomiast skutki będą identyczne. Dynamika rozwoju technicznego przyczynia się do powstania zagrożeń ekologicznych. Konstruktorzy urządzeń technicznych, często ze względów ekonomicznych, nie konstruują ich w układy sprzyjające ekologii środowiska. Interes społeczny w tym względzie schodzi na plan dalszy ustępując skutkom działalności użytkowej. Zagrożenia ekologiczne pojmowane są powszechnie jako potencjalne zmiany w środowisku fizycznym, biologicznym i społecznym, w sumie niekorzystne i upośledzające jego egzystencję.

Do najczęściej występujących form tych zagrożeń zalicza się:

- degradację bogactw i zasobów naturalnych, która wyraża się w obniżeniu ilości i jakości zasobów mineralnych, lasów, gleby, wód itp.;
- zanieczyszczenia biologiczne, powodujące schorzenia człowieka i świata przyrody;
- zanieczyszczenia chemiczne, pyłowe, gazowe powietrza, gleby, wody, środków spożywczych, a w konsekwencji organizmów żywych;
- zanieczyszczenia fizyczne, akustyczne, termiczne, radioaktywne;
- zanieczyszczenia estetyczne, wyrażające się w brzydocie, chaosie, bezładzie przestrzennym, braku organizacji, naruszaniu harmonii krajobrazu.

Źródeł zagrożeń ekologicznych należy zatem poszukiwać w niekontrolowanym dążeniu człowieka do zaspokajania nowych potrzeb cywilizacyjnych kosztem realizacji potrzeb biologicznych i społecznych, przy najmniejszych nakładach finansowych. Wraz z rozwojem cywilizacji, a szczególnie przemysłowej, pojawiły się zagrożenia, które człowiek sam generuje, na wskutek niedoskonałości swoich wytworów jak też niedoskonałości swego działania.

Tymczasem społeczność zagrożona jest znacznie szerszą gamą niebezpieczeństw wywołanych, zarówno przez klęski żywiołowe, jak i przez przemysł lub transport (wybuchy, uwolnienia toksycznych substancji, pożary). Równie niebezpieczne dla funkcjonowania państwa są zagrożenia spowodowane działaniami żywiołów oraz zachowaniem ludzi. w ustawodawstwie niektórych państw określa się je jako nadzwyczajne zagrożenia wewnętrzne, do których zalicza się: zagrożenia ustroju konstytucyjnego, zagrożenia bezpieczeństwa i porządku

Broń chemiczna i biologiczna powoduje szczególne zagrożenie, ponieważ jest przeznaczona do niszczenia i skażenia wybranych materiałów, terenów lub zabijania grup ludzi. Pomimo międzynarodowych ograniczeń dotyczących tego typu broni, istnieją jej różne odmiany.

Broń konwencjonalna może być bardzo skuteczna przeciwko wszelkim rodzajom instalacji telekomunikacyjnych. Uszkodzenia systemów telekomunikacyjnych są powodowane bezpośrednimi atakami oraz efektami ubocznymi innych wybuchów (pożary, odłamki itp.).

Walka elektroniczna może mieć wpływ na wszystkie sieci i systemy telekomunikacyjne. Obejmuje proste zakłócanie pracy bardziej skomplikowanych urządzeń powodowane przez silne promieniowanie z radarów albo innych urządzeń zakłócających. Takie promieniowanie może doprowadzić do uszkodzenia elementów sieci. Łącza radiowe (np. wysokich częstotliwości oraz komercyjne łącza satelitarne) oraz w szczególności łącza o stałych częstotliwościach są bardzo podatne na zakłócenia. Fale radiowe mogą być również używane do naprowadzania środków bojowych na źródło promieniowania elektromagnetycznego. Dodatkowym zagrożeniem mogą być ataki na elementy systemów satelitarnych znajdujące się na ziemi i w przestrzeni kosmicznej.

Zakłóceniem funkcjonowania systemu telekomunikacyjnego może stać się również ***przeciążenie*** powodujące brak możliwości świadczenia usług telekomunikacyjnych. Może być ono spowodowane uszkodzeniem sieci wynikającym z celowych działań, klęsk żywiołowych albo katastrof, a tym samym ze wzrastającego wykorzystania przez użytkowników będącego reakcją na wynikłe wydarzenia.

Wyzyskiwanie – jako zakłócenie funkcjonowania systemu telekomunikacyjnego obejmuje szeroki wachlarz ukrytych działań. Jednymi z najbardziej powszechnych sposobów wykorzystania publicznej sieci telefonicznej jest gromadzenie informacji (poprzez monitoring), powodowanie przeciążeń, uzyskiwanie nielegalnego dostępu do systemów informacyjnych dla przechwycenia danych lub ich zafałszowania oraz wykorzystanie mediów publicznych dla prowadzenia własnej propagandy.

„silniejszych" organów państwa. Większość działań wiąże się z braniem zakładników. Ma to na celu nasilenie dramatyzmu zdarzenia, zdobycie rozgłosu dla głoszonej idei oraz umocnienie pozycji terrorystów przy pertraktacjach. Terroryzm wiąże się także z handlem narkotykami, żywym towarem, bronią i materiałami rozszczepialnymi. Dogodne warunki do dalszego rozwoju i działania organizacji o charakterze terrorystycznym stwarzają terroryzm bliskowschodni, fundamentalizm muzułmański (dżihad), nacjonalizm postsowiecki, tendencje nacjonalistyczne w byłej NRD i rozpad Jugosławii[213].

Od aktów ściśle terrorystycznych należy odróżnić zwyczajne czyny kryminalne o pewnych znamionach terroryzmu, np. obecnie w Polsce anonimowe telefony o podłożeniu materiałów wybuchowych w obiektach użyteczności publicznej, eksplozje takich ładunków na tle porachunków między gangami przestępczymi czy też z motywu zemsty lub w celu zastraszenia urzędników państw (prokuratorów, sędziów, celników itp.).

Sabotaż to atak fizyczny na obiekty (często ukryte), mający na celu uniemożliwienie świadczenia usług telekomunikacyjnych i uszkodzenie całego systemu. Obejmuje, również próby spenetrowania i skorumpowania elementów systemów informacyjnych. Działania wywrotowe obejmują przykładowo podsłuch elektroniczny oraz przeniknięcie i manipulowanie kadrami.

Broń jądrowa może mieć wieloraki wpływ na systemy łączności. Wybuchy na niskiej wysokości mogą spowodować bezpośrednie uszkodzenia instalacji przez siłę eksplozji, wysoką temperaturę oraz bliskość promieniowania. Wybuchy na dużych wysokościach mogą zakłócać lub uszkodzić instalacje telekomunikacyjne przez efekt impulsu elektromagnetycznego (Elektro Magnetic Pulse - EMP). Inne konsekwencje ataków jądrowych obejmują absorbcję transmisji satelitarnej oraz długodystansowych dróg propagacji, generowanie EMP skierowane przeciwko satelitom oraz efekty magnetyczno-hydrodynamiczne (MHD) skierowane przeciwko liniom długodystansowym oraz kablom podmorskim. Należy jednak pamiętać, że tego typu dużej skali ataki jądrowe są mało prawdopodobne w obecnej sytuacji politycznej.

---

[213] W terroryzmie można wyróżnić następujące rodzaje: światowy, międzynarodowy, polityczny, cyberterroryzm i narkoterroryzm.

- ujawnienie informacji lub korupcję spowodowana przez wyzyskiwanie, sabotaż, wojnę elektroniczną, itp.;
- utratę kontroli operacyjnej nad siecią spowodowana wyzyskiwaniem, sabotażem albo fizycznym uszkodzeniem lub brakiem kadr;
- stopniową utratę usług spowodowaną brakiem kadr odpowiedzialnych za obsługę i serwisowanie.

Takie sytuacje mogą poważnie zdezorganizować działania państwa poprzez zakłócanie zarządzania kryzysowego, konsultacji, koordynacji i przetwarzania informacji chyba, że zostaną podjęte odpowiednie środki mające zagwarantować ciągłe świadczenie najważniejszych usług telekomunikacyjnych.

Źródeł zagrożeń bezpieczeństwa ekonomicznego Polski należy doszukiwać się także w niedorozwoju gospodarczym, w stosunku do rozwiniętego świata, zarówno sfery realnej jak i sfery regulacji. Idzie tu zwłaszcza o zapóźnienia o charakterze strukturalnym, techniczno - technologicznym i organizacyjnym. Są to:

- przestarzała struktura gospodarki;
- niedostateczne tempo w wytwarzania produktów technologicznie intensywnych, czy też przetworzonych artykułów rolno-spożywczych, na które popyt zagraniczny rośnie w największym stopniu;
- dość słaba dynamika procesów prywatyzacyjnych, zwłaszcza dotyczących sektorów „problemowych";
- zdominowanie polityki makroekonomicznej przez politykę duszenia inflacji, co ogranicza zastosowanie innych instrumentów wspierania produkcji i eksportu.

Wewnętrzne źródła zagrożeń bezpieczeństwa ekonomicznego Polski[214] można pogrupować w kilku najważniejszych obszarach wiążących się z:

- wyborem dróg rozwoju gospodarczego;
- transformacją ustrojową;
- rynkiem (rynkowym systemem funkcjonowania gospodarki);
- możliwościami reprodukcji rozszerzonej;
- problemami techniczno-organizacyjnymi i technologicznymi;

---

[214]Por. Bariery i zagrożenia gospodarcze dla systemu obronnego Polski, w „Materiały i Studia", IEO WS-0, nr 8 (26), AON, Warszawa 1994.

Katastrofy naturalne – powodowane są przez np. susze, powodzie, pioruny, wstrząsy sejsmiczne, sztormy, huragany, szkodniki, choroby itp.

Katastrofy ekologiczne - mogą być spowodowane przez działania człowieka np.: awarie, nieprawidłowe użytkowanie materiałów niebezpiecznych i środków ochrony roślin, opóźnienia pracy, strajki itd. Dynamika rozwoju technicznego i technologicznego przyczynia się do powstania szeregu zagrożeń. Konstruktorzy urządzeń technicznych, często ze względów ekonomicznych, nie konstruują ich w układy sprzyjające społeczeństwu czy ekologii środowiska. Interes społeczny w tym względzie schodzi na plan dalszy ustępując skutkom działalności użytkowej.

Nadzwyczajne zagrożenia – mają charakter nagły, na skutek katastrofy przemysłowej czy klęski żywiołowej może powstać nagle nadzwyczajne zagrożenie życia i zdrowia ludzi lub środowiska przyrodniczego.

Z nadzwyczajnymi zagrożeniami związane są specyficzne problemy i zagadnienia nie występujące w tym natężeniu w tradycyjnej ochronie środowiska. Najważniejszym z nich jest prewencja, czyli ograniczenie do minimum prawdopodobieństwa wystąpienia katastrofy lub awarii. Ponieważ katastrof nie można uniknąć, ani im całkowicie zapobiec, istotne znaczenie ma przewidywanie ich skutków, przygotowanie zawczasu właściwych planów ratowniczych, procedur postępowania, zapewnienia sił i środków, przygotowanie systemów powiadamiania i ewakuacji ludności. Niezwykle ważny jest też problem budzenia świadomości społeczeństwa i przekazanie ludności odpowiedniej informacji, by umożliwić jej prawidłowe reakcje oraz by uniknąć paniki. Wreszcie niezwykle istotnymi elementami są szkolenia i ćwiczenia zespołów przygotowywanych do przeprowadzania akcji ratowniczej, a także ćwiczenia z udziałem całej załogi zakładów i mieszkańców zagrożonego obszaru. Bacznej uwagi wymaga zapewnienie prawidłowego postępowania poawaryjnego oraz umiejętność analizy oraz wyciągania wniosków na przyszłość z zaistniałej sytuacji.

Przedstawione bariery i zagrożenia mogą utrudniać świadczenie usług telekomunikacyjnych i powodować następujące zjawiska negatywne:

- utratę usług albo ograniczenie ich dostępności spowodowane pojedynczymi lub wieloma zagrożeniami;

telekomunikacyjnej na potrzeby sytuacji szczególnych zagrożeń, a także przewiduje się ograniczenie skutków możliwych uszkodzeń i zniszczeń do minimalnego poziomu. Przesyłanie i przetwarzanie dużych ilości wiarygodnych, terminowych i utajnionych wiadomości jest warunkiem koniecznym zapewnienia bezpieczeństwa państwa a szczególnie bezpieczeństwa ekonomicznego. Dlatego operatorzy telekomunikacyjni muszą uwzględniać w codziennej działalności wiele zdarzeń, które mają wpływ na możliwości obsługi ruchu i świadczenia usług. Sposób ich działania w czasie pokoju powinien być kontynuowany w sytuacjach kryzysowych i stanie wojny tak dalece jak tylko jest to możliwe. Jednakże muszą oni zaplanować i przygotować już w czasie pokoju właściwą infrastrukturę sieci telekomunikacyjnej i przewidzieć szereg stosownych działań na wypadek szczególnych zagrożeń, które mogą wystąpić podczas eskalacji sytuacji kryzysowych.

Możliwości wzmocnienia bezpieczeństwa ekonomicznego można osiągnąć poprzez uodpornienie elementów rozwijanej infrastruktury telekomunikacyjnej, zmniejszy to prawdopodobieństwo wystąpienia zniszczenia, a skutki uszkodzeń będzie można zlikwidować zanim system telekomunikacyjny zostanie zablokowany w wyniku nadmiernego wzrostu natężenia ruchu w traktach nie uszkodzonych. Na wskazane działania mogą mieć wpływ:

1. Stopień przygotowania i gotowości kadr do realizacji czynności wyższych stanów gotowości;
2. Stopień zabezpieczenia (odporności) systemu na destrukcyjne oddziaływania:
   a) zewnętrzne (niezależne od systemu):
      - bojowe oddziaływanie przeciwnika;
      - radioelektroniczne oddziaływanie przeciwnika;
      - klęski żywiołowe, katastrofy, awarie, warunki pogodowe, pory roku itp.;
      - uzyskanie w odpowiednim czasie, przez eksploatatorów systemu łączności, danych o zmianie stanu gotowości obronnej państwa (dające możliwość wyprzedzającej reakcji).
   b) wewnętrzne obniżające sprawność systemu (zależne od systemu):

- brakiem dostatecznych środków na sferę dostarczania dóbr publicznych.

Problemy rozwoju sytuacji wewnętrznej znajdują odzwierciedlenie w potrzebie realizacji całego szeregu, takich zadań jak:

- zakończenie procesu prywatyzacyjnego;
- zakończenie procesu przekształceń strukturalnych w ważniejszych gałęziach przemysłu tj.: węglowym, hutnictwie, obronnym, naftowym;
- opracowanie i wdrożenie programu modernizacji rolnictwa;
- dokończenie transformacji systemowej;
- podniesienie nakładów na szkolnictwo i badania naukowe;
- dojście, a następnie utrzymanie w trendzie kilku, kilkunastoletnim wzrostu gospodarczego na poziomie 6-8%;
- stworzenie dogodnych warunków dla inwestycji krajowych i zagranicznych, jako podstawowego elementu walki z bezrobociem i rozwoju kraju;
- stworzenie programu ochrony biologicznej;
- stworzenie spójnego systemu obronnego, tak w sferze doktrynalnej, jak i realizacyjnej;
- dopasowanie potencjału gospodarczo-obronnego do możliwości jego wykorzystania oraz skali zagrożeń;
- dostosowanie potencjału gospodarczo - obronnego do zasad gospodarki rynkowej;
- pełne przystosowanie struktur polskich sił zbrojnych do współdziałania z armiami sojuszniczymi;
- zwiększenie wydatków na zakup sprzętu i uzbrojenia wojskowego.

2.3.2.2. Szanse i możliwości wzmocnienia bezpieczeństwa ekonomicznego w oparciu o rozwój infrastruktury telekomunikacyjnej

Efektywne kierowanie i zarządzanie państwem jest uzależnione od przesyłania terminowych, wiernych i skrytych informacji w systemie teleinformatycznym państwa. Teleinformatyczne systemy są rozwijane i wykorzystywane przede wszystkim pod względem zaspokojenia potrzeb ludności w czasie pokoju. Ale również planuje się rozwój infrastruktury sieci

- przygotowania właściwej organizacji i usług w tych obszarach, w których można przewidywać zintensyfikowane działania;
- przygotowania lub wzmocnienia środków bezpieczeństwa wewnętrznego i zwiększenia stanu osobowego personelu odpowiedzialnego za ochronę przed aktami sabotażu, działaniami wywrotowymi itp.;
- przygotowania systemów rezerwowych, zapasów, zdolności produkcyjnych i możliwości napraw oraz zapewnienia, gdzie jest to możliwe, użyteczności tych zasobów w czasie kryzysów i wojny;
- informowania i instruowania ludności na temat dobrowolnych i obowiązkowych ograniczeń w zakresie korzystania z usług telekomunikacyjnych stosownie do bieżącej sytuacji.

W celu spełnienia wymagań obronności państwa, a przede wszystkim wzmocnienia bezpieczeństwa ekonomicznego, biorąc pod uwagę dotychczasowy stan i potrzeby rozwoju sieci telekomunikacyjnej, jak i realne możliwości techniczne oraz ograniczenia finansowe, należy uwzględnić i zapewnić:

- łącza z każdym krajem członkowskim NATO na trasach geograficznie niezależnych;
- możliwie maksymalną różnorodność trasowania naziemnych łączy kablowych, mikrofalowych i satelitarnych pomiędzy krajami członkowskimi;
- połączenia najważniejszych łączy należy wykonywać w taki sposób, aby najważniejsze węzły były zdublowane;
- sprzęt rezerwowy we właściwych stacjach wzmacniakowych;
- należy przyjąć, że w czasie kryzysów natężenie ruchu telefonicznego będzie większe niż w czasie pokoju;
- wystarczającą pojemność sieci, która będzie w stanie obsłużyć to zwiększone zapotrzebowanie; inny ruch, który również może wzrosnąć, musi być w ostateczności ograniczony tak, aby osiągnąć zamierzony cel;
- typową technikę kierowania ruchu na maksymalną liczbę różnych tras (z automatyczną rezerwą), aby móc obsłużyć najważniejszy ruch w przypadku uszkodzenia wielu łączy;

- wielowariantowość i realność planów osiągania gotowości systemu łączności;
- stopień wyszkolenia etatowych obsług węzłów, stacji wzmacniakowych i linii łączności;
- stopień znajomości sieci - systemu przez osoby zarządzające – w zakresie jego konfiguracji;
- stopień ukompletowania sił i środków realizujących system łączności ;
- stan utrzymania i sprawność środków łączności;
- stopień standaryzacji sprzętu, wg najnowszych norm, pozwalający na szybką zmianę konfiguracji systemu.

Zwiększenie odporności infrastruktury telekomunikacyjnej na zagrożenia można uzyskać przez:

- zmiany rozmieszczenia elementów sieci, rozproszenie sprzętu w miejscach największych zagrożeń;
- zastosowanie przedsięwzięć organizacyjno - technicznych w zależności od stopnia poszczególnych zagrożeń;
- zrealizowanie struktury telekomunikacyjnej powiązanych liniami łączności ze sobą węzłów, podwęzłów i automatyczne wybieranie drogi obejściowej dla połączenia w wypadku uszkodzenia odcinka traktu powoduje skuteczne zabezpieczenie systemu przed brakiem łączności w wyniku uszkodzeń pojedynczych traktów czy podwęzłów.

Należy brać pod uwagę możliwości zagwarantowania wystarczających zasobów ludzkich, które są ograniczone na potrzeby mobilizacji powszechnej tak, aby podjąć odpowiednie działania ogólnokrajowe w zakresie dyspozycyjności wykwalifikowanych fachowców łączności. Wyznaczony personel musi być przeszkolony, np. dzięki uczestnictwu w ćwiczeniach. Należy poczynić przygotowania na potrzeby:

- powołania centrów zarządzania kryzysowego zapewniając wystarczające i bezpieczne środki łączności oraz procedury stopniowej zmiany funkcji stosownie do potrzeb sytuacji kryzysowych i wojny;

Dla utrzymania właściwego stanu infrastruktury i zapewnienia świadczenia istniejących usług telekomunikacyjnych na szczeblu krajowym powinno się dokonać niezbędnych przygotowań i podjąć odpowiednie działania do ograniczenia wpływu występujących zagrożeń. Niejednokrotnie, społeczności lokalne i przemysł są świadome potrzeby zapobiegania i przeciwdziałania awariom, działając samodzielnie nie osiągają zadawalających efektów. Współdziałanie i koordynacja są ważne w celu osiągnięcia maksimum efektywności wykorzystania dostępnych zasobów ludzkich i materialnych.

Jednym z wielu sposobów zapewniających właściwe działanie infrastruktury telekomunikacyjnej w zakresie obsługi abonentów podczas zwiększonego natężenia ruchu w sytuacjach szczególnych zagrożeń państwa, jest korzystanie z programu uprzywilejowanego dostępu ważnych użytkowników (abonentów specjalnych) z zasobów sieci telekomunikacyjnej.

Większość krajów posiada narodowe programy uprzywilejowanego dostępu, które umożliwiają funkcjonowanie tego istotnego krajowego ruchu telekomunikacyjnego. Jednakże, sprawą znaczącej wagi dla NATO jest wsparcie krajów członkowskich w czasie kryzysu i przedstawienie zasad interoperacyjności umożliwiających łączność pomiędzy ważnymi użytkownikami w obszarze wykraczającym poza jedno państwo. Międzynarodowy Program Uprzywilejowanego Dostępu – IEPS (ang. – International Emergency Preference Scheme) wynika konsekwentnie z tych zasad jako całości. Zasadniczym celem zastosowania programu uprzywilejowanego dostępu IEPS jest zapewnienie możliwości zarządzania kryzysowego NATO. Program uprzywilejowanego dostępu IEPS mógłby w sposób znaczący zwiększyć zdolność ważnych użytkowników do uruchomienia i ukończenia łączności (głos i dane) poprzez publiczną komutowaną sieć telefoniczną.

Narodowe programy uprzywilejowanego dostępu są przeznaczone do zastosowania w sytuacjach kryzysowych, lecz mogą zaistnieć sytuacje, kiedy może wystąpić konieczność bez uruchomienia międzynarodowego programu uprzywilejowanego dostępu IEPS bez uruchomienia systemu narodowego. Przykładem tego jest sytuacja, gdy tworzy się intensywny ruch międzynarodowy do odległego kraju znajdującego się w stanie kryzysu. Stąd międzynarodowe i krajowe

- ciągły nadzór poszczególnych elementów sieci, który umożliwia odpowiednie raportowanie stanu tych elementów, a także właściwe przygotowane łącza na potrzeby zarządzania siecią.

W celu zagwarantowania niezawodności i dużej odporności sieci na uszkodzenia, pamiętając o potrzebie zachowania równowagi pomiędzy wymaganiami sojuszu, należy uwzględnić i zapewnić:

- ☐ krajowe i międzynarodowe węzły komutacyjne oraz centra systemów zarządzania powinny mieć możliwość wzajemnego przejmowania swoich funkcji z powodu uszkodzenia jednego lub więcej węzłów;
- ☐ należy zapewnić wysoki poziom ochrony fizycznej wszystkich tych elementów sieci, które obsługują łączność specjalną, a szczególnie ważnych węzłów komutacyjnych i ich wyposażenia, kluczowych stacji wzmacniakowych, stacji końcowych kabli i wyposażenia wszystkich stacji radiowych;
- ☐ zabezpieczenie przed możliwymi uszkodzeniami spowodowanymi wyładowaniami atmosferycznymi pomimo, że uszkodzenia tego typu nie są obecnie uznawane jako stwarzające poważne ryzyko;
- ☐ wykorzystać naturalne ukształtowanie terenu już w trakcie podejmowania decyzji o lokalizacji instalacji telekomunikacyjnych specjalnego przeznaczenia, magazynów i warsztatów w celu zapewnienia dodatkowej ochrony;
- ☐ zabezpieczyć zasilanie rezerwowe i dostawy paliwa do agregatów prądotwórczych w kluczowych instalacjach;
- ☐ w celu ułatwienia odtwarzania łączności należy magazynować sprzęt rezerwowy i części zamienne w miejscu instalacji;
- ☐ logistyczne zabezpieczenie systemu łączności, w tym utrzymanie zapasu remontowego;
- ☐ w celu minimalizacji ryzyka sabotażu, przechwytywania informacji, namierzania lokalizacji systemów radiowych należy brać pod uwagę ograniczenie emisji radiowej.

Planując obsługę techniczną w czasie pokoju należy zwrócić szczególną uwagę i na zwiększone zapotrzebowanie na takie usługi w czasie kryzysów i wojny.

działania, które mogą być ustanawiane przez lub dla danego wywołującego abonenta. Nie może występować konflikt pomiędzy połączeniem preferencyjnym ze strony ważnego użytkownika i priorytetem (kolejnością) połączeń nieważnego użytkownika, a obsługą w sytuacjach krytycznych.

Wszystkie ograniczenia połączeń do pewnych określonych obszarów (np. numery kierunkowe krajów, numery kierunkowe regionów, numery kierunkowe miejscowości) będą właściwe, gdy zostanie uruchomiony program IEPS. Takie ograniczenia nie powinny odnosić się do użytkowników programu IEPS. Pozostałe kierunki powinny być dostępne w dalszym ciągu do użytkowników nie związanych z programem IEPS. Muszą być ustalone, zarówno środki techniczne, jak i procedury zarządzania związane z uruchomieniem i działaniem IEPS kompatybilne z istniejącymi programami zarządzania krajowej sieci ruchu telefonicznego. Połączenia pochodzące od użytkowników programu uprzywilejowanego dostępu, powinny mieć priorytet w połączonych sieciach, gdy zostanie uruchomiony program IEPS.

Państwa są zobowiązane określić status preferencyjny połączeń pochodzących od ważnych użytkowników z państw sojuszniczych oraz tych z innych krajów, z którymi zawarto umowy międzynarodowe. Sprawą zasadniczą jest ogólne zrozumienie kategorii użytkowników pomiędzy krajami członkowskimi. Powinny być ustalone, zarówno środki techniczne, jak i procedury zarządzania związane z uruchomieniem i działaniem IEPS kompatybilne z istniejącymi programami zarządzania krajowej sieci ruchu telefonicznego. Dla skutecznego wdrożenia programu uprzywilejowanego dostępu, konieczne jest zastosowanie systemu sygnalizacyjnego nr 7, zarówno dla sygnalizacji krajowej, jak i międzynarodowej[215]. Koszty wdrażania i obsługi programu uprzywilejowanego dostępu ponoszą dane zainteresowane kraje. Konieczne ustanowienie krajowego ustawodawstwa w celu wdrożenia programu uprzywilejowanego dostępu i ograniczenia jego właściwości jedynie do rozmów upoważnionych użytkowników. Program uprzywilejowanego dostępu powinien być regularnie i okresowo

---

[215]Sygnalizacja SS 7 (ang. Comon Chanel Signal – ling 7) wspólnokanałowy, scentralizowany system sygnalizacji numer 7, stosowany w sieciach cyfrowych ISDN i telekomunikacyjnych przekazach cyfrowych.

programy uprzywilejowanego dostępu powinny być rozważane jako niezależne i interoperacyjne.

Najwyższe organa władzy i administracji państwa oraz dowodzenia siłami zbrojnymi są odpowiedzialne za przygotowanie listy abonentów specjalnych, którzy są ważni z punktu widzenia prawidłowego funkcjonowania państwa. Opierając się na wytycznych władz centralnych, regionalne władze krajowe powinny opracować listy abonentów specjalnych. Listy te (kategorie) powinny uwzględniać tych abonentów, którzy mają zasadnicze znaczenie dla prawidłowego funkcjonowania państwa, abonentów ważnych, a także tych abonentów, którzy są mało ważni. Określając kategorie abonentów centralne władze krajowe powinny wziąć pod uwagę te funkcje, których prawidłowa realizacja zależy od łączności cywilnej. Listy te powinny być przesłane bezpośrednio do odpowiednich organów administracji telekomunikacji w celu podjęcia stosownych działań na rzecz zapewnienia ciągłości świadczenia usług abonentom specjalnym. W odniesieniu do własnych wymagań operatorów telekomunikacyjnych w zakresie zobowiązań na potrzeby szczególnych zagrożeń, powinni oni opracować podobne listy i działać stosownie do treści tych dokumentów.

Upoważnieni użytkownicy krajowego programu uprzywilejowanego dostępu mogą nie być pożądanymi do uzyskania dostępu do programu uprzywilejowanego dostępu, lecz upoważnieni użytkownicy programu międzynarodowego muszą być zdolni do wykorzystania ich własnych krajowych programów uprzywilejowanego dostępu. W celu wykorzystania uprzywilejowanego dostępu IEPS konieczne jest, aby główni użytkownicy byli w stanie wykorzystywać swoje urządzenia telekomunikacyjne w okresach kryzysowych. Podczas połączeń IEPS publiczna komutowana sieć telefoniczna nie może się różnić dla ważnego użytkownika. Połączenia pochodzące od użytkowników programu uprzywilejowanego dostępu powinny mieć priorytet w połączonych sieciach, gdy zostanie uruchomiony program IEPS. W warunkach poważnego uszkodzenia lub zatoru, państwa powinny być w stanie realizować kontrolę, w szczególności nad ruchem wchodzącym, nawet gdy program IEPS został uruchomiony. W celu umożliwienia preferencyjnemu użytkownikowi zrealizowania danego połączenia telefonicznego z innym użytkownikiem nie powinna być uruchamiana rejestracja połączeń lub podobne

zorganizowane grupy o nastawieniu antyspołecznym i antypaństwowym, co w pewien sposób poruszało problematykę cyberterroryzmu. Proponowane działania legislacyjne miały rozwijać się w dwóch kierunkach: ku stworzeniu komputerowej, sieciowej bazy aktów prawnych, stale aktualizowanej i zabezpieczanej przed ingerencją zewnętrzną (informatyzacja legislacji) oraz ku zdynamizowaniu prac prawodawczych związanych z informatyzacją (legislacja informatyzacji), co powinno odbywać się z uwzględnieniem specjalistycznych opinii informatyków.

Drugi Kongres Informatyki Polskiej zorganizowany został po upływie pięciu lat, na przełomie listopada i grudnia 1999 roku. Natomiast trzeci Kongres Informatyki Polskiej odbył się w dniach 2÷4 w Poznaniu 2003 roku[217].

W przyjętych raportach sformułowano szereg istotnych, dla bezpieczeństwa i rozwoju gospodarczego państwa, wniosków końcowych. Stwierdzono, że: „Państwo jest generalnie nieprzygotowane do absorpcji technologii teleinformatycznych w sposób racjonalny. Kręgom politycznym i gospodarczym brak odpowiedniej wiedzy o znaczeniu zastosowań informatyki dla sprawnego funkcjonowania administracji. Przejawia się to brakiem wyraźnie zdefiniowanego zapotrzebowania na informację źródłową, przepływ, zbieranie, przetwarzanie i wykorzystywanie informacji oraz barkiem spójnego planu informatyzacji administracji państwowej i samorządowej."

Jednym z kolejnych znaczących wniosków dotyczących istniejących uwarunkowań legislacyjno – prawnych był zapis „Konieczność zmian legislacyjnych wynikających z upowszechniania się nowych technik informatycznych wypływa ze stale zwiększającego się zagrożenia przestępstwami komputerowymi. Włamania do systemów, wprowadzanie niszczących wirusów czy kradzież danych oraz zmiany zapisów księgowych powodują coraz większe szkody finansowe i mogą obecnie dotknąć każdego obywatela - nawet nie korzystającego z komputera. Dlatego konieczne jest analizowanie tego rodzaju przestępstw, odpowiednie przeszkolenie policji oraz organów śledczych, a także wprowadzenie do kodeksów karnych i handlowych odpowiednich zapisów umożliwiających skazanie złapanych przestępców komputerowych".

---

[217]Organizatorem Kongresu Informatyki Polskiej była Polska Izba Informatyki i Telekomunikacji.

sprawdzany poprzez stosowanie odpowiednich testów i prób. Użytkownicy programu uprzywilejowanego dostępu powinni być wyznaczeni przez NATO i państwa członkowskie.

W sytuacji zagrożenia niezależnie od własności i przynależności winny być użyte w miejscu i czasie, gdzie są najbardziej potrzebne. Współpraca na szczeblu lokalnym ma kluczowe znaczenie. Powinna ona prowadzić do organizacji sprawnego, niekosztownego systemu prewencji i przeciwdziałania w sytuacjach niebezpiecznych. Dlatego też, istnieje pilna potrzeba opracowania ustawy tworzącej system przeciwdziałania nadzwyczajnym zagrożeniom cywilizacyjnym i środowiskowym.

Dyskusja w środowiskach specjalistycznych na temat infrastruktury telekomunikacyjnej i zaawansowania informatycznego polskiej gospodarki po transformacji systemowej rozpoczęła się w latach dziewięćdziesiątych. W 1994 roku w Poznaniu odbył się Pierwszy Kongres Informatyki Polskiej, którego raport podsumowywał stan przygotowania do informatyzacji gospodarki i życia publicznego.

Autorzy raportu rzetelnie i krytycznie ocenili rozwój technik i technologii informatycznych w Polsce: „Nasze społeczeństwo ma obojętny stosunek do informatyki i nie jest przekonane do korzyści wynikających z jej powszechnego stosowania. Nie widzi również możliwych zagrożeń”[216]. Wśród tych ostatnich, autorzy opracowania wyszczególnili przede wszystkim naruszenie poufności danych, szczególnie danych osobowych, i wskazali konieczne legislacyjne środki prewencji.

Dostrzeżono również groźbę rozwarstwienia społecznego. Ponadto uznano za niepokojący dystans, który może powstać, gdy program znajdzie zastosowanie w administracji publicznej, czemu nie będzie towarzyszył rozwój dostępności nowych mediów. Aby temu zapobiec, postulowano właściwą, szybką procedurę legislacyjną, uzupełnianą przez promocję szkoleń i kształcenia, pozwalającą na opanowanie obsługi komputerów i sieci. Pośrednio wypowiadano się również o niebezpieczeństwach, spowodowanych przejęciem kontroli nad informacją przez

---

[216]Por. *Strategia Rozwoju Informatyki w Polsce; Stan, Perspektywy, Zalecenia,* Poznań 1994; URL - http://www.kongres.org.pl/on-line/1-szy_Kongres/Raport.html.

kluczowych ośrodków akademickich w kraju, stwierdzali we wprowadzeniu m.in.: „Pierwsze kraje, które wkroczą do społeczeństwa informacyjnego, uzyskają największe korzyści. One ustalą porządek rzeczy dla wszystkich, którzy pójdą w ich ślady. Dla kontrastu, kraje, które odkładają decyzje lub preferują rozwiązania częściowe, mogą doświadczyć w najbliższej dekadzie katastrofalnego spadku inwestycji i zmniejszenia liczby miejsc pracy”[220]. Dostrzegano także zagrożenia płynące z rozwoju i upowszechniania techniki informatycznej i cywilizacji informacyjnej. „Wskazuje się, że rozwój technik informacyjnych i wzrost gospodarczej roli informacji może prowadzić do rozwarstwienia społecznego, w wyniku którego osoby nie posiadające dostępu do informacji będą cywilizacyjnie i ekonomicznie upośledzone. Ułatwiony dostęp do informacji może zagrażać prywatności [...] oraz wywołać pojawienie się nowej grupy przestępstw”[221].

Określona została równocześnie rola państwa jako podmiotu zapobiegającego zagrożeniom, który to cel realizować należy w postaci skoordynowanego planu obejmującego główne dziedziny strategiczne i działy pomocnicze. Autorzy raportu podjęli próbę zdefiniowana polityki państwa w zakresie implementacji idei społeczeństwa obywatelskiego jako: „zespołu działań zmierzających do zapewnienia wszystkim obywatelom dostępu do informacji [...]”, przy czym stwierdzono, że społeczeństwo informacyjne w Polsce zostanie ukształtowane siłami rynkowymi, z udziałem mechanizmów społecznych. Zadanie rządu sprowadza się do „stworzenia odpowiednich mechanizmów ekonomicznych, prawnych i administracyjnych dla zagwarantowania powszechnego dostępu do informacji, zapewnienia uczciwej konkurencji, umożliwienia zainteresowanym podmiotom korzystania z istniejących i przyszłych możliwości zastosowań teleinformatyki oraz tworzenia nowych rozwiązań, tak w sferze techniki jak i organizacji pracy”[222]. Podkreślono konieczność szybkiego rozwoju infrastruktury krytycznej w naszym kraju, powszechnego dostępu do informacji, a także dostosowania standardów społeczeństwa informacyjnego do zasad i przepisów konstytucji RP. Art. 54 stwierdza, że obywatelom polskim przysługuje prawo do

---

[220]Raporty: Komitetu Integracji Europejskiej, *Rozwój społeczeństwa*...,wyd. cyt., s. 17, i Komitetu Badań Naukowych, *Cele i kierunki rozwoju*..., wyd. cyt., s. 2.
[221]Tamże, s. 3.
[222]Tamże, s. 4.

We wnioskach na podkreślenie zasługuje stwierdzenie, że „Infrastruktura teleinformatyczna jest jednym z fundamentów wzrostu gospodarczego i cywilizacyjnego. Zbyt niskie tempo jej rozwoju grozi pozostawieniem w gronie maruderów Unii Europejskiej, przyczyniając się do urzeczywistnienia niechlubnego modelu „Europy dwóch prędkości", przed czym przywódcy europejscy przestrzegają już dziś"[218].

Uznano, że dla środowiska informatycznego ważnymi regulacjami prawnymi, które weszły w życie w minionych kilku latach, były:

- „Prawo telekomunikacyjne" z 2000 roku (z późniejszymi zmianami);
- o podpisie elektronicznym z 2001 roku;
- raport w sprawie dostosowań instytucjonalnych w Polsce do wymogów członkostwa w Unii Europejskiej z 2002 roku.

Do dyskusji włączył się również parlament. Sejm w uchwale z 14 lipca 2000 roku, w sprawie budowania społeczeństwa informacyjnego, diagnozował, iż „system prawny i polityka rządu nie tworzą dostatecznych warunków rozwoju społeczeństwa informacyjnego"[219]. Delegowano zatem na Radę Ministrów kompetencje w zakresie przygotowania narodowej strategii rozwoju społeczeństwa informacyjnego, czego efektem stał się raport KBN z listopada 2000 roku.

W uchwale sejmowej wyodrębniono następujące zadania strategiczne: powszechny dostęp do Internetu; rozwój *e-government, e-education;* szybki Internet dla ośrodków naukowo-badawczych; teleinformatyka w systemie finansowym i obronności, transporcie i ochronie zdrowia oraz prewencji kryminalnej; wreszcie zgodna ze standardami międzynarodowymi - transformacja – aktów prawnych regulujących problemy bezpieczeństwa informacyjnego, kryptografii, podpisu elektronicznego itp.

W listopadzie 2000 roku Komitet Badań Naukowych (KBN) przedstawił raport *„Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce"*, a Komitet Integracji Europejskiej w 2002 roku przyjął raport *„Rozwój społeczeństwa informacyjnego w Polsce"*. Autorzy tych dokumentów, naukowcy

---

[218]Zob. Raport: *2. Kongres Informatyki Polskiej,* i *3. Kongres Informatyki Polskiej*, www. kongres. org. pl/3KIP_raport.htm.

[219]Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 14 lipca 2000 r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce, w „Monitor Polski" 2000, nr 22, poz. 448.

ustawiczną zmienność środków teleinformatycznych, zachowywałyby krótką aktualność. Właściwsza wydaje się technika nowelizacji już istniejących ustaw oraz przepisów wykonawczych na szczeblach resortów.

Proponowano też przyjęcie ogólnych zasad, opartych na istniejących przepisach prawnych. Na przykład ochrona danych osobowych, a nawet pełna anonimowość użytkowników sieci, winna być zapewniona wszędzie tam, gdzie może być ona zachowana poza siecią. Postulowano również implementację porozumień w sprawie handlowych aspektów ochrony własności intelektualnej (TRIPS), podpisanych przez Polskę w ramach porozumień Światowej Organizacji Handlu (WTO) w 1996 roku i uznano, że należy podjąć starania o przystąpienie do traktatu o prawie autorskim Światowej Organizacji Własności Intelektualnej (WIPO). Raport nie zawierał definicji przestępstwa komputerowego ani cyberterroryzmu, kluczowych pojęć badanego przez nas zagadnienia. Dowodził natomiast świadomości zagrożeń, które autorzy dostrzegali w niekontrolowanym rozwoju telemediów. „Nowym jakościowo zjawiskiem jest pojawienie się w sieciach telekomunikacyjnych treści nielegalnych i szkodliwych, a w tym pornografii, materiałów nacjonalistycznych i terrorystycznych. Należy, podchodząc ze szczególną uwagą do kwestii wolności wypowiedzi, szybko opracować założenia do ustawy o zakazie rozpowszechniania treści nielegalnych i szkodliwych w sieciach teleinformatycznych, przyjmując za punkt wyjścia prace OECD oraz Uchwałę Rady Europy z dnia 17 lutego 1997 roku. Ustawa powinna jasno określać odpowiedzialność osób i instytucji, będących źródłem informacji, jej edytorem oraz jej dostarczycielem w długim nieraz łańcuchu pośredników”[226].

Powinna również określać formalno-prawne mechanizmy kontroli treści udostępnianych w sieciach, przy zapewnieniu swobodnej wymiany informacji. W celu ochrony nieletnich przed treściami szkodliwymi należy wprowadzić i upowszechnić system niezależnego, dobrowolnego rankingu i klasyfikacji treści publikowanych w sieciach teleinformatycznych przez organizacje konsumenckie[227]. W raporcie zajęto się także szyfrowaniem informacji przesyłanych w sieciach teleinformatycznych. O ile powszechnie uznaje się szyfrowanie informacji za

---

[226]Tamże, s. 41.
[227]Tamże, s. 72.

pozyskiwania informacji mających dużą wartość gospodarczą, polityczną czy kulturalną.

Na państwie spoczywa zatem obowiązek zapewnienia najszerszego dostępu użytkownikom do nowoczesnego systemu usług teleinformatycznych, jak również konieczność zadbania o równouprawnienie wszystkich w dostępie do nich (zasada równouprawnienia obywateli — art. 32 Konstytucji). W związku ze sklasyfikowaniem telemediów na równi z innymi środkami masowego przekazu, obejmie je w przyszłości konstytucyjny zapis, zawarty w art. 14, dotyczący wolności prasy i innych środków społecznego przekazu. „Usługi te nie będą podlegać koncesjonowaniu [...]"[223]. W art. 61 Konstytucji RP zapisano: „Obywatel ma prawo uzyskiwania informacji o działalności organów władzy publicznej [...]. Ograniczenie prawa, o którym mowa, może nastąpić wyłącznie ze względu na określone ustawą prawa i wolności innych osób, [...] ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa"[224].

Odnosząc się do powyższych zadań państwa, uznano, że Internet staje się jednym ze środków, którymi spełniać będzie ono w niedalekiej przyszłości ten konstytucyjny obowiązek. Sugerowano, by rozwój telekomunikacji był równocześnie: koordynowany przez stosowne resorty rządowe, skorelowany z procesami integracyjnymi Polski z Unią Europejską i by uwzględniał potrzebę standaryzacji usług, jako niezbędny i minimalny warunek bezpieczeństwa infrastruktury krytycznej państwa. W rozdziale pt. *„Prawo i przestępstwa teleinformatyczne"* jako cel podaje się: „dostosowanie regulacji prawnych do wymagań szybkiego postępu technicznego i ery społeczeństwa informacyjnego. Zastosowanie technik teleinformatycznych do opracowania nowych aktów prawnych"[225].

Pojawienie się nowych rodzajów przestępstw interpretowano jako konsekwencję nowych zagrożeń bezpieczeństwa obywateli w zakresie prawa do prywatności i danych osobowych. Równocześnie autorzy raportu sugerowali zmniejszenie do minimum liczby nowych regulacji prawnych, które ze względu na

---

[223]Tamże, s. 7.
[224]Konstytucja Rzeczypospolitej Polskiej, Warszawa 1997, s. 12.
[225]Raport KBN, *Cele i kierunki rozwoju...*, wyd. cyt., s. 14.

teleinformatycznych oraz przetwarzanych w nich danych. W wielu przypadkach rozpoznanie, w którym miejscu popełnione zostały wyżej wymienione przestępstwa, może nastręczać wiele trudności. Często miejsce, gdzie znajduje się osoba naruszająca prawo oraz miejsce przechwycenia, nadania, odbioru czy powstania informacji w sieci mogą być zlokalizowane w różnych państwach. Dlatego konieczna jest ponadnarodowa harmonizacja regulacji prawnych oraz międzynarodowe działania operacyjne.

W celu umożliwienia wczesnego wykrywania przestępstw popełnianych w sieciach teleinformatycznych, konieczne jest jak najszybsze ustanowienie całodobowych służb zbierających informacje o domniemanych przestępstwach, posiadających wydzielony kontaktowy numer telefoniczny, telefaksowy i elektroniczny adres sieciowy. Służby te powinny ściśle współpracować z międzynarodową siecią tego typu punktów kontaktowych.

Konieczne jest również powołanie biegłych sądowych w dziedzinie teleinformatyki oraz przygotowanie odpowiednich kursów informatyki dla prawników i studentów prawa, jak również dla pracowników urzędów celnych"[228]. Zgodnie z ustaleniami podjętymi podczas posiedzenia Rady Ministrów w dniu 28 listopada 2000 r., Przewodniczący Komitetu Badań Naukowych został zobowiązany do monitorowania stanu realizacji zadań w zakresie rozwoju społeczeństwa informacyjnego w Polsce oraz do przedkładania Radzie Ministrów co kwartał odpowiednich informacji. W związku z tym, począwszy od 2001 roku, publikowane są co trzy miesiące krótkie raporty tematyczne, omawiające zmiany w zakresie rozwoju społeczeństwa informacyjnego w Polsce[229].

Przedstawiona problematyka skłania do sformułowania szeregu uwag. Niejednokrotnie ekonomiści różnią się w stwierdzeniach, jak rozpatrywać nowe techniki i technologie a przede wszystkim infrastrukturę teleinformatyczną kraju i jej rozwój w aspekcie bezpieczeństwa państwa, to jednak są one szeroko postrzegane jako kluczowy czynnik, zarówno we wzroście wydajności, jak i wzroście ekonomicznym oraz jako czynnik rozróżniający bogate kraje od biednych.

---

[228]Tamże, s. 13-14.
[229]Por. - http://www.kbn.gov.pl/cele/raporty/1ndex.html.

konieczne dla zapewnienia prywatności i bezpieczeństwa użytkowników sieci oraz poprawnego rozwoju gospodarki elektronicznej, o tyle stopień skomplikowania klucza (jego długość) i algorytmu szyfrującego, oraz dostęp agend rządowych do tego klucza, pozostaje kwestią sporną. Doradzano, by dla zachowania bezpieczeństwa kraju i ochrony przed terroryzmem, rozważyć umożliwienie agendom rządowym dostępu do kluczy szyfrowania wszelkich informacji w sieciach publicznych, co stanowiłoby jednak naruszenie tajemnicy komunikowania się (por. art. 49 Konstytucji RP).

Proponowano przyjęcie takich rozwiązań prawnych i systemów zarządzania kluczami, by zachowana została równowaga pomiędzy interesami państwa, uzasadnionymi jego bezpieczeństwem, a interesami jego obywateli. Regulacje takie w tym zakresie powinny być tworzone w uzgodnieniu z Unią Europejską, gdzie proponuje się obecnie powołanie niezależnych instytucji przechowujących klucze szyfrujące i udostępniających je agendom rządowym po okazaniu nakazu prokuratorskiego. Uprawnia on do naruszenia tajemnicy poczty elektronicznej, podobnie jak do założenia podsłuchu. Szyfrowanie informacji może podlegać pewnym ograniczeniom, a jej deszyfrowanie nie powinno być dozwolone bez wiedzy nadawcy (ze wskazanym wcześniej wyjątkiem). Regulacje te powinny uwzględniać wytyczne dla polityki szyfrowania, opracowane przez OECD. Należy również zapewnić warunki techniczne umożliwiające rozkodowywanie informacji pochodzących z innych krajów świata, w tym z Unii Europejskiej oraz nawiązanie współpracy operacyjnej w tym zakresie.

Systemy tworzone na potrzeby zapewnienia bezpieczeństwa państwa, obejmujące administrację, policję, wojsko, służby specjalne i niektóre instytucje komercyjne, powinny wykorzystywać najnowocześniejsze metody zabezpieczeń. Jasne jest, że nie istnieją i być może nigdy nie powstaną zabezpieczenia pewne, których nie da się złamać. Ogólnie jednak przyjmuje się, że informacja jest dobrze zabezpieczona, gdy koszt złamania zabezpieczenia jest wyższy od wartości tej informacji. Dlatego też stosowane w takich systemach urządzenia i techniki powinny posiadać odpowiedni certyfikat Agencji Bezpieczeństwa Wewnętrznego.

Konieczne jest również podjęcie na potrzeby państwa badań nad technicznymi i organizacyjnymi metodami zabezpieczeń systemów

3. MODEL KSZTAŁTOWANIA BEZPIECZEŃSTWA EKONOMICZNEGO W OPARCIU O INFRASTRUKTURĘ TELEKOMUNIKACYJNĄ

3.1. Ogólne założenia uwarunkowań budowy postulatywnego modelu kształtowania bezpieczeństwa ekonomicznego państwa

Określenie zasad funkcjonowania oraz obszaru oddziaływania postulowanego modelu kształtowania bezpieczeństwa ekonomicznego stwarza konieczność odwołania się do szeregu procedur. W procesie konstruowania modelu procedury postępowania będą rzutować na jego zakres, relacje zachodzące wewnątrz niego oraz produkt finalny, którym będzie zbiór postulatów. Wskazanym będzie określenie i ocena ogólnych uwarunkowań tworzenia postulatywnego modelu kształtowania bezpieczeństwa ekonomicznego.

Konstrukcja postulowanego modelu kształtowania bezpieczeństwa ekonomicznego jest czynnością wieloetapową, w pierwszym etapie sprowadza się do sformułowania najważniejszych uwarunkowań wynikających z funkcjonowania istniejących systemów wewnętrznych państwa, a także ich kształtu, jakiego nabierają pod wpływem układu zewnętrznego. W drugim etapie będzie określenie realnych wymagań dla bezpieczeństwa ekonomicznego, jakie będą wynikały z powiązań o charakterze gospodarczym, politycznym i społecznym ze strategią obronną. Natomiast trzeci etap budowy modelu będzie ukazywał, jakie wymagania generowane przez strategię obronną są podstawą dla prawidłowego funkcjonowania modelu. Etapem końcowym będzie próba sformułowanie głównych założeń postulowanego modelu.

Jakość i poziom obronności państwa dawno przestał być tylko efektem potrzeb zgłaszanych przez układ militarny i pozamilitarny go tworzący. Jego kształt i jakość zależy w pierwszym rzędzie od spełnienia przez gospodarkę narodową szeregu wymagań rodzących się w obszarze obronności kraju. Pierwszoplanową rolę w ich realizacji spełnia gospodarka narodowa, która bezpośrednio przyczynia się do budowy zrębów gospodarczych podstaw obronności. Przy tworzeniu postulatywnego modelu kształtowania bezpieczeństwa ekonomicznego w świetle wymagań strategii obronnej należy uwzględniać wpływ zarówno wewnętrznych, jak i zewnętrznych uwarunkowań ekonomiczno-politycznych[229]. Czynniki te będą

---

[229]Por. Z. Królak, *Polska wobec wyzwań XXI wieku. Zarys strategii na I dekadę,* Wydawnictwo alfa2, Warszawa 2000, s. 164÷182; 197÷207.

Podkreśla się, że szczególnie nowe techniki i technologie w systemach informacyjnych są krytycznym czynnikiem długoterminowego wzrostu ekonomicznego nowoczesnych gospodarek i trwałym komponentem bezpieczeństwa. Same nowe techniki i technologie w systemach informacyjnych nie dają gwarancji bezpieczeństwa. Konieczne jest skuteczne optymalizowanie i organizowanie sił, które je wykorzystują. Sukces w tym zakresie zależy od przyjętej strategii rozwijanej pod przymusem konkurencyjności. Dlatego państwa szukają, obok konfrontacji nowych technik i możliwości technologicznych, również przewagi w osiągnięciach organizacyjnych. Organizacja jest tak samo decydująca, jak np. technologie teleinformatyczne, które dają początek nowym sieciowym formom organizacyjnym i umożliwiają pracę, przyczyniając się do wzrostu siły niepaństwowych podmiotów, często przewyższających potencjałem poszczególne państwa.

Przyszłość ekonomiczną narodu a rolę systemu informacyjnego i nowych technologii w inicjowaniu wzrostu gospodarczego należy widzieć jako zasadnicze filary w rozważaniach tradycyjnego bezpieczeństwa państwa. Można ogólnie powiedzieć, że dzisiejsza gospodarka państwa jest polem bitwy, że narodowe bezpieczeństwo zależy od bezpieczeństwa ekonomicznego. Zadanie przygotowania bezpiecznej przyszłości państwa wymaga silnej gospodarki i zapewnienia wymaganej zdolności nie tylko sile militarnej ale i efektywności systemu informacyjnego. Dzisiaj szeroko rozumiana obronność państwa powinna być rozumiana w kategoriach prowadzenia biznesu. W kierowaniu państwem najwyższe organa władzy i administracji powinny postrzegać techniki i technologie informacyjne jako swoje nowe zbrojne ramię, i jako nowe założenie polityki bezpieczeństwa państwa wkraczającego w XXI wiek.

omawianego sytemu znaczący wpływ posiada układ zewnętrzny, a także obowiązująca polityka bezpieczeństwa państwa, a w tym polityka bezpieczeństwa ekonomicznego państwa.

Ogólne założenia postulatywnego modelu wynikają z implikacji, jakie zaistniały po wygenerowaniu określonego modelu, czy też formuły makroorganizacji oraz sposobów komunikowania się (przepływu informacji), wypracowywania decyzji itd. Jego forma zależy w znacznym stopniu od panującego ustroju politycznego, stosunków społecznych, a zmiany w tych obszarach są pobudzane poprzez funkcjonowanie makroorganizacji. Z ustroju politycznego wynika forma prawna makroorganizacji oraz sposoby legislacyjno-wykonawcze realizacji wytyczonych przed nią celów. Te zaś są w dużej mierze zależne od postrzegania kwestii bezpieczeństwa ekonomicznego przez partie polityczne w naszym kraju[230]. Na determinanty politycznego kształtu, czy też formuły makroorganizacji duży wpływ posiada także czynnik społeczny. Ponadto w funkcjonującej makroorganizacji można doszukać się wpływu innych czynników takich jak: gospodarczych, kulturowych, religijnych itd., które jednak posiadają znaczenie drugorzędne.

Dużą wagę posiadają wzajemne relacje i poziom powiązań pomiędzy trzema filarami władzy tj. ustawodawczą, wykonawczą i sądowniczą. Wzajemne relacje w tym obszarze powiązań wynikają z aktu ustrojowego, jakim jest konstytucja, która jednocześnie określa kompetencje poszczególnych organów reprezentujących te trzy filary. Jest ona uzupełniona poprzez szereg ustaw, które odnoszą się bardziej do sfery realizacyjnej.

Najważniejszymi elementami wpływającymi na kształt postulatywnego modelu są: władza ustawodawcza i wykonawcza. To w ich kompetencjach znajduje się problematyka gospodarcza i obronna, odniesiona zarówno do fazy kreatywnej jak i realizacyjnej obu obszarów. Oznacza to, iż kształt postulatywnego modelu w znacznym stopniu zależy od zasad rządzących funkcjonowaniem makroorganizacji. Zapewne to omawiany model będzie się przystosowywał do formuły makroorganizacji, a dopiero w wyniku spójnego współistnienia będzie

---

[230]Por Z. Kołodziejak, *Próba identyfikacji problemu bezpieczeństwa ekonomicznego w poglądach partii politycznych w Polsce,* w: „Zeszyty Naukowe WSFiZ w Siedlcach"2004 nr 1, s.228÷241.

posiadać częstokroć rolę determinanta w kształtowaniu tegoż modelu. Bowiem to w ich obszarze będą się rodziły szanse i zagrożenia, które będzie można wykorzystać w osiąganiu określonego celu lub przeciwdziałać ich skutkom. Wymagania te mogą być realizowane tylko, gdy zaistnieją dwa warunki, a mianowicie gospodarka narodowa będzie się dynamicznie rozwijać oraz sfera gospodarcza będzie widzieć potrzebę łożenia świadczeń o określonej wysokości na rzecz sfery obronnej. Innymi słowami to ujmując musi zaistnieć potencjalna możliwość i wola do podjęcia określonych działań.

Określenie uwarunkowań stworzenia postulatywnego modelu kształtowania bezpieczeństwa ekonomicznego z punktu widzenia strategii obronnej będzie przebiegać poprzez system zarządzania państwem do systemu gospodarczego i systemu obronnego. System zarządzania będzie wiązał pozostałe systemy. Bezpieczeństwo ekonomiczne będzie wyrażane przez system gospodarczy, na który będzie się składała gospodarka narodowa wraz z podsystemem gospodarki obronnej. Strategia obronna będzie wynikała z obronności państwa wchodzącego w skład systemu obronnego. Oba te systemy będą scalane i koordynowane przez system zarządzania państwem. Wszystkie trzy podsystemy będą skupiały się w polityce bezpieczeństwa państwa, a całość będzie się składała na politykę bezpieczeństwa państwa.

Ogólnie uwarunkowania postulatywnego modelu będą wypływać z trzech obszarów oraz wynikających pomiędzy nimi powiązań, korelacji i sprzężeń. System zarządzania będzie nadrzędny wobec pozostałych dwóch systemów. Ogólne założenia postulatywnego modelu są w pierwszym rzędzie wypadkową trzech elementów:

- polityki bezpieczeństwa ekonomicznego kraju;
- polityki bezpieczeństwa państwa (wynikającej z polityki bezpieczeństwa ekonomicznego i wypływającą na nią);
- systemu zewnętrznego, który rzutuje na wszystkie elementy obszaru i wewnętrznego.

Charakterystyka tych elementów jest wypadkową systemu zarządzania państwem. System zarządzania państwem jest natomiast wypadkową przyjętej formuły mikroorganizacyjnej państwa. Na zachodzące przemiany w obrębie

formuły makroorganizacji i polityki bezpieczeństwa oraz jej powiązań z polityką bezpieczeństwa ekonomicznego kraju.

Duży wpływ na kształt postulatywnego modelu posiada system obronny. Znajduje się on pod wpływem systemu zarządzania państwem i funkcjonuje w powiązaniu z systemem gospodarczym. W skład systemu obronnego wchodzi podsystem obronności państwa, na który składa się strategia obronna i polityka obronna oraz podległy mu podsystem militarny i niemilitarny. Kształtowany jest także pod wpływem polityki bezpieczeństwa państwa i polityki bezpieczeństwa ekonomicznego kraju oraz układu zewnętrznego, przeciw którego negatywnym postępowaniom jest skierowany. Podsystem kierowania obronnością jest elementem wspólnym z systemem kierowania państwem, w którego skład wchodzą organy administracyjne państwa (państwowe i samorządowe) stworzone z myślą o obu systemach, a także o systemie obronnym państwa.

Podsystem pozamilitarny obejmuje szereg ogniw administracyjnych, organizacyjnych i gospodarczych, których działalność lub jej część jest skierowana na wsparcie systemu obronnego państwa. Należy podkreślić, iż jest to wsparcie o wymiarze rzeczowo-usługowym np. ochrona, produkcja na rzecz obronności, wsparcie organizacyjne itd. W tym obszarze znajdują się przedsiębiorstwa produkcyjne i usługowe, różne służby np. służby specjalne, policja, straż pożarna, obrona cywilna itd. Kolejnym podsystemem jest podsystem militarny, który obejmuje siły zbrojne danego kraju. Można powiedzieć, iż ten podsystem reprezentuje jedną z podgrup narzędziowych systemu obronnego, która jest uzupełniana, a także sterowana przez strategię obronną i politykę obronną państwa. Ostatnim elementem posiadającym znaczący wpływ na ogólne uwarunkowania tworzenia postulatywnego modelu kształtowania bezpieczeństwa ekonomicznego w świetle wymagań strategii obronnej jest system gospodarczy. W jego obszarze znajduje się podsystem gospodarki narodowej wraz z występującą w jej obszarze cyrkulacją gospodarczą. W skład podsystemu gospodarki narodowej wchodzi gospodarka obronna. System gospodarczy znajduje się współcześnie pod silnym wpływem systemu zewnętrznego oraz coraz mniejszym wpływem systemu zarządzania państwem.

Warto zauważyć, iż gospodarka obronna jest częścią wspólną gospodarki

powodował zmiany w jej formule poprzez narzucanie nowych rozwiązań działania, prognozowania itd. w obszarze bezpieczeństwa państwa. Duże znaczenie będzie posiadał w tym wypadku charakter organizacyjny makroorganizacji, a w szczególności struktura i kompetencje władzy ustawodawczej, jej możliwości wpływu na procesy gospodarcze, społeczne i legislacyjne oraz możliwości i zakres sprawowania nadzoru nad władzą wykonawczą. Znaczący wpływ będzie miał sposób organizacji władzy wykonawczej, jej zakres praw i obowiązków oraz sposób nadzoru nad nią. Ważnym elementem będą obowiązujące formuły wypracowywania decyzji i związane z nią przesyłanie informacji (pionowe, poziome lub mieszane), wynikający stąd zakres kompetencyjny poszczególnych poziomów organizacyjnych. Ważkim elementem w tym układzie będzie sposób organizacji poszczególnych szczebli władzy wykonawczej i powiązań pomiędzy różnymi jej organami. Kolejnym elementem posiadającym znaczenie dla postulatywnego modelu będzie stabilność organizacyjna i legislacyjna makroorganizacji.

Strategia obronna, reprezentująca obszar obronny, wobec bezpieczeństwa ekonomicznego (reprezentującego obszar gospodarczy), jest obszarem generującym potrzeby, które należałoby odczytywać jako wymagania. Obszar gospodarczy z kolei przesyła sygnał korygujący poziom wymagań, czyli staje się odniesieniem dla poziomu potrzeb. Potrzeby zgłaszane przez strategię obronną staję się źródłem wymagań wobec mechanizmów funkcjonowania oraz rozwoju społeczno-gospodarczego. Te z kolei generują nie tylko projekcję odniesienia, ale także pobudzają powstanie wymagań współzależnych z obszaru funkcjonowania i rozwoju społeczno-gospodarczego dla obszaru bezpieczeństwa państwa, a także dla podsystemu gospodarczo-obronnego.

System zarządzania państwem jest w procesie tworzenia postulatywnego modelu elementem spajającym i organizacyjnym wobec pozostałych podsystemów. Silny wpływ na ten system posiada sfera polityczna ukazana poprzez politykę bezpieczeństwa państwa i politykę bezpieczeństwa ekonomicznego. Ponadto duży wpływ na ten system posiada układ zewnętrzny. W skład tego systemu wchodzi podsystem gospodarki obronnej, będący wynikiem

polityka gospodarczo-obronna poprzez przyjęte procedury i praktykę w sposób skoordynowany i kompletny bada wykonalność projektowanych zamierzeń w obszarze bezpieczeństwa ekonomicznego, czyli dopuszczalność zakładanych strategii. Poprzez ten obszar następuje selekcja strategii i określenie tych z nich, które są dopuszczalne w konkretnych warunkach.

W Polsce wytworzyła się sytuacja, w której cele i metody restrukturyzacji wymagają akceptacji społecznej, aby uniknąć niepokojów społecznych lub w najlepszym razie niezadowolenia społecznego. Dlatego restrukturyzacja sektora gospodarki obronnej nie można przeprowadzić jedynie w oparciu o centralne zamierzenia, które nie uwzględniałyby problematyki lokalnej. W szczególności odnosi się to problematyki mikroekonomicznej najlepiej uwzględniającej lokalne potrzeby.

Z tego powodu wydaje się, iż potrzebą chwili jest wprowadzenie zhumanizowanego podejścia do planowania rozwoju gospodarki obronnej. Takie podejście może zapewnić społeczną akceptację celów i warunków przemian w obszarze gospodarki obronnej. Jednoczesnym następstwem takiego podejścia będzie decentralizacja zarządzania przedsiębiorstwami, przy jednoczesnej koncentracji zakładów obronnych. Jeżeli nie zostałyby wprowadzone tego typu mechanizm wówczas będzie miało miejsce dalsze wymuszanie ze strony polityki na rozwiązywanie narastających problemów, a w szczególności społecznych, kosztem poziomu i jakości obronności, a w konsekwencji bezpieczeństwa państwa. Charakter wymuszeń może być różny i będzie zależny od szeregu wypadkowych, które mogą posiadać charakter zarówno społeczny, polityczny, jak i gospodarczy. Szczególnie silne wymuszenia mogą powstać pod wpływem bodźców zewnętrznych, co wymaga prowadzenia konsekwentnej, spójnej i adekwatnej polityki narodowej.

Kolejnym postulatem strategii obronnej jest rozpoznawanie obszarów i procesów restrukturyzacji. Będzie to się odnosiło zarówno do sfery gospodarczej, społecznej, jak i politycznej. Należy przy tym pamiętać, iż wszelkiego rodzaju ruchy restrukturyzacyjne wiążą się w znacznym stopniu z przemianami struktur, powiązań, a co za tym idzie zasad funkcjonowania określonych systemów. Należałoby przy tym zwrócić uwagę na fakt, iż procesy restrukturyzacyjne są

narodowej i systemu obronnego państwa. Przenika ona praktycznie wszystkie działy gospodarki narodowej stanowiąc ich część, nie zawsze dającą się jednak statystycznie wyliczyć, czy wyodrębnić. Obecne uwarunkowania sprawiają, że trudno byłoby wskazać taką dziedzinę gospodarki, która w sposób bezpośredni lub pośredni nie ma związku z szeroko pojętym bezpieczeństwem i obronnością państwa.

Gospodarka narodowa jest zasadniczym źródłem zaopatrywania państwa i społeczeństwa w produkty lub usługi. Ze względu na występujące powiązania i współzależności jej potencjał determinuje możliwości tworzenia siły obronnej państwa i stwarza warunki dla zaspokojenia przyszłych potrzeb obronnych. W zależności od wielkości wysiłku obronnego, celów strategii i charakteru zagrożenia gospodarka w różnym stopniu i zakresie spełnia swoje funkcje.

Ponadto na ogólne uwarunkowania postulatywnego modelu nakładają się postulaty, jakie zgłasza strategia obronna wobec bezpieczeństwa ekonomicznego. Można je podzielić na dwa obszary:

- pierwszy obszar obejmuje obszarów i procesów restrukturyzacji oraz identyfikację warunków kształtowania bezpieczeństwa ekonomicznego, można go określić jako obszar badawczo-identyfikacyjny;
- drugi obszar obejmuje pierwiastek nieekonomiczny i ekonomiczny badanego obiektu.

W obu tych obszarach występują procedury, mechanizmy weryfikacyjne i dostosowawcze w stosunku do poszczególnych elementów tam występujących.

Ponadto pomiędzy oboma obszarami następuje szereg powiązań, korelacji i współzależności. Postulaty wysuwane przez strategię obronną wobec bezpieczeństwa ekonomicznego narzucają potrzebę określenia, czy też zdefiniowania procedur wyboru strategii dopuszczalnych, które mogą być realizowane w oparciu o możliwości ekonomiczne i militarne.

Punktem wyjścia do wskazania obszaru dopuszczalnych strategii jest polityka gospodarczo-obronna państwa[231]. Bowiem to właśnie ona w gospodarce rynkowej określa cele rozwojowe w obszarze gospodarczo-obronnym. Ponadto

---

[231]Por. Z. Stachowiak, Polityka gospodarczo-obronna, AON, Warszawa 1996.

a także warunki kształtowania strategii obronnej. W nim to będą zawarte wszelkie powiązania organizacyjne i wynikające z nich obowiązki i prawa w układzie międzynarodowym oraz uwarunkowania wewnętrzne tj. polityczne, prawne i organizatorskie, które decydują o funkcjonowaniu całego systemu. Posiadają one, tak w wymiarze zewnętrznym jak i zewnętrznym, duży wpływ na poziom procesów rozwojowych, czy też rozwój owo-restrukturyzacyjnych w obszarze gospodarki obronnej kraju i strategii obronnej oraz stabilizacji podstaw systemu obronnego gospodarki rynkowej.

Natomiast w kolejnym etapie badań powinna zostać przeprowadzona próba oceny stopnia zaawansowania procesów restrukturyzacyjno-rozwojowych w obszarze gospodarki obronnej i strategii obronnej oraz stabilizacji systemu obronnego gospodarki rynkowej. Zgodnie z poprzednimi analizami problemu ocena warunków o podstawowym znaczeniu dla bezpieczeństwa ekonomicznego wymagała przede wszystkim dokonania analizy poziomej nieekonomicznego bezpieczeństwa narodowego, a zwłaszcza dokonanie oceny, pod kątem oszacowania całego systemu obronnego, dla którego gospodarka obronnie zorientowana stanowi podsystem. Jednak istotą, na jaką można oprzeć oceny w tym obszarze jest uzależnienie przebudowy systemu obronnego Polski od realnych nakładów finansowych na modernizację techniczną Sił Zbrojnych RP.

Ponadto w tym układzie dokonywana jest ocena systemu kierowania państwem, a w szczególności zarządzania w dziedzinie gospodarki obronnej. Ocena skuteczności działania układu kierowania w tym obszarze jest jednak niska. Dokonywane oceny potencjału obronnego Polski, tak oficjalne, jak i nieoficjalne określają jego stan jako krytyczny, przy zaznaczeniu, iż kryzys finansów publicznych jest groźniejszy niż kryzys gospodarki obronnej. Taka ocena wynika z następujących faktów:

- jakość uzbrojenia i sprzętu technicznego będąca na wyposażeniu SZ RP odbiega w wielu wypadkach od przeciętnych norm obowiązujących w poszczególnych państwach członkowskich NATO;
- struktura głównych rodzajów uzbrojenia i sprzętu wojskowego jest asymetryczna w stosunku do państw sojuszniczych, a zmiany w tym obszarze są bardzo kosztowne;

z zasady procesami rozwojowymi. Warunki regulacyjne i systemowe są odbiciem i jednocześnie syntezą współzależności, jakie występują pomiędzy wzrostem efektywności gospodarowania a zmianami lub stagnacji struktur gospodarczych państwa. Szczególnie ważne staje się to w momencie dokonywania weryfikacji przyjętych założeń z osiągniętymi efektami, czego wyrazem będzie z kolei akceptacja społeczna lub jej brak - jest to bardzo ważne na obecnym etapie rozwoju społeczno-gospodarczego Polski. Aby proces restrukturyzacji przynosił zamierzony efekt koniecznym staje się wprowadzenie następujących narzędzi:

- skutecznej i stałej koordynacji procesów planowania;
- skutecznej i stałej koordynacji procesów organizowania;
- doskonalenia zawodowego;
- nadzoru i koordynacji przebiegu całego założonego procesu;
- elastyczności planów.

Elastyczność planów posiada szczególną rolę w okresie transformacji społeczno-gospodarczej tj. restrukturyzacji struktur państwa i społeczeństwa, gdyż dynamika wynikająca z przebiegających i procesów zmienność powoduje konieczność kreowania nowych, częstokroć przejściowych zachowań i ich podstaw teoretyczno-metodycznych.

Bez identyfikacji warunków kształtowania bezpieczeństwa ekonomicznego trudno jest oczekiwać, aby mogło zaistnieć bezpieczeństwo ekonomiczne państwa. Nie zidentyfikowanie warunków kształtowania bezpieczeństwa ekonomicznego będzie uniemożliwiał korelowanie celów gospodarczych i obronnych oraz celów wynikłych z tych obszarów z celami politycznymi i społecznymi, co będzie się przekładało na trudności w prowadzeniu spójnej polityki wewnętrznej i zewnętrznej oraz niemożliwość przyjmowania wymaganym rozwojem sytuacji wewnętrznej i zewnętrznej strategii gospodarczych i obronnych.

Drugi blok współtworzący postulaty, jakie zgłasza strategia obronna wobec bezpieczeństwa ekonomicznego obejmuje dwa podstawowe elementy: nieekonomiczne i ekonomiczne. Obszar nieekonomiczny składa się z podobszaru regulacji prawno-legislacyjnych oraz organizatorskiego. Z tychże obszarów wynikają warunki funkcjonowania gospodarczych podstaw obronności kraju, szczegółowe uwarunkowania kształtowania bezpieczeństwa ekonomicznego,

i wojskowo-militarnej w przypadku wystąpienia zagrożenia wojennego, czy też wojny. Istniejące sytuacje konfliktowe i rozwiązania systemowe, które w swej istocie są konfliktogenne w ramach systemu obronnego zwiększają jednocześnie społeczne koszty restrukturyzacji, a także uniemożliwiają wprowadzanie kompleksowych rozwiązań w tym obszarze.

Ponadto niski stopień zintegrowania systemu zarządzania w dziedzinie obronności, a w szczególności koordynacji działań, przyczynia się do niskiej skuteczności, czy wręcz nieskuteczności przetwarzania diagnostycznych ocen strategicznych na decyzje strategiczne.

Można stwierdzić, iż przy obecnym stanie rzeczy strategia obronna jest spychana na dalszy plan przez strategię gospodarczą, przez co nie można w pełni realizować założeń strategii obronnej, a m.in. z tego powodu gospodarka obronna nie jest w stanie samodzielnie opracować i wdrożyć własnego programu restrukturyzacji i rozwoju. Drugim obszarem są uwarunkowania ekonomiczne, które decydują o kształtowaniu gospodarczych podstaw obronności. Kształtowanie gospodarczych podstaw obronności odbywa się poprzez procesy przebiegające w trzech podsystemach, a mianowicie:

- systemie kierowania gospodarczymi podstawami obronności;
- systemie gospodarki obronnej;
- systemie logistyki obronnej.

Wyraźnie widać, iż dotykają one swoim zakresem większości obszarów funkcjonowania państwa. System kierowania gospodarczymi podstawami obronności jest wypadkową systemu organizacji państwa, który obejmuje takie elementy jak: organizacji państwa, ludzi i środki go współtworzące. Te elementy spełniają bardzo ważne funkcje, gdyż to od nich zależy wielowymiarowy system organizacyjny państwa, poziom i zakres realizowanych przez niego zadań itd.

System gospodarki obronnej ukazuje pragmatykę realizacji zadań z obszaru gospodarczych podstaw bezpieczeństwa. System logistyki obronnej jest praktyczną metodą redystrybucji środków, materiałów itd. na rzecz systemu bezpieczeństwa. System kierowania gospodarczymi podstawami obronności swym zakresem obejmuje:

- zarządzanie w dziedzinie obrony, zwłaszcza organizacji SZ RP są uwarunkowane panującym kryzysem finansów publicznych państwa, czego konsekwencją jest ograniczanie wydatków na obronę narodową;
- infrastruktura systemu obronnego nadal nie jest dostosowana do nowego geopolitycznego otoczenia Polski, a jego dostosowanie w krótkim czasie przekracza możliwości finansowe państwa; - poziom przydzielanych środków finansowych w poszczególnych latach dla MON nie dają możliwości dokonania odpowiednio do potrzeb modernizacji SZ RP.

Przeprowadzając diagnozę obecnego stanu i porównując go do stanu pożądanego tworzy się obraz różnic. Stąd wypływa konieczność przeprowadzenia analizy wielowariantowej decyzji rozwojowych. Poprzez takie działanie można zbudować strukturę istotnych celów rozwojowych i w oparciu o to można dokonać restrukturyzacji gospodarki narodowej, przy zaangażowaniu własnego potencjału naukowego.

Obszar nieekonomiczny można analizować w ujęciu systemowo-programowym (analiza pozioma) oraz w analizie pionowej, która będzie analizą uzupełniającą. Analiza pionowa obejmie procesy wpływu warunków obronnych na decyzje polityczne, a zwłaszcza na doktrynę i strategię obronną. Centralnym punktem tej analizy stanowi państwowy mechanizm bezpieczeństwa narodowego, a w szczególności stopień zintegrowania systemu politycznego wokół problemów bezpieczeństwa narodowego.

Niestety niski stopień zintegrowania systemu politycznego opóźnia w polskich warunkach procesy dostosowawcze do współcześnie istniejących warunków polityczno-ekonomicznych, przez co zostają powiększone społeczne koszty reform gospodarki obronnej. Stopień zintegrowania systemu politycznego wokół problemów bezpieczeństwa narodowego w Polsce charakteryzuje prowadzenie sporów na temat podziału kompetencji pomiędzy poszczególne organy państwa.

Rozbieżności kompetencyjne, które się utrzymują w polskim systemie politycznym znacznie spowalniają procesy restrukturyzacyjne i rozwojowe w gospodarce obronnej, a także w całym systemie obronnym kraju, gdyż utrudniają koordynację procesów przygotowawczych do mobilizacji gospodarczej, cywilnej

1. Prezydent Rzeczypospolitej Polskiej, który wykonuje swoje zadania w oparciu o Konstytucje RP i inne uchwały, jego kompetencje wynikają z przypisanych obowiązków tj. stania na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium, w tym zakresie jest wspierany przez organ doradczy tj. Radę Bezpieczeństwa Narodowego, ponadto jest Najwyższym Zwierzchnikiem Sił Zbrojnych RP.
2. Rada Ministrów, która także wykonuje swoje zadania w oparciu o Konstytucję i inne uchwały, w jej kompetencjach znajduje się prowadzenie polityki wewnętrznej i zagranicznej RP, zapewnia jej bezpieczeństwo wewnętrzne i zewnętrzne oraz sprawuje ogólne kierownictwo w dziedzinie obronności, kieruje obronnością kraju w czasie pokoju współdziałając z Prezydentem RP. Organem doradczym w tym obszarze jest Komitet Spraw Obronnych Rady Ministrów, w razie konieczności mogą być tworzone dodatkowe struktury (komitety, zespoły, pełnomocnicy itd.) oraz mogą być wprowadzane dodatkowe procedury.

Celem funkcjonowania podsystemu kierowania gospodarką obronną jest przygotowanie gospodarki narodowej do realizacji określonych zadań w okresach zagrożeń dla bezpieczeństwa państwa, a w szczególności w okresach zagrożeń militarnych. Powinno to być realizowane w oparciu o istniejący system prawny.

Stąd wynika, iż podsystem kierowania gospodarką obronną jest w pierwszym rzędzie wypadkową zapisów zawartych w Konstytucji RP dotyczących bezpieczeństwa, następnie przyjętej doktryny obronnej oraz innych ustaw poruszających tę problematykę. Te uwarunkowania narzucają kierunki działań dla władzy ustawodawczej i wykonawczej.

Narzuca to odgórnie następującą strukturę podsystemu kierowania gospodarką obronną, nad całością jego funkcjonowania pieczę posiada: Parlament, Prezydent i Premier (jako kierujący rządem), w tym trójkącie następuje wypracowanie decyzji, ukierunkowanie działań i nadzór ich realizacji w układzie militarnym i pozamilitarnym. Prezydent posiada bezpośredni wpływ na układ militarny (jako Najwyższy Zwierzchnik SZ RP) oraz pośredni poprzez Premiera i Radę Ministrów na układ pozamilitarny.

a) podsystem kierowania gospodarką obronną[232];
b) podsystem mobilizacji gospodarczej[233];
c) podsystem dostosowywania potrzeb obronności kraju do możliwości gospodarki materiałowej.

Podsystem kierowania gospodarką obronną można ująć dwojako:

a) podmiotowo rozumiejąc ją jako zbiór centralnych organów władzy i administracji państwowej, urzędy wojewódzkie oraz organy samorządowe, a także podmioty gospodarcze (bez względu na ich formę własności);
b) przedmiotowo, rozumiejąc ją jako system podejmowania decyzji o kształcie:
   - programów strategicznych oraz średniookresowych;
   - założeń polityki bezpieczeństwa narodowego i obrony kraju;
   - planów rozwoju sił zbrojnych;
   - planów przygotowań obronnych w gospodarce;
   - ustawy budżetowej - tj. budżetu państwa oraz budżetów samorządowych.

Podsystem kierowania gospodarką obronną jest wypracowywany w czasie pokoju, jego głównym zadaniem jest przygotowanie struktur państwa do funkcjonowania w czasach zagrożenia dla bezpieczeństwa kraju w przypadku wystąpienia kryzysu polityczno-militarnego, czy też wojny.

Realizacja kierowania gospodarką obronną jest dokonywana na wszystkich szczeblach struktur państwowych i samorządowych oraz w obszarze gospodarczym, na poziomie podmiotów gospodarczych. Jest to wykonywane w ramach kompetencji posiadanych przez poszczególne szczeble. Kompetencje poszczególnych organów i podmiotów wynikając z ustalonych ram prawnych. Organa wykonujące zadania z tego obszaru są powiązane ze sobą informacyjnie.

Naczelnymi organami władzy wykonawczej w tym obszarze są:

---

[232]Gospodarka obronna – część gospodarki narodowej, zabezpieczająca potrzeby obronne państwa. Obejmuje zasoby osobowe, rzeczowe i finansowe oraz ich użycie zgodnie z zasadami gospodarności. W: *Słownik terminów z zakresu bezpieczeństwa narodowego*, pod red. J. Pawłowskiego, AON, Warszawa 2002, s. 41.

[233]Mobilizacja gospodarki – część mobilizacji powszechnej (narodowej), obejmującej zespół działań związanych z przystosowaniem gospodarki do przejścia i funkcjonowania w warunkach wojennych (przestawienie gospodarki pokojowej na gospodarkę wojenną). Tamże s. 69.

do pragmatyki samo adaptacyjnej cechy systemu kierowania.

Druga funkcja jest w praktyce najtrudniejsza do realizacji, gdyż wymaga odpowiedzenia na pytanie: ile może być wolności gospodarczej w sferze kształtującej bezpieczeństwo państwa w obszarze odpowiedzialnym za przeciwdziałanie zagrożeniom militarnym, politycznym itd.? Trzecia funkcja jest powiązana z dwoma pierwszymi i dotyczy podejmowania działań przez państwo łagodzących negatywne skutki procesów gospodarczych.

By podsystem kierowania gospodarką obronną posiadał odpowiedni poziom skuteczności i efektywności powinien być wewnętrznie spójny. Można to osiągnąć poprzez wprowadzenie procesów koordynacji działań. Koordynacja w tym ujęciu powinna być rozumiana jako pewien proces polegający na integrowaniu zadań i działań szeregu odrębnych organizacyjnie podmiotów w celu osiągania celów nadrzędnych.

Podstawą koordynacji działań jest stworzenie sprawnego systemu przepływu informacji. Koordynacja to w istocie rzeczy sprawny system przepływu i przetwarzania informacji. Wydaje się, iż dla osiągnięcia celów stawianych przed koordynacją istnieje potrzeba stworzenia systemu przesyłania informacji w pionie i poziomie, co spowoduje usprawnienie podsystemu kierowania. Ponadto system kierowania gospodarką obronną powinien uwzględniać specyfikę funkcjonowania gospodarki obronnej w trzech stanach gotowości obronnej:

- pierwszy - stan stałej gotowości obronnej - temu stanowi odpowiada gospodarka narodowa okresu pokojowego. Wówczas to procesy planistyczne i realizacja zamierzeń na rzecz obronności w sferze gospodarczo-politycznej, przekłada się na następujące działania:
  - zaspokajanie bieżących potrzeb sił zbrojnych;
  - przygotowanie obronne wybranych elementów infrastruktury państwa;
  - gromadzenie rezerw państwowych;
  - organizowanie systemów obronny cywilnej.
- drugi - stan podwyższonej gotowości obronnej - temu stanowi odpowiada gospodarka zagrożenia wojennego. Podejmowane są wówczas działania organizacyjno-rzeczowe, które mają zaspokajać zwiększone potrzeby

W skład układu militarnego wchodzi Minister Obrony (będący elementem także układu pozamilitarnego), Sztab Generalny oraz Dowództwa Rodzajów Sił Zbrojnych, a w czasie wojny Naczelny Dowódca Sił Zbrojnych RP (wyznaczany przez Prezydenta na wniosek Prezesa Rady Ministrów). Do układu pozamilitarnego kierowania gospodarką obronną przede wszystkim wchodzą Minister Gospodarki, Minister Finansów, Minister Spraw Zagranicznych, Minister Spraw Wewnętrznych i Administracji, Minister Obrony Narodowej oraz inni Ministrowie zgodnie ze zleconymi zadaniami z tego obszaru. Z wzajemnych relacji i udzielanych kompetencji wyłania się podsystem kierowania gospodarką obronną

Zadania dla podsystemu kierowania gospodarką obronną wypływają z funkcji państwa, jaką jest zapewnienie bezpieczeństwa narodowego. Obejmują one kierowanie bieżącym funkcjonowaniem państwa oraz rozwojem gospodarki obronnej, stosownie do potrzeb obronnych państwa. Są one realizowane niezależnie od konkretnych rozwiązań ustrojowych, ponieważ zmieniają się jedynie sposoby realizacji tych i zadań. Zadania te są realizowane przy oddziaływaniu mechanizmów rynkowych i ostatecznym formowaniu się ustroju społeczno-gospodarczego.

Podsystem kierowania gospodarką obronną jest wypadkową trzech funkcji państwa:

- publicznej sprowadza się do „zapewnienia bezpieczeństwa narodowego", która obejmuje następujące zadania:
  - kierowanie bieżącym funkcjonowaniem gospodarki obronnej,
  - kierowanie rozwojem gospodarki obronnej,
  - kierowanie samo adaptacją systemu kierowania;
- kształtowania infrastruktury rynkowej w gospodarce obronnej;
- interwencjonizmu państwowego.

Poprzez wypełnianie tych funkcji przez państwo będzie następowało kształtowanie procesów gospodarczych i ukierunkowywanie działań podmiotów gospodarczych w obszarze gospodarczo-obronnym. Należy podkreślić w odniesieniu do pierwszej funkcji, iż kierowanie bieżącym funkcjonowaniem gospodarki obronnej odnosi się do jej systemu wykonawczego, kierowanie jej rozwojem przekłada się na kształtowanie systemu wykonawczego, jak i wdrożenie

realnej spadek wartości waluty itd. Chodzi o to, aby przyjęte plany kształtowania polityki obronnej kraju posiadały zabezpieczenie finansowe dla osiągnięcia założonych celów.

Kolejnym elementem systemu kierowania gospodarczymi podstawami obronności jest podsystem mobilizacji gospodarczej. Podsystem mobilizacji gospodarczej powinien charakteryzować się cechami: elastycznością gospodarki narodowej, niepodzielnością czynników produkcji, adekwatność zasobów będących w dyspozycji, żywotność gospodarki narodowej

Elastycznością gospodarki narodowej, jest jej zdolność do osiągania kolejnych szczebli gotowości w czasie. Polega to na możliwościach dokonywania zmian w wymiarze organizacyjnym, technicznym itd. zgodnie z zaistniałym zagrożeniem. Duże znaczenie na poziom elastyczności gospodarki narodowej mają powiązania gospodarcze z innymi rynkami. Duży wpływ na elastyczność posiada **niepodzielność czynników produkcji** w gospodarce narodowej. Należałoby go traktować jako samodzielny czynnik, o dużym wpływie na podsystem mobilizacji gospodarczej.

Adekwatność zasobów będących w dyspozycji gospodarki narodowej, która także jest bezpośrednio powiązana z elastycznością, w znacznym stopniu decyduje o poziomie i strukturze zaspokojenia potrzeb obronnych. Od jej poziomu zależą możliwości zaspakajania potrzeb obronnych w stanach zagrożeń dla bezpieczeństwa kraju.

Żywotność gospodarki narodowej, jest także określana jako odporność gospodarki na oddziaływanie przeciwnika, a także jako zdolność do przezwyciężania wynikłego z zagrożeń trudności. Czynnik ten decyduje o stopniu zaspokojenia potrzeb obronnych w trakcie trwania konfliktu. Podsystem mobilizacji gospodarczej składa się z trzech następujących elementów:

- mobilizacji zasobów ludzkich;
- mobilizacji aparatu wytwórczego;
- wykorzystanie rezerw i zasobów mobilizacyjnych.

Mobilizacja zasobów ludzkich na rzecz obronności kraju będzie przebiegała dwukierunkowo, część zasobów zostanie skierowana na potrzeby fizycznej obrony, pozostała część będzie wykorzystywana dla potrzeb gospodarki

sfery obronnej przy jednoczesnej realizacji zadań odpowiadających stałej gotowości bojowej, ewentualnie wprowadzane są ograniczenia popytu, mogą one obejmować:

- zaspokajanie bieżących potrzeb sił zbrojnych;
- zaspokajanie mobilizacyjnych i wojennych potrzeb sił zbrojnych;
- przygotowanie obronne wybranych elementów infrastruktury państwa;
- obronne wykorzystywanie infrastruktury państwa;
- gromadzenie rezerw państwowych;
- wykorzystywanie rezerw państwowych dla potrzeb obronnych państwa;
- organizowanie systemów obrony cywilnej;
- przygotowanie i wykorzystywanie systemów obrony cywilnej na potrzeby obronności;
- reglamentacja towarów i wyrobów.

- trzeci - stan pełnej gotowości obronnej - temu stanowi odpowiada gospodarka wojenna. Wówczas jest wprowadzany nakazowo-rozdzielczy system zarządzania gospodarką narodową, odgórnie ogranicza się popyt na rynku wewnętrznym, braki są uzupełniane z rezerw państwowych.

Kontynuowane są następujące działania w sferze gospodarczej:

- zaspokajanie mobilizacyjnych i wojennych potrzeb sił zbrojnych;
- obronne wykorzystanie infrastruktury państwa;
- wykorzystanie rezerw państwowych dla potrzeb obronnych państwa;
- wykorzystanie systemów obronny cywilnej;
- reglamentacja towarów i wyrobów.

Ważną kwestią dla skuteczności działań z obszaru kierowania gospodarką obronną jest ustalenie w perspektywie długookresowej tj. min. 10-15 lat poziomu nakładów na obronność. Prognozowane plany finansowe powinny określać procentowo poziom udziału wskaźnika nakładów na obronność w produkcie krajowym brutto. Można taki wskaźnik ustalić także w stosunku do budżetu państwa. Jednak należałoby go obłożyć dodatkowymi rygorami, które niwelowałyby realne spadki nakładów na tę sferę tj. uwzględniające inflację,

wskazuje, iż potrzeby obronne będą głównie mogły być zaspokajane z trzech źródeł: istniejącego potencjału rodzimego przemysłu zbrojeniowego, importu i posiadanych rezerw.

Wykorzystanie rezerw i zapasów mobilizacyjnych jest ważnym elementem w gospodarce obronnej. W Polsce, podobnie jak w innych krajach z ogółu posiadanych zasobów można wyróżnić dwa jego elementy: zasoby wykorzystywane i nie wykorzystywane. Jeżeli pojęcie zasobów wykorzystywanych jest jednoznaczne, to przyczyn niewykorzystywania można dopatrywać się w różnych źródłach. Może to wynikać ze świadomej działalności, kiedy pozostawia się część zasobów w rezerwie na wypadek wystąpienia określonych zagrożeń lub jest to wymuszone sytuacją rynkową. Część zasobów jest nie wykorzystywana nieświadomie, wynika to w znacznym stopniu z wadliwej organizacji podmiotów gospodarczych. W wyniku świadomej działalności z zasobów wyodrębnione są rezerwy państwowe, na które składają się rezerwy gospodarcze i obronne.

Stanowią one bardzo ważny i jednocześnie bardzo mobilny czynnik zaspokajania potrzeb obronnych. Ponadto można dopatrywać się z punktu widzenia obronności istnienia rezerw potencjalnych tj. rezerw, które zostały stworzone z myślą o zabezpieczeniu różnych funkcji państwa i jednocześnie są podwójnego zastosowania (gospodarczo-obronnego). Współcześnie zauważalnym trendem jest dawanie priorytetu rezerwom gospodarczym, jednak w krajach wysokorozwiniętych dużą uwagę także poświęca się rezerwom obronnym. Wydaje się, iż różnice pomiędzy rezerwami obronnymi o gospodarczymi w obecnej dobie będą się zacierały w wielu obszarach, jedyne różnice pozostaną w artykułach posiadających wyraźną i specjalizację.

Ponadto duży wpływ na kształt rezerw będą miały rezerwy domowe, w szczególności w stanach zagrożenia wojennego oraz krótkotrwałych konfliktach. Wielkość oraz różnorodność rezerw domowych będzie się przekładać na:

- ograniczenie wzrostu cen dóbr konsumpcyjnych;
- zwiększenie odporności społeczeństwa na trudności spowodowane konfliktem;
- ułatwienie konwersji gospodarki czasu pokoju na gospodarkę wojenną;
- zmniejszenie „parcia" społecznego na dostępność rezerw kosztem

wojennej, czy też gospodarki pogotowia wojennego. Efektem tego będzie zmiana proporcji pomiędzy strukturą zatrudnienia, a zaangażowaniem na rzecz sił zbrojnych. Ponadto będzie temu towarzyszyć uaktywnienie ludności dotychczas biernej zawodowo np. szersze wykorzystanie kobiet. Poziom mobilizacji zasobów ludzkich będzie zależał od takich czynników jak: skala zagrożenia, prędkość rozwoju sytuacji, długotrwałości konfliktu.

Możliwości mobilizacji zasobów ludzkich będą dodatkowo ograniczane w znacznym stopniu takimi cechami jak przydatność gospodarcza poszczególnych grup zawodowych oraz możliwością zapewnienia przez nie wydajnością produkcji. Zapewnienie pożądanego poziomu mobilizacji zasobów ludzkich będzie wymagało wprowadzenia szeregu rozwiązań w sferze prawnej tj.:

- powszechnego obowiązku pracy;
- ograniczenia praw pracowniczych np. wydłużenie czasu pracy, ograniczenie prawdo urlopu, zakaz strajków itd.;
- stworzenia planowego systemu zatrudnienia.

Mobilizacja aparatu wytwórczego to wykorzystywanie maszyn, urządzeń, instalacji itd. na rzecz obronności, które do tego momentu były wykorzystywane w sferze pozamilitarnej gospodarki. Z tego punktu widzenia aparat wytwórczy posiada następującą cechę - różny poziom przydatności dla gospodarki obronnej. Wynika to z dwóch aspektów:

- poziomu technologicznego i technicznego aparatu wytwórczego, jego struktury przedmiotowej i przestrzennej;
- charakteru konfliktu.

Szczególną rolę w tym obszarze posiada przemysł zbrojeniowy, gdyż to dla jego produktów „wzrasta chłonność rynku". Ponadto jako pierwszy jest w stanie zaspokajać rosnące potrzeby obronne, poprzez intensyfikacje produkcji. Powiększenie mocy produkcyjnych w pierwszej kolejności zostanie uzyskany kosztem ograniczonej lub całkowicie wyeliminowanej produkcji cywilnej. Ponadto stanowi zaplecze wyspecjalizowanej kadry dla zakładów przechodzących z produkcji cywilnej na produkcję wojenną. Może być także przygotowany do udzielenia pomocy technicznej dla innych zakładów podejmujących produkcję na rzecz wojska. Przewidywana dynamika współczesnych konfliktów zbrojnych

gospodarcze wynikające z zachodzących przemian w Siłach Zbrojnych RP i restrukturyzacji całego sektora zbrojeniowego. Ponadto można spojrzeć na przemysł obronny jako element obciążający system gospodarczy lub element wspierający jego rozwój. Jeżeli podejdzie się do tego obszaru w sposób statyczny, czyli kreowanie przemysłu obronnego głównie z myślą o zaspokojeniu własnych potrzeb obronnych będzie tworzyło jedynie obciążenie dla systemu gospodarki narodowej.

Natomiast, jeżeli spojrzeć na przemysł obronny jako kompilacja produkcji specjalnej i cywilnej, który w swych działaniach będzie wspierany przez państwo szczególnie w działaniach eksportowych w pierwszym obszarze produkcji może się to przekładać na stworzenie silnej gałęzi przemysłowej o dużym znaczeniu dla rozwoju gospodarczego kraju. Silny przemysł obronny może być, podobnie jak w gospodarce amerykańskiej, francuskiej i niemieckiej, motorem postępu naukowego i technologicznego dla przemysłu krajowego.

Infrastruktura gospodarczo-obronna jest wypadkową będących w dyspozycji urządzeń, systemów oraz funkcjonujących w państwie instytucji. Składają się na nią następujące podsystemy:

- kierowania państwem;
- przepływu informacji;
- infrastruktury gospodarczej.

Podsystem kierowania państwem jest odwzorowaniem filozofii jego i zarządzania, która wynika z istniejącego systemu politycznego, a także sytuacji międzynarodowej i wewnętrznej kraju. Przez ten podsystem należy rozumieć instytucje reprezentujące, czy też realizujące interesy państwa, a są nimi instytucje centralne, terenowe administracji rządowej oraz instytucje samorządowe oraz system współpracy pomiędzy nimi, a także innymi podmiotami życia gospodarczego i państwowego. To od przyjętej filozofii zarządzania państwem zależy, czy będzie to system scentralizowany, czy też zdecentralizowany i jaki będzie zakres swobody w podejmowaniu decyzji na poszczególnych jego szczeblach. Ponadto będzie z niego wynikał sposób i zakres przekazywania kompetencji w różnych obszarach funkcjonowania państwem (szkolnictwie, ochronie zdrowia, pomocy społecznej, przeciwdziałaniu bezrobociu, obronie

obronności.

Zasoby i rezerwy będące w dyspozycji państwa decydują o jego możliwościach przetrwania, reorganizacji w okresie konfliktu i odbudowy oraz rozwoju po jego zakończeniu. Bezpośrednio przekładają się na możliwości obronne, a także w znacznym stopniu rzutują na możliwości podsystemu mobilizacji gospodarczej.

Kolejnym elementem tego podsystemu jest podsystem dostosowania potrzeb obronności kraju do możliwości gospodarki materiałowej. Na niego - składa się szereg instytucji funkcjonujących w obszarze obronnym, gospodarczym i na pograniczu obu obszarów, a także wchodzący w ich skład ludzie i urządzenia. Jest to element planistyczno kontrolny całego systemu, którego zadaniem jest zapobieganie powstawaniu wektorów sił o przeciwstawnych kierunkach, które wywodziłyby się z systemu obronnego i gospodarczego.

System gospodarki wojennej w znacznej mierze decyduje o sile, odporności, mobilności gospodarki obronnej oraz o możliwościach zaspokojenia potrzeb obronnych państwa. W skład tego systemu wchodzą takie elementy gospodarki narodowej jak: przemysł obronny, infrastruktura gospodarczo-obronna, rezerwy gospodarczo-obronne, postęp naukowo-techniczny oraz międzynarodowa współpraca gospodarczo-obronna.

Kształt przemysłu obronnego powinien być uzależniony od wyzwań militarnych stojących przed państwem, międzynarodowych powiązań gospodarczo-politycznych, a także możliwości technologicznych gospodarki narodowej.

Dla rozważań na temat przemysłu obronnego w systemie gospodarki obronnej można przyjąć następujący podział przedsiębiorstw realizujących zadania w tym obszarze:

- typu A: produkujące artykuły mające zastosowanie w sferze gospodarczej i obronnej;
- typu B: produkujące artykuły mające zastosowanie wyłącznie w sferze obronnej.

Wydaje się, iż główną uwagę należałoby skoncentrować na przedsiębiorstwach typu B, gdyż to przed nimi stoją poważne wyzwania

obronna, czyli od rozwoju struktur gospodarczych zależy poziom i jakość struktur obronnych. Dlatego współcześnie wydaje się bardzo ważne tworzenie takiej infrastruktury, która konstruowana z myślą o potrzebach gospodarczych realizowałaby także potrzeby obronne.

Z tych powodów wydaje się także ważne stworzenie spójnego podejścia do tej problematyki poprzez podsystem kierowania państwem. Jednako ważnym z punktu widzenia sfery gospodarczej, jak i obronnej jest zapewnienie funkcjonowania następujących obszarów:

- łączności: w tym łączności stacjonarnej, komórkowej, Internetu, a także nowości na tym rynku UMTS;
- sieci drogowej: w tym sieci dróg lokalnych, ekspresowych i autostrad;
- sieci połączeń kolejowych;
- sieci innych połączeń będących uzupełnieniem dla sieci drogowej i kolejowej;
- infrastruktury proekologicznej tj. oczyszczalni ścieków, nowoczesnych zwałowisk śmieci itd.

Bezpośredni wpływ na realizację procesów w obszarze bezpieczeństwa ekonomicznego posiadają uwarunkowania infrastrukturalne. Wpływają one na i kształtowanie się ich jego, w następujących wymiarach:

- w wymiarze ekonomicznym - koncentrując się na problemie niepodzielności nakładów w skali zaangażowania poszczególnych rodzajów kapitału, pracochłonności i kapitałochłonności przedsięwzięć, a także na kwestie zmian jakościowych;
- w wymiarze społecznym - koncentrując się na działaniach administracji państwowej i samorządowej na rzecz zapewnienia pożądanej sytuacji prawno-ekonomicznej społeczeństwa;
- w wymiarze techniczno - organizacyjnym są odpowiedzialne za realizację zarządzania i koordynowania procesów kształtowania bezpieczeństwa ekonomicznego, a także kształtowanie cech niezbędnych do realizacji tych przedsięwzięć tj. dużej mobilności, żywotności przestrzennej, jedności funkcjonalnej itd.

Uwarunkowania infrastrukturalne winny zapewniać rozwiązania, które sprzyjałyby

cywilnej itd.), co będzie warunkować sposób realizacji zadań z zakresu bezpieczeństwa w ujęciu gospodarczym, jak i obronnym. Podsystem kierowania państwem narzuca sposoby przypływu i formy przepływu informacji w pionie i w poziomie, formy organizowania się samorządów różnych szczebli, a także sposób współpracy pomiędzy organami samorządowymi i rządowymi.

Podsystem funkcjonowania państwem w Polsce przeszedł, czy też nadal przechodzi ewolucyjnie od systemu centralistycznego do systemu zdecentralizowanego. Coraz więcej kompetencji jest przekazywane na niższe szczeble zarządzania państwem. Następuje silna integracja struktur państwowych w poziomie, szczególnie odnosi się to do struktur samorządowych, przy zachowaniu wystarczających powiązań w pionie.

Dużym problemem wydaje się nadmierny rozrost administracji rządowej i samorządowej, która wymaga na swoje funkcjonowanie coraz większych nakładów finansowych, a przy tym staje się coraz bardziej w swych działaniach skostniała tj. wydłużane są i komplikowane są sposoby podejmowania decyzji, brakuje jednoosobowej odpowiedzialności za podejmowane decyzje, a wręcz widoczne jest unikanie jej, za decyzję ponosi jedynie odpowiedzialność urząd, a nie ją podejmujący.

Jednak ten problem nie leży w głównym nurcie rozważań, bowiem jest nim zakres kompetencji poszczególnych jednostek tworzących ten podsystem, sposoby realizacji zadań i cedowania ich na niższe szczeble, a także możliwości ich egzekwowania.

Ponadto na możliwości realizacji zadań przez ten podsystem nakładają się możliwości pozostałych dwóch systemów z tego obszaru tj. przepływu informacji - rozumianego jako posiadane możliwości techniczne przesyłania informacji w obszarze państwa, jak i poza niego oraz infrastrukturę gospodarczą - która jest w znacznym stopniu wypadkową dwu pierwszych.

Po pierwsze poziom rozwoju infrastruktury gospodarczo-obronnej decyduje o poziomie zainteresowania całym obszarem państwa lub jego częścią przez inwestorów krajowych i zagranicznych.

Po drugie infrastruktura gospodarczo-obronna to przede wszystkim infrastruktura gospodarcza, z której obszaru może być generowana infrastruktura

3.2. Postulowany model kształtowania bezpieczeństwa ekonomicznego państwa i wymagania w zakresie rozwoju infrastruktury telekomunikacyjnej kraju

Bezpieczeństwo ekonomiczne można traktować jako określony stan, jako narzędzie niezbędne do osiągnięcia danych celów, czy jako weryfikator dla innych obszarów działalności państwa. W tym wypadku bezpieczeństwo ekonomiczne jest traktowane jako narzędzie i weryfikator.

W pierwszej kolejności należy zadać sobie pytanie: wobec jakich obszarów wysuwa bezpieczeństwo ekonomiczne postulaty podejmowania określonych działań, utrzymywania danego stanu itd.?

Dla celów prowadzonej analizy można wyodrębnić obszary, które powinny realizować zadania na rzecz bezpieczeństwa ekonomicznego pozostającego w korelacji ze strategią obronną i funkcjonującą na jego rzecz. Są nimi: obszary nieekonomiczny, w którym kreowane są zadania polityczne, społeczne i naukowe; oraz obszar ekonomiczny obejmujący gospodarkę narodową, wymianę międzynarodową, finanse publiczne oraz infrastrukturę gospodarczą.

Bezpieczeństwo ekonomiczne kieruje do obu obszarów innego rodzaju postulatywne wymagania. Do obszaru nieekonomicznego wysyłany jest postulatywny sygnał pożądania poparcia dla realizacji, czy też osiągania określonych celów na rzecz strategii obronnej. Natomiast wobec obszaru ekonomicznego wysuwane są postulatywne wymagania zaspakajania określonych potrzeb w formie zasilania rzeczowego i finansowego. Należy zaznaczyć, iż oba obszary zachodzą na siebie wytwarzając wspólną przestrzeń, której „zabarwienie" zależy od przeważania danego obszaru. Ukazuje nam ona, czy sfera nieekonomiczna, czy też ekonomiczna uzyskuje rolę dominującą na danym etapie rozwoju państwa, społeczeństwa i gospodarki. Współcześnie wydaje się, iż dominantom w tym układzie jest sfera ekonomiczna, gdyż to ona determinuje kierunki rozwoju nie tylko gospodarczego, ale także kulturowego we współczesnym świecie.

Co to oznacza dla bezpieczeństwa ekonomicznego? Pierwotnym obszarem, który będzie decydował o poziomie zaspokojenia postulowanych potrzeb zgłaszanych przez bezpieczeństwo ekonomiczne będzie obszar ekonomiczny, który decyduje o kształcie politycznym, społecznym, kulturowy i kierunkach rozwoju

rozwojowi poziomu bezpieczeństwa jednostki, podmiotów gospodarczych, gałęzi przemysłu, aż do bezpieczeństwa państwa.

Przynależność Polski do NATO i wynikająca z tego rola państwa-gospodarza stawia w pierwszej kolejności dokonania bilansu zobowiązań i korzyści wynikających z tego faktu. Wynikające z położenia geograficznego Polski miano kraju frontowego, przyjęte zobowiązania sojusznicze oraz umowy dwu i wielostronne z poszczególnymi partnerami z koalicji powodują konieczność rozstrzygnięcia szeregu dylematów o charakterze politycznym, ekonomicznym, militarnym i społecznym. Prognozowane zagrożenia dla bezpieczeństwa Polski, jak i innych państwa należących do NATO zakładają konieczność rozmieszczenia na jej terytorium wojsk sojuszniczych lub przemieszczania się ich. Rodzi to potrzebę dokonywania prognoz odnośnie ilości i czasu w realizowaniu powyższych działań.

Udzielenie odpowiedzi na następujące pytania pozwoli dostosować infrastrukturę gospodarczo-obronną polski do wypełniania roli państwa-gospodarcza:

- jakie i o jakiej skali są przewidywane zagrożenia militarne dla Polski i Sojuszu, które będą wymagały wykorzystania terytorium naszego kraju?;
- jakiego zaangażowania sił sojuszniczych będą wymagały przewidywane konflikty?;
- jakie będą przewidywane potrzeby zaangażowanych sił zbrojnych w systemie obronności państwa?

Rozstrzygnięcie wskazanych dylematów może nastąpić w tym obszarze w wyniku ścisłej współpracy pomiędzy Polską i jej koalicjantami. Będą zapewne wypadkową obowiązujących w NATO procedur planistycznych. Ponadto rozstrzygnięcie problemów wynikających z funkcji państwa - gospodarza nie można rozpatrywać jedynie z punktu widzenia bezpieczeństwa militarnego, bowiem konieczność poniesienia nakładów na stworzenie odpowiednie infrastruktury będzie się także przekładało sferę gospodarczą, która w wielu dziedzinach będzie aktywnie uczestniczyć w jej tworzeniu. Może to mieć także korzystny wpływ na rozwój szeregu regionów Polski.

Oznacza to, iż wola i naciski generowane z obszaru ekonomicznego będą decydowały o kierunku działań polityki, kierunkach rozwoju nauki, a w sposób pośredni na społeczeństwo, jego wolę i poziom akceptacji dla postulatów stawianych przez bezpieczeństwo ekonomiczne wynikające z korelacji ze strategią obronną. Choć omawiany model jest zdeterminowany przez stronę ekonomiczną, to nie bez znaczenia jest sfera nieekonomiczna. Bezpieczeństwo ekonomiczne zgłasza wobec tego obszaru wymagane racją stanu sygnały o poziomie zapotrzebowania na przepływ od obszaru gospodarczego do obszaru obronnego (szeroko rozumianego - nie tylko wojskowego) zasobów rzeczowych i finansowych. Pierwszym elementem odbierającym te sygnały jest podsystem polityczny, wówczas postulatywne pożądanie, czy też zapotrzebowanie rodzi określony proces analityczny weryfikujący sygnały kierowane z obszaru bezpieczeństwa ekonomicznego. Dla pozytywnego rozpatrywania postulatywnego pożądania wymagane jest, aby podsystem polityczny wykazał zrozumienie i wolę do realizacji tych potrzeb.

W tym momencie powstaje szereg komplikacji, gdyż podsystem polityczny posiada dwa obszary zasilania, które z kolei rodzą dwa główne strumienie zasilania, a ich poziomy zależą od stopnia integralności celów. Pierwszym obszarem i jednocześnie podsystemem obszaru nieekonomicznego jest społeczeństwo. To od poziomu akceptacji społecznej dla podsystemu politycznego zależy jego trwanie i forma. Poziom akceptacji społecznej decyduje o poziomie możliwych wyrzeczeń lub przyzwolenia na realizowanie planów akceptowalnych przez podsystem polityczny. Czyli poziom realizacji postulatywnych pożądań zgłaszanych przez bezpieczeństwo ekonomiczne zależy od poziomu spójności pomiędzy podsystemem politycznym i społecznym. Odnosi się to do systemów politycznych, w których brany jest pod uwagę „głos ludu" - bez rozstrzygania, z jakich powodów jest to czynione.

Na poziom akceptowalności społecznej nakładają się dwa wyodrębnione w modelu elementy tj. kultura i nauka. Trendy kulturowe występujące w danym społeczeństwie posiadają niepośledni wpływ na poziom skłonności społecznej i politycznej do akceptacji szeregu postulowanych działań z obszaru obronności, podnoszenia poziomu bezpieczeństwa narodowego w ujęciu wieloaspektowym, a nie tylko w sensie bytu ekonomicznego. Ten aspekt posiada także bezpośrednie

nauki. To od zrozumienia celowości postulowanych wymagań stawianych przez obszar ekonomiczny w znacznej mierze zależy poziom ich zaspokojenia. Należy przy tym zaznaczyć, iż nie jest to proces jednolity w skali systemu gospodarczo-politycznego świata. Widoczna jest zależność od poziomu rozwoju gospodarczego i dynamiki wzrostu gospodarczego. Im kraj wyżej rozwinięty, a także utrzymujący dynamikę na poziomie zapewniającym oddalenie groźby recesji gospodarczej tym większe znaczenie i wpływ sfery gospodarczej na funkcjonowanie państwa. Im mniej rozwiniętej gospodarki, tym więcej polityki w życiu gospodarczym. Oczywiście jest to założenie modelowe i nie można go w pełni odnieść do tzw. trzeciej drogi rozwojowej.

Odnosząc ten problem do warunków polskich zauważalnym elementem determinującym wszelkie poczynania jest transformacja systemowej. Widoczne są różnice pomiędzy systemem politycznym i gospodarczym na początku lat dziewięćdziesiątych i przełomie wieków, jednak nadal jest to proces nie zakończony. Jeżeli przyjąć, iż system polityczny w Polsce już przyjął ogólne docelowe kształty, czy też ramy funkcjonowania, to proces kształtowania systemu gospodarczego nie można uznać za zakończony. Powoduje to spowalnianie procesów formowania się grup społecznych.

Polska znajduje się na wpół drogi pomiędzy przewagą elementu nieekonomicznego a ekonomicznego. Poprzedni ustrój polityczno-gospodarczy preferował element nieekonomiczny jako zarządzający państwem. Natomiast współcześnie widoczna jest tendencja do przekazania tej roli elementowi ekonomicznemu. Wpływa na ten trend wiele czynników między innymi:

- przejście od gospodarki centralnie zarządzanej do gospodarki rynkowej;
- gospodarcze otwarcie się kraju;
- naciski zewnętrzne wynikające z coraz większego powiązania gospodarki narodowej z gospodarką światową;
- istnienie silnego podobnego trendu w światowym systemie gospodarczo-politycznym;
- członkostwo lub dążenie do członkostwa w organizacjach międzynarodowych popierających ten model np. OECD, MFW, UE itd.

zwiększenia konsumpcji indywidualnej. Jest to jeden z głównych nacisków, który ogranicza i będzie ograniczał poziom postulowanych żądań generowanych przez bezpieczeństwo ekonomiczne. Można nazwać to zjawisko swoistym rodzajem nacisku, który mówi albo będziemy czynili maksymalnie wysokie nakłady na rozwój gospodarczy kosztem innych dziedzin, albo ograniczymy je kosztem tychże dziedzin wydłużając drogę do zaspokojenia potrzeb konsumenckich, w domyśle znajduje się możliwość nadrobienia niedociągnięć w innych dziedzinach w późniejszych okresach - po osiągnięciu odpowiednio wysokiej stopy rozwojowej. Jednak powstaje w tym momencie pytanie: czy kiedykolwiek zostanie osiągnięta ta wymarzona stopa rozwoju gospodarczego - a może jest to droga bez końca? Oczywiście należy się liczyć z tym, że im niższy poziom rozwoju gospodarczego i niższa dynamika tego procesu tym większa siła przeciwstawna do postulowanych potrzeb przez bezpieczeństwo ekonomiczne. Bowiem potrzeby zgłaszane przez społeczeństwo oraz różnego rodzaju naciski ze strony konkurencji zewnętrznej powodują pragnienie czynienia odpowiednich nakładów na sferę gospodarczą, która jest pierwotna dla wymiany międzynarodowej, finansów publicznych i infrastruktury gospodarczej. Im będzie występował większy „poziom głodu" w sferze gospodarczej na nakłady rzeczowe i finansowe, tym większe będą wysyłane sygnały o możliwości przesunięcia nakładów z innych obszarów funkcjonowania państwa, które będą uznawane za nieprodukcyjne. Sygnały te będą wzmacniane poprzez słabość finansów publicznych, które dla społeczeństw przyzwyczajonych do określonego poziomu opieki, czy też pomocy ze strony państwa będzie wskazywało na utrzymanie ich na dotychczasowym poziomie kosztem sfer wskazywanych przez obszar bezpieczeństwa ekonomicznego. Szczególnie mocno odnosi się to do państwa posiadające poziom rozwoju gospodarczego podobny do poziomu rozwoju Polski, które przechodzą transformację ustrojową. Społeczeństwo polskie jest „spragnione" dobrobytu, a przy tym dobrze pamięta zakres osłon proponowanych przez państwo socjalistyczne. Kondycja finansów publicznych w krajach przeobrażających system gospodarczy jest słaba przy jednocześnie istniejących dużych potrzebach czynienia wysokich nakładów na infrastrukturę gospodarczą kraju jej, bowiem wymagają inwestorzy chętni do podjęcia działalności na terenie Polski. Bez udziału

przełożenie na sferę polityczną, która jest przecież wyłoniona ze społeczeństwa. Ponadto element nazwany naukowym posiada ujęcie wielowymiarowe poczynając od poziomu i obszaru nauczania skończywszy na postępie techniczny. Choć są one ze sobą powiązane to jednak mówią o nakładach na szkolnictwo i jego dostępność i nakładach na postęp techniczny, w pewnym sensie one są odwzorowaniem poziomu rozwoju przemysłowego państwa. Posiadają one wpływ na poziom rozwoju intelektualnego, kulturowego i ekonomicznego rozwoju społeczeństwa, a przez to decydują o skłonnościach sfery społecznej, a także politycznej do podejmowania i zrozumienia sensu działań w obszarze bezpieczeństwa ekonomicznego.

Ze wzajemnych powiązań poszczególnych elementów obszaru nieekonomicznego, a można powiedzieć, iż w ich wyniku rodzi się określona wola potrzeba do podejmowania działań na rzecz wspierania pozyskiwania środków ze sfery ekonomicznej na rzecz utrzymywania odpowiedniego poziomu bezpieczeństwa ekonomicznego z punktu widzenia jego powiązań ze strategią obronną. Działania i skłonności, które są w tym celu wykorzystywane przez sferę nieekonomiczną składają się na obszar wspólny tworzony z obszarem ekonomicznym.

Obszar ekonomiczny posiada kilka głównych składowych, do którego są kierowane wymagania ze strony bezpieczeństwa ekonomicznego, a w szczególności z punktu widzenia jego funkcjonowania na rzecz strategii obronnej. Wytworzenie, czy też wygenerowanie woli do skierowania części zasobów rzeczowych na rzecz sfery obronnej, a nie na pomnażanie kapitału odtowrzeniowo-inwestycyjnego przebiega w pierwszym rzędzie pośrednio tzn. poprzez obszar nieekonomiczny. Można ten proces nazwać racjonalnym zrezygnowaniem z zysków o wymiarze jedynie w ujęciu ekonomicznym na rzecz zysków o wymiarze znacznie szerszym, a wymiernym w długich okresach tj. 10-20 lat i posiadających charakter ekonomiczny, społeczny i militarny oraz polityczny. Jednak we współczesnym świecie trudnym do przekonania jest w krajach będących na dorobku o słuszności takich działań. Wynika to z faktu, iż w gospodarkach tego typu istnieje brak środków rzeczowych i finansowych na zaspokojenie potrzeb rozwojowych gospodarki, a w domyśle podniesienie stopy życia w społeczeństwie, czyli

wyprowadzić krąg wzajemnych powiązań, który ukazuje nam kierunki tego zjawiska. W zależności od uznania za obszar pierwotny gospodarki lub polityki procesy będą posiadały przeciwstawny wektor oddziaływania,

Jeżeli pierwotnym obszarem będzie polityka wówczas wektory ukazujące kierunki oddziaływania będą przebiegały od polityki poprzez strategię obronną, bezpieczeństwo ekonomiczne do gospodarki. Natomiast, gdy obszarem pierwotnym stanie się gospodarka wektor będzie miał przeciwstawny kierunek do sytuacji poprzedniej. Powstaje w tym momencie pytanie: dlaczego tak się dzieje? Wynika to z faktu określenia determinanta danego procesu, jeżeli będzie nim polityka to w tym momencie wyznaczanie celów, które należałoby osiągnąć będą generowane poprzez perspektywę działań doraźnych potrzeb i sukcesów. Wówczas to obszar polityczny będzie kreował w dużym stopniu rzeczywistość gospodarczą.

Natomiast w wypadku, gdy dominantom będzie gospodarka wektory przebiegających procesów będą miały kierunek od gospodarki poprzez bezpieczeństwo ekonomiczne, strategię obronną do polityki. Można powiedzieć, iż ustalanie procedur, celów i mechanizmów działania w państwie będzie formułowane poprzez perspektywy szans, możliwości i woli wynikającej z części gospodarczej. Wola obszaru gospodarczego będzie realizowana poprzez narzucanie możliwości i zakresu działania na coraz wyższych szczeblach poczynając od najbardziej zależnych od gospodarki do zależnych jedynie w pewnym sensie pośrednio.

W obu przypadkach będzie przychodził sygnał zwrotny, czy to od sfery gospodarczej, czy to od sfery politycznej, ale będzie posiadał zawsze kierunek zgodny z całym procesem zachodzącym w państwie. Należałoby zauważyć jeszcze jeden element tych procesów, a mianowicie wynikające z nich i zachodzące jednocześnie sprzężenia zwrotne pomiędzy poszczególnymi elementami tegoż zjawiska. Siła tych sprzężeń zależy od wielu aspektów, które będą zależne i niezależne od nich. Zależne będą przede wszystkim te aspekty, których kształt, czy też forma będzie wynikała z zasad wynikających z wewnętrznych rozwiązań poszczególnych elementów np. poziom rezerw państwowych, zdolność do przeciwstawienia się powstałym zagrożeniom, system prawny itd. Duży wpływ na poziom zależności posiada czynnik zewnętrzny, który może wpływać na

bezpośrednich inwestycji zagranicznych system gospodarczy wykazuje brak odpowiednio wysokich własnych nakładów inwestycyjnych, które mogłyby stworzyć konkurencyjny system gospodarczy na arenie międzynarodowej, a przede wszystkim w ujęciu regionalnym. Niestety potrzebę istnienia elementu bezpieczeństwa można dostrzec wyraziście w wymianie handlowej przy założeniu aktywnego uczestnictwa państwa w tym podsystemie. W polskim systemie gospodarczym także podsystem wymiany międzynarodowej został pozostawiony prawu „niewidzialnej ręki rynku", państwo znacznie ograniczało swój udział w spieraniu międzynarodowej wymiany gospodarczej czynionej przez rodzime podmioty gospodarcze. Był to jeden z powodów, z których przychylił się do tego, aby system gospodarczy utracił w dużym stopniu sens wspierania we wszelkich wymiarach postulatów zgłaszanych przez bezpieczeństwo ekonomiczne, które wynikałyby z jego powiązań ze strategią obronną. W polityce reprezentowanej przez kolejne rządy praktycznie nie zaistniał nurt, który wspierałby działania gospodarcze poprzez działania polityczne oparte na silnych podstawach bezpieczeństwa ekonomicznego i bezpieczeństwa militarnego. Jeżeli nie starano się wykorzystywać tego typu narzędzi w działaniach na rzecz sfery gospodarczej, wyjaśnia to niechęć czynienia nakładów na obszary bierne i kosztowne w utrzymaniu.

W tym momencie wykreowała się kolejna funkcja polityki wobec sfery bezpieczeństwa ekonomicznego i militarnego, a mianowicie właściwe ich wykorzystanie dla potrzeb wielowymiarowego rozwoju kraju. Jeżeli ta funkcja nie jest wykorzystywana ukazuje ona jedynie bezcelowość dokonywania nakładów na coś, co nie może spełniać swoich najważniejszych funkcji. Poprzez takie podejście sfera ekonomiczna staje się weryfikatorem działań sfery nieekonomicznej i funkcjonowania państwa w różnych wymiarach.

Symptomatycznym jest, iż w sferze ekonomicznej powstają najbardziej realne oceny przebiegających zjawisk w większości wymiarów funkcjonowania państwa. Z nich wywodzi się określona wola i generowanie nacisków na inne obszary, to te elementy tworzą podzbiór wspólny, który decyduje o kształcie bezpieczeństwa ekonomicznego i strategii obronnej, a także poziomie zaspokojenia postulowanych potrzeb tak rzeczowych, jak i finansowych. Stąd można

wymagania bezpieczeństwa ekonomicznego samoistnie zostają poszerzone o elementy zapewniające bezpieczeństwo militarne państwa. Można w związku z tym przyjąć, iż obszar bezpieczeństwa ekonomicznego powinien być weryfikatorem potrzeb obronnych i możliwości ich spełnienia. Natomiast poziom zaspokojenia pożądań bezpieczeństwa ekonomicznego dla zapewnienia jego odpowiedniego poziomu bezie jednocześnie wskaźnikiem poziomu zabezpieczenia potrzeb wynikających z przyjętej strategii obronnej.

Uwarunkowania nieekonomiczne dostrzegać należy przede wszystkim na płaszczyźnie regulacji prawno-legislacyjnych i organizacyjnych z punktu widzenia procesów transformacji restrukturyzacyjnych, różnych stanów bezpieczeństwa oraz realizacji programów i zadań dostosowawczych, wynikających z procesów integracyjnych.

Kreśląc formułę przyszłościowych organizacyjnych i legislacyjno-prawnych warunków funkcjonowania gospodarczych podstaw obronności kraju, zasadnicza uwaga skoncentrowana zostanie na problemie ogólnych i szczegółowych uwarunkowań bezpieczeństwa ekonomicznego oraz na warunkach kształtowania strategii bezpieczeństwa państwa.

W analizie ogólnych warunków funkcjonowania gospodarki obronnej, przyjmuje się założenie, że pożądany model warunków organizacyjnych i prawno-legoislacyjnych może być rozumiany jako teoretyczny wzorzec idealny lub wzorzec teoretyczno-pragmatyczny zbliżony do wzorca przewidywanego ustaleniach Układu Europejskiego. Drugim kryterium, stosowanym kontekstowo, będzie dodatkowo społeczna akceptacja reform i zmian systemowych. Ponieważ w dotychczasowych badaniach dominujące znaczenie ma przede wszystkim identyfikacja teoretycznych współzależności między warunkami, a mechanizmami funkcjonowania i rozwoju zbudowanych wokół modelu równowagi ogólnej polityki bezpieczeństwa ekonomiki i obrony, to w kolejnym etapie badań przeprowadzona musi zostać próba oceny przede wszystkim tych warunków, które mają podstawowe znaczenie dla oceny stopnia zaawansowania procesów restrukturyzacyjno-rozwojowych w zakresie gospodarki obronnej państwa i strategii bezpieczeństwa oraz stabilizacji podstaw systemu obronnego gospodarki rynkowej. Ocena warunków o podstawowym znaczeniu funkcjonalnym dla bezpieczeństwa ekonomicznego

poszczególne elementy wewnętrznego systemu państw i przez to decydować o wielu rozwiązaniach w sferze politycznej, gospodarczej, czy też społecznej. Poziom odporności na oddziaływanie zewnętrzne wynika z jakości zachodzących sprzężeń pomiędzy poszczególnymi elementami całego układu i ich prędkości.

Z tych rozważań można wysnuć wniosek, że jeżeli spojrzeć na bezpieczeństwo ekonomiczne, którego kształt jest determinowane poprzez jego powiązania ze strategią obronną to następuje jego uzależnienie od celów i kierunków narzucanych przez sferę polityczną. To w tym obszarze w takim wypadku następuje starcie pomiędzy celami narzucanymi przez sferę polityczną a wolą i możliwościami do ich realizacji przez sferę gospodarczą. Można przypuszczać, iż w wielu przypadkach o dominacji jednych celów na innymi będą decydowały efekty rozstrzygnięć w obszarze bezpieczeństwa ekonomicznego. W każdym z omawianych wypadków tj. przewagi obszaru politycznego lub gospodarczego wymagania bezpieczeństwa ekonomicznego z punktu widzenia jego powiązań ze strategią obronną będą się koncentrowały na wymuszeniu na sferze gospodarczej zapewnienia dopływu zasilania rzeczowego dla potrzeb wynikłych z założeń tejże strategii i pośrednio od niej zasilania finansowego. Natomiast na sferę polityczną wymuszenia zostaną skierowane na wytworzenie zrozumienia i woli dla zapewnienia przez państwo możliwie najlepszej strategii obronnej i prowadzenia, jak najbardziej efektywnych działań na rzecz szeroko rozumianego bezpieczeństwa ekonomicznego państwa Korelacja działań w obu obszarach jest konieczne, gdyż zasilanie finansowe jest generowane z dwóch obszarów jednocześnie, w pierwszej kolejności wytwarza je obszar gospodarczy, a w następnej części z nich jest alokowana przez sferę polityczną. Czyli część energii wymuszenia w tym ujęciu jest także skierowana na obie sfery, a jej wielkość jest zależna od roli pierwiastka politycznego i gospodarczego w systemie państwowym.

Ponadto bezpieczeństwo ekonomiczne w swej istocie kierunkuje swoje działania na zapewnienie bezpieczeństwa państwa. Skoro strategia obronna jest jednym z elementów bezpieczeństwa militarnego, które współtworzy cały system bezpieczeństwa państwa to bezpieczeństwo ekonomiczne jakby ze swej natury staje się jednym z jego komponentów. Stąd wynika, iż w sprawnie działającym systemie

- zarządzanie w dziedzinie obrony, zwłaszcza reorganizacja Sił Zbrojnych RP, są nadal uwarunkowane kryzysem finansów publicznych państwa i w konsekwencji ograniczaniem wydatków na obronę narodową;
- infrastruktura systemu obrony jest niedostosowana do nowego, geopolitycznego otoczenia Polski, natomiast jej dostosowanie w krótkim okresie przekracza obecne możliwości budżetowe państwa;
- upoważnienia budżetowe dla MON nie zapewniają odpowiednich do wymagań modernizacji technicznej Sił Zbrojnych, zakupów uzbrojenia i sprzętu wojskowego.

Diagnoza stanu obecnego, w porównaniu ze stanem docelowym (pożądanym), tworzy obraz różnic, który następnie wymaga analiz wariantów decyzji rozwojowych, zbudowania systemu istotnych celów rozwoju, dokonanie restrukturyzacji gospodarki narodowej w ten sposób, aby możliwe stało się zbudowanie w oparciu o polski potencjał naukowy systemu obronnego suwerennego państwa polskiego. Należy w tym miejscu podkreślić, że:

- przy obecnym stanie gospodarki obronnie zorientowanej przyspieszenie modernizacji bez dodatkowych nakładów publicznych jest niewykonalne;
- strategia wzrostu nakładów publicznych na techniczne wyposażenie armii może być zrealizowana w obecnych warunkach jedynie kosztem zmniejszenia stanów osobowych i majątkowych Sił Zbrojnych RP.

Analiza funkcjonalna warunków funkcjonowania jest niepełna - zwłaszcza w okresie transformacji - bez analizy pionowej. Wskazane wnioski z analizy systemowo-programowej (poziomej) wymagają, zatem uzupełnienia wnioskami z oceny pionowej warunków funkcjonowania i rozwoju gospodarki obronnej.

Analiza pionowa obejmuje proces wpływu warunków obronnych na decyzje polityczne, zwłaszcza na strategię bezpieczeństwa i strategię obronności państwa. Centralnym przedmiotem oceny jest w ramach tej analizy państwowy mechanizm bezpieczeństwa państwa. Nisko stopień zintegrowania systemu politycznego opóźnia procesy dostosowawcze i zwiększa społeczne koszty reform gospodarki obronnej.

Stopień zintegrowania systemu politycznego wokół problemów bezpieczeństwa państwa w naszym kraju charakteryzują przede wszystkim spory

wymaga przede wszystkim analizy poziomej ogólnego nieekonomicznego bezpieczeństwa państwa - w tym zwłaszcza wstępnego opracowania wynikowych ocen generalnych całego systemu obronnego, dla którego gospodarka obronnie zorientowana stanowi podsystem (obejmujący także logistykę).

Przed analizą gospodarki obronnej z punktu widzenia efektywności gospodarowania i gotowości obronnej można wykorzystać dostępne, oficjalne oceny obecnego stanu (potencjału obronnego i jego gotowości zarówno ilościowe, jak jakościowe) oraz zarysować stan obecny w ujęciu rzeczowym i procesowym. Istotą tych ocen jest uzależnienie przebudowy systemu obronnego naszego kraju od finansowania modernizacji technicznej Sił Zbrojnych RP.

Z analizy całego systemu społeczno-gospodarczego wynika, że kryzys finansów publicznych jest groźniejszy niż kryzys w obszarze gospodarki obronnej.

W analizach procesowych - mimo nakładania się problemów interpretacyjnych - można jednak ocenić zarówno skuteczność kierowania, jak i zarządzania w dziedzinie gospodarki obronnej. Skuteczność ogólna, jak już wcześniej podkreślano, jest niska - stan ten potwierdza także rządowe przedłożenie sejmowe.

Oceny generalne gospodarki obronnej prezentowane są zarówno nieoficjalnie, jak i oficjalnie, przy czym w zakresie oficjalnych ocen istnieje daleko idąca zgodność wniosków i ich interpretacji między głównymi uczestnikami zarządzania w dziedzinie obrony. W ocenach generalnych podkreśla się w szczególności, że obecnie potencjał obronny naszego kraju i jego składowa gospodarczo-obronna są w stanie krytycznym, gdyż:

- jakość uzbrojenia i sprzętu technicznego należącą do uzbrojenia Sił Zbrojnych RP odbiega od przeciętnych norm obowiązujących w NATO lub od tzw. standardów europejskich;
- struktura głównych rodzajów uzbrojenia i sprzętu wojskowego jest asymetryczna w stosunku do państw NATO, natomiast jej zmiana bardzo kosztowna (m.in. wymaga intensywnego rozwinięcia systemu obrony powietrznej kraju);

dwa obszary wpływające na poziom wymagań; i możliwości ich realizacji. Pierwszym jest obszar zewnętrzny wynikający z kontaktów utrzymywanych przez Polskę, drugim zaś obszarem jest obszar wewnętrzny i wynikające stąd uwarunkowania rozwoju gospodarczego.

Z punktu widzenia przeprowadzonych rozważań istotnym problemem są powiązania i wynikające z nich współzależności rozwoju gospodarczego kraju i bezpieczeństwa państwa. Jest to pochodną tego, iż współcześnie potrzeby bezpieczeństwa państwa coraz silniej oddziaływają na płynność procesów rozwojowych. Dlatego też formułując wymagania ze strony strategii obronnej wobec bezpieczeństwa ekonomicznego kraju i uwarunkowań jego kształtowania należy zwrócić uwagę na przesłanki, które określają potrzeby obronne kraju i wynikające z nich potrzeby i możliwości rozwoju gospodarczego. Powinny być one rozpatrywane z punktu widzenia potrzeb obronnych i zdolności ich zaspokojenia w różnych stanach zagrożenia państwa.

Pierwszym założeniem przy konstruowaniu modelu jest to, że gospodarka narodowa jako podstawowy składnik siły obronnej państwa, gdyż to ona dostarcza poszczególnym jego elementom różnego rodzaju źródła i świadczy na jego rzecz usługi. Przy takim ujęciu należy traktować składowe gospodarki narodowej pod względem stopnia przydatności dla zaspokojenia potrzeb obronnych. Na tej podstawie zostały wydzielone w gospodarce narodowej trzy obszary:

1. Obszar A jest niedostępny dla zaspokojenia potrzeb związanych z bezpieczeństwem, a w szczególności potrzeb Systemu Obrony Państwa (SOP), można powiedzieć, że głównym celem jego istnienia jest zaspokajanie potrzeb rozwojowych gospodarki;
2. Obszar B jest obszarem podwójnego zastosowania, stopień wykorzystania go na rzecz potrzeb rozwojowych gospodarki, bądź też potrzeb obronnych zależy od uwarunkowań wewnętrznych i zewnętrznych, które decydują o stopniu zagrożenia bezpieczeństwa państwa;
3. Obszar C z punktu widzenia potrzeb rozwojowych gospodarki jest niedostępny i stanowi źródło obciążenia dla gospodarki narodowej, można to obciążenie nazwać kosztem alternatywnym bezpieczeństwa

wokół podziału kompetencji organów państwa. Utrzymywanie rozbieżności kompetencyjnych nie tylko nie sprzyja procesowi restrukturyzacyjno-rozwojowym w gospodarce obronnej, ale także utrudnia bieżącą koordynację procesów przygotowawczych do mobilizacji gospodarczej, cywilnej i wojskowo-militamej dla okresów zagrożenia wojennego i wojny.

Niski stopień zintegrowania kierowania i koordynacji w dziedzinie obronnej powoduje ponadto nieskuteczność przetwarzania diagnostycznych ocen strategicznych na decyzje strategiczne. Przykładowo, jeżeli stan obecny potencjału obronnego i jego gotowości jest ogólnie oceniany krytycznie, to nie jest to równoznaczne z uznaniem przez system faktyczny konieczności zintegrowanego przeciwdziałania dla poprawy tego stanu. Strategia bezpieczeństwa jest, zatem obecnie bezsilna wobec finansów publicznych, które nie tylko preferują strategię gospodarczą, ale uniemożliwiają realizację strategii bezpieczeństwa, natomiast gospodarka obronna nie jest sama zdolna do opanowania własnego programu restrukturyzacji i rozwoju.

Proces przemian gospodarczo-politycznych, jakie się dokonały w ostatnich latach w Polsce w znacznym stopniu ograniczyły naszą niezależność gospodarczo-polityczną, a w konsekwencji osłabienie bezpieczeństwa ekonomicznego kraju. Wpływ na ten stan rzeczy miały z jednej strony słabość systemu gospodarczego Polski, z drugiej zaś podjęte kierunki przemian. Przy tym wszystkim Polska została włączona do nurtu globalizacji gospodarczej, jaki zaistniał we współczesnym świecie u schyłku XX wieku. Oznacza to, iż w polskim systemie pierwiastek ekonomiczny zdobył rolę dominującą. Bezpieczeństwu ekonomicznemu coraz częściej przypisuje się rolę kontrolera działalności sfery politycznej i militarnej. Zapewnienie bezpieczeństwa ekonomicznego przekłada się na szeroko rozumiane bezpieczeństwo państwa, a także na pewne zagrożenia dla niego. Taka sytuacja stawia nowe wyzwania przed systemem gospodarczo-politycznym, który musi dostosować zasady postępowania do nowych wyzwań. Stąd też wypływają wymagania, jakie stawia strategia obronna bezpieczeństwu ekonomicznemu, poczynając od problematyki zasilania rzeczowego, a skończywszy na postulowaniu i wymuszaniu na sferze gospodarczej postawy pro obronnej. Natomiast sprowadzając wywody bliżej realiów gospodarczo-społecznym można wyodrębnić

4. ***Wydzielenia w obszarze gospodarki wojennej sił i środków*** niezbędnych dla przetrwania społeczeństwa oraz funkcjonowania wybranych elementów państwa.

Strategia obronna wysuwa sformalizowane postulaty monitorowania stanu gospodarki obronnej w odniesieniu do zgłaszanych wobec niej potrzeb, aby ta drogą ujawniać istniejące dysproporcje. Dokonując takiego porównania na podstawie dostępnych danych można wysnuć następujące wnioski:

- poziom nakładów na sferę obronną uniemożliwia powstrzymanie procesów degradacji w wymiarze rzeczowym i infrastrukturalnym, co ponadto uniemożliwia rozpoczęcie efektywnych procesów modernizacyjnych w tym obszarze;
- istnienie niedopasowania pomiędzy strukturą i zdolnościami wytwórczymi gospodarki obronnej a popytem i przyszłymi potrzebami systemu obronnego;
- niedoboru zdolności produkcyjnych do sprostania zwiększonym potrzebom okresów zagrożenia i wojny;
- zapóźnienia i wadliwe działanie infrastruktury gospodarczo-obronnej kraju;
- niski poziom na prace badawczo rozwojowe na rzecz gospodarki obronnej.

Jeżeli zostaną połączone dwa elementy a mianowicie obszar gospodarki przydatnej dla obronności i jej kondycję, to wówczas wyłonią się różnice, jakie występują pomiędzy potrzebami obronnymi wynikającymi z przyjętej strategii obronnej a możliwościami ich zaspokojenia. Wydaje się, iż właśnie ten element determinuje wymogi, jakie stawia strategia obronna bezpieczeństwu ekonomicznemu.

Wymogi stawiane bezpieczeństwu ekonomicznemu przez strategię obronną posiadają różnorodny charakter i zakres, lecz można je ująć w następujących kategoriach: zabezpieczającej, sygnalizującej, koordynującej oraz wymuszającej. Jeżeli zostaje uwidoczniony niedowład ze strony gospodarki obronnej, która nie jest w stanie zapewnić odpowiednich dostaw rzeczowych na rzecz systemu obronnego, które to są wypadkową narzuconych zadań ze strony obowiązującej strategii.

wobec innych potrzeb, rozmiar tego obszaru obrazuje skalę obciążenia gospodarki narodowej świadczeniami na rzecz bezpieczeństwa, mogą to być następujące elementy:

- przemysł zbrojeniowy;
- infrastruktura obronna;
- zwiększenie poziomu rezerw o wielkości większe niż wymaga tego zabezpieczenie funkcjonowania systemu gospodarczego;
- koszty utrzymania sił zbrojnych;
- koszty utrzymania innych elementów SOP.

Obszary B i C łącznie tworzą gospodarcze podstawy bezpieczeństwa (GPB) państwa[234]. Taki układ umożliwia sformułowanie następujących ***postulatów rozwojowych*** dla gospodarki narodowej:

1. ***Szybki wzrost gospodarczy***, którego efektem byłoby powiększenie rozmiarów gospodarki. Dzięki temu procesowi będą mogły maleć relatywnie obciążenia gospodarki narodowej świadczeniami na rzecz bezpieczeństwa państwa, a szczególnie na rzecz SOP, przy jednoczesnym utrzymywaniu na podobnym poziomie lub nawet powiększając te na kłady.
2. ***Mobilność***, która odnosi się do obszaru podwójnego zastosowania. Chodzi o zapewnienie zdolności do płynnej metamorfozy części zasobów i strumieni zasilania w sytuacjach narastania potrzeb ze strony SOP. Przy jednoczesnym zastrzeżeniu, iż powinien to być proces płynny, który byłby realizowany w wymaganym czasie i o pożądanej wielkości. Postulat mobilności odnosi się do procesu mobilizacji gospodarki.
3. ***Zgodności struktury gospodarki z cywilnymi i militarnymi celami gospodarowania.*** Wdrożenie go do pragmatyki gospodarczej dla zdolności do zmiennego zaspokajania potrzeb gospodarki obronnej, potrzeb rozwojowych oraz potrzeb konsumpcyjnych.

---

[234]Por. S. Kurek, *Bezpieczeństwo ekonomiczne państwa, w: Ekonomika bezpieczeństwa państwa średniej wielkości. Teoria i praktyka,* pod red. M. Krća, S. Kurini, Warszawa-Brno 2000, s. 47.

Zauważalną problematyką w omawianym obszarze są postulaty kierowane poprzez bezpieczeństwo ekonomiczne w stosunku do poziomu i kierunków rozwoju gospodarki, od czego to w istocie rzeczy zależy stan gospodarki obronnej, a w rezultacie możliwości konstruowania i realizowania strategii obronnej zgodnej z wymogami interesu narodowego. Patrząc perspektywicznie na ten problem wyłaniają się wymagania odnoszące się do utrzymania odpowiedniego do zagrożeń tępa postępu naukowo-technicznego, a zwłaszcza w tym obszarze, który decyduje o poziomie nowoczesności wyposażenia armii. W tym aspekcie decydują wymogi współczesnych konfliktów zbrojnych. Jednocześnie należałoby zauważać elementy determinujące pokojowy rozwój gospodarki obronnej:

- obowiązujące porozumienia rozbrojeniowe, czy też odnoszące się do stanów liczbowych sprzętu wojskowego układy międzynarodowe dwu i wielostronne;
- zobowiązania wynikające z przynależności do sojuszów wojskowych i politycznych.

Z tych przesłanek można wnioskować, jakie będą prawdopodobne progi graniczne dla zaangażowania się gospodarki w tworzenie podstaw obronności państwa. W rzeczywistości jest to bardzo trudne zadanie, gdyż dzisiaj można jedynie przewidywać, jaki będzie miał charakter przyszły konflikt. Dlatego można stwierdzić, iż najkorzystniejszym jest stworzenie odpowiednio wysokiego potencjału obronnego, który odpowiadałby potencjałom obronnym państw będących zagrożeniem dla stabilizacji. Wynika to z faktu, iż jest on najbardziej mobilny z punktu widzenia konfliktu, czyli tworzenia strategii obronnej. Jego rozmiary powinny zależeć od obecnego oraz od przewidywanego zagrożenia. Gospodarka narodowa w związku z małym prawdopodobieństwem wystąpienia konfliktu zbrojnego powinna być ewolucyjnie przystosowana do zaspokajania potrzeb obronnych podczas poziomów zagrożenia:

- w okresie pokoju: zadaniem gospodarki narodowej jest dostarczanie niezbędnych środków, których wymaga obronność zgodnie z doktryną obronną oraz przygotowania podstaw do zaangażowania innych segmentów gospodarki w przypadku wystąpienia wyższych poziomów zagrożenia;

Ograniczenia te wynikają z istniejących uwarunkowań wewnętrznych i zewnętrznych to wówczas znaczną część ciężaru w sytuacjach zagrożeń, w których będzie konieczność stosowania elementu militarnego, zostanie przerzucona na sferę odpowiedzialną za kształt i poziom ogólnego bezpieczeństwa państwa. Inaczej mówiąc im gorszy stan tej części gospodarki mogącej wytwarzać na rzecz sfery obronnej tym bardziej rosną wymagania wobec bezpieczeństwa ekonomicznego, które ze swej natury i zgodnie z oczekiwaniami zabezpiecza funkcjonowanie państwa zarówno w wymiarze gospodarczym, jak i obronnym. Strategia obronna oczekuje od bezpieczeństwa ekonomicznego zapewnienia potencjału, który byłby w stanie zabezpieczać różnego rodzaju procesy przebiegające w różnych stanach zagrożenia militarnego państwa. Im większe prawdopodobieństwo wystąpienia określonego zagrożenia i jednocześnie niska kondycja gospodarki obronnej wówczas rosną oczekiwania wobec sfery bezpieczeństwa ekonomicznego, jako elementu zabezpieczającego. Jednocześnie należy zaznaczyć, iż poziom bezpieczeństwa ekonomicznego jest funkcją kondycji państwa, odbiciem stanu gospodarki, struktur społecznych, systemu politycznego. Powoduje to, iż pierwsze symptomy narastania sytuacji kryzysowych rodzących się w państwie można odnaleźć właśnie w obszarze bezpieczeństwa ekonomicznego, stąd rodzi się kolejny wymóg wobec niego. Chodzi o sprawowanie swoistego rodzaju sygnalizatora powstawania, czy też narastania sytuacji kryzysowych w państwie - różnych jego wymiarach. Ponadto w tym obszarze skupiającym działania z różnych dziedzin życia gospodarczo-politycznego następuje koordynowanie działań, określanie priorytetów i ważenie pomiędzy nakładami na bezpieczeństwo w wymiarze gospodarczym i obronnym. Jest to znacząca rola, gdyż to od niej zależy efektywność wykorzystana dostępnych środków, ich koncentracja i alokacja.

Kolejnym wymogiem jest możliwość ukierunkowania działań - możliwe, że pod wpływem presji - w określonych obszarach bytu państwowego na rzecz danego wymiaru bezpieczeństwa. Nie jest to czynione w sensie przymusu fizycznego, ale zasadzie przymusu psychicznego. Sygnalizując nieustannie kierunek, poziom, czy narastanie zagrożenia, co przyczynia się do „stworzenia" potrzeby przeciwdziałania temu zjawisku zgodnie z odwieczną potrzebą posiadania bezpieczeństwa.

warunkach gospodarczych i politycznych to można stwierdzić jednocześnie zauważamy, że są one istotnymi elementami tworzenia bezpieczeństwa państwa. Przez to ważnym jest odpowiednie stymulowanie rozwoju tych działów gospodarki narodowej przez państwo. Rozwój tych obszarów, podobnie jak innych, jest zależny od poziomu inwestycji. Z kolei poziom inwestycji wynika z ilości środków możliwych do przeznaczenia na ten cel. Mogą to być środki pochodzące z procesów akumulacji dokonywanych przez same podmioty gospodarcze, jak i ze źródeł zewnętrznych -pożyczek komercyjnych, państwowych, subsydiów itd. Poziom akumulacji środków własnych przedsiębiorstw, a także dostępność do środków zewnętrznych zależy od prowadzonej przez państwo polityki gospodarczej, a szczególnie polityki podatkowej, polityki społecznej (np. system emerytalno - rentowy i ubezpieczeniowy), polityki monetarnej itd.. Ponadto poziom inwestycji w wysokości pożądanej z punktu widzenia bezpieczeństwa państwa zależy w znacznym stopniu od angażowania państwa się w proces inwestycyjny. Państwo angażuje się: poprzez pomoc bezpośrednią i pośrednią dla przedsiębiorstw, a także bezpośrednio w inwestycje niezbędne z punktu widzenia rozwoju gospodarczego oraz bezpieczeństwa a będące jednocześnie inwestycjami mającymi znaczenie dla procesów reinwestycyjnych w innych dziedzinach np. energetyka, telekomunikacja, czy też będące inwestycjami kapitałochłonnymi, czy też o długiej stopie zwrotu np. hutnictwo, górnictwo, zakłady chemiczne itd., a także inwestycjami mogącymi posiadać wymiar społeczny i obronny np. metro.

Bardzo ważną kwestią jest dopuszczenie do obszaru inwestycji ważnych pod względem gospodarczym i obronnym kapitału zagranicznego. Rodzi się jednak w tym momencie problem sposobu wprowadzenia kontroli tegoż kapitału w obszarze tychże dziedzin gospodarki. Ponadto zakres i głębokość inwestycji zagranicznych w tych obszarach powinien być wynikiem planowanych działań państwa, które stwarza korzystne warunki dla zaistnienia kapitału zagranicznego w określonych branżach. Celem tych działań jest uzyskanie przez ważne dla bezpieczeństwa państwa i gospodarki narodowe działy, gałęzie i branże tempa wzrostu wyprzedzające wskaźniki rozwojowe całej gospodarki. Jeżeli nie to występowało w całym okresie objętym planowanie, to powinno wystąpić w pewnym przedziale czasowym, umożliwiające zaistnienie trwałego bodźca

- w okresie narastania zagrożeń, a w szczególności zagrożeń o charakterze militarnym, najważniejszym zadaniem staje się zmiana celu gospodarowania, struktury wytwarzania oraz uruchamianie, zgodnie z zaistniałymi potrzebami, rezerw i zapasów nagromadzonych w okresach poprzednich;
- w okresie wojny priorytetowym zadaniem staje się dostarczanie w pożądanej wysokości jakości dóbr i usług na rzecz systemu obronnego np. dla wojsk walczących z przeciwnikiem i jego szeroko rozumianego zaplecza.

Ogólnie można sprowadzić wymagania sfery obronnej wobec gospodarki narodowej do dwóch ujęć:

- zasobowego tj. zdolności do wytworzenia określonych dóbr i świadczenia pożądanych usług zgodnie z potrzebami wynikającymi z utrzymaniem danego poziomu bezpieczeństwa;
- funkcjonalnego tj. zdolności do przekształcania wyżej wymienionych dóbr i usług w strumienie produkcji oraz dostawy dokonywane w pożądanym czasie.

W związku z istnieniem konfliktu wynikającego ze szczupłości dostępnych środków, które można przeznaczyć na realizację potrzeb rozwojowych gospodarki narodowej i gospodarki obronnej, należy określić priorytety rozwojowe. Priorytety te powinny stanowić równocześnie nośniki rozwojowe dla gospodarki narodowej i obronnej. Rozpatrując ten problem z punktu widzenia realiów naszego kraju takimi nośnikami mogą być:

- zasoby siły roboczej i związane z tym jej kondycja zdrowotna, wielkość przyrostu, poziom kwalifikacji, mobilność;
- wyselekcjonowanie gałęzie przemysłu np.: maszynowy, elektroniczny, elektrotechniczny, chemiczny, petrochemiczny, energetyczny, spożywczy czy budownictwo;
- rolnictwo wraz związaną z nim infrastrukturą gospodarczą;
- infrastruktura transportowa i telekomunikacyjna kraju.

Jeżeli wybrane nośniki ze wskazanych elementów systemu gospodarczego będą stanowiły siłę napędową rozwoju gospodarki narodowej naszego państwa

kryzysowych może nie zapewnić zaspokojenia potrzeb obronnych, gospodarczych i społecznych choćby na minimalnym poziomie.

Jednym z ważniejszych zadań gospodarki obronnej jest zapewnienie dostaw żywności w wypadku wystąpienia zagrożenia wojennego i wojny na potrzeby działań bojowych oraz jego zaplecza, lub prób izolacji kraju. Stąd rodzące się potrzeby rozbudowy przemysłu spożywczego, a szczególnie w zakresie magazynowania i przechowywania[235].

Szacując potrzeby rozwojowe tych gałęzi zarówno z punktu rozwiązań systemowych oraz potrzebnych do ich zrealizowania nakładów finansowych wydaje się, iż jest to zadania długofalowe, wymagających koordynacji sfery gospodarczej i politycznej. Koniecznym jest osiągnięcie stanu bliskiego równowadze pomiędzy możliwościami wymienionych gałęzi przemysłu a potrzebami rozwojowymi gospodarki narodowej i obronnej. Stan taki pozwoli na zaspokajanie potrzeb obronnych kraju, a tym samym realizowanie założeń wynikających ze strategii obronnej. W sposób naturalny zostałby ukazany kształt modelu działania i współdziałania gospodarki i obronności. Funkcjonowanie prezentowanego modelu kształtowania bezpieczeństwa ekonomicznego z punktu widzenia strategii obronnej odbywa się na zasadzie sprzężeń zwrotnych, jakie zachodziłyby pomiędzy poszczególnymi jego elementami w czasie i przestrzeni. Sprzężenia te mogą zachodzić równocześnie, jak i w różnym czasie -w tych samych obszarach, jak i w różnych obszarach. Pierwotnym źródłem generującym sprzężenia pomiędzy elementami modelu są sygnały wysyłane przez poszczególne jego obszary. Pod takimi sygnałami kryją się pożądane kierunki rozwoju, określone wstępnie potrzeby wynikłe z przewidywania, czy też prognozowania przyszłości, a także potrzeby narzucone przez różnego rodzaju przyjęte zobowiązania wobec otoczenia.

Bezpieczeństwo ekonomiczne będzie w takim modelu postrzegane trójwymiarowo:

- jako stan: będzie się wówczas rozumiane jako element określający poziom rozwoju gospodarki narodowej i efektów prowadzonej polityki przez państwo;

---

[235] Por. M. Jabłonowski, *Wobec zagrożenia...*, Wyd. cyt., s. 75÷97.

rozwojowego w całej gospodarce. Oznacza to, iż powinien to być początkowy okres poprzedzający rozwój całej gospodarki.

W uwarunkowaniach naszego kraju, zgodnie z przyjętymi programami rozwoju społeczeństwa informacyjnego, celowym a wręcz koniecznym jest podniesienie nakładów na inwestycję w telekomunikacji i informatyce aby utrzymać tempo rozwoju łączności na obecnym poziomie. Spadek inwestycji w tym obszarze może spowodować, że dotychczasowe rodzaje świadczonych usług multimedialnych, zwiększą jeszcze istniejącą już różnicę w poziomie ich rozwoju pomiędzy Polską a czołówką światową.

Infrastruktura gospodarcza wymaga konsekwentnej, długofalowej polityki inwestycyjnej, która zapewniałaby rozbudowę istniejącej sieci gazociągów, budowę rozprężalni gazu w portach i stopniowe zwiększanie ich mocy przerobowych oraz budowy zbiorników gazu ziemnego zapewniających rezerwy w wysokości dziewięćdziesięciu dni zapotrzebowania ze strony gospodarki narodowej i całego społeczeństwa. Przystąpienia do modernizacji istniejącej sieci drogowej oraz budowy dróg szybkiego ruchu i autostrad, a także dokonywania modernizacji sieci kolejowej. Łożenia odpowiednich środków na modernizację sieci elektroenergetycznej kraju, ale nie tylko poprzez ich prywatyzację.

Z punktu widzenia gospodarki narodowej oraz gospodarki obronnej wymagane jest wspomaganie rozwoju gałęzi przemysłu decydujących o ich poziomie. Odnosi się to w szczególności do przemysłu budowlanego, elektronicznego, elektromaszynowego, precyzyjnego, optycznego i chemicznego. Ich poziom rozwoju decyduje o poziomie rozwoju technicznego i dynamice wzrostu gospodarczego kraju. Zakres samowystarczalności w wytwarzaniu półproduktów i produktów decydujących o poziomie nowoczesności innych gałęzi przemysłu, a tym samym poziomie nowoczesności składowych systemu obronnego. Ponadto nakładów wymaga przemysł petrochemiczny, gdyż we współczesnych warunkach prowadzenia działań zbrojnych jest narażony na duże zniszczenia. Stąd wynika potrzeba zwiększenia jego mocy przerobowych oraz rozbudowa systemu rezerw paliw zgodnie ze standardami UE. Przy obecnym poziomie posiadanych rezerw, możliwości przerobowych i niskiej odporności na zniszczenia, w sytuacjach

kosztem tempa wzrostu gospodarczego, poziomu bezpieczeństwa, znaczenia na arenie międzynarodowej w ujęciu gospodarczym i politycznym.

Postulowany model kształtowania bezpieczeństwa ekonomicznego w świetle wymagań strategii obronnej okazał się w wyniku przeprowadzonych rozważań w istocie rzeczy istniejącymi i faktycznie funkcjonującymi powiązaniami, sprzężeniami i zależnościami. Uzmysłowienie tego pozwala na wykorzystanie naturalnie istniejącego układu dla potrzeb szeroko rozumianego bezpieczeństwa państwa. Wydaje się, iż dodatkowo pokazuje potrzebę odkrywania i wykorzystywania istniejących i towarzyszących nam zjawisk.

Strategia bezpieczeństwa Polski, jeśli formułować wobec niej postulaty ze strony polityki gospodarczo-obronnej postrzegane z punktu widzenia wymogów funkcjonowania gospodarki obronnej państwa zdeterminowane są szeregiem czynników, które można zgrupować w trzech zbiorach a mianowicie:

- nieekonomicznych;
- ekonomicznych;
- polityki bezpieczeństwa.

Każda z nich zarówno ze względu na jego kształtowanie, jak i na powstawanie zagrożeń dla tego stanu ujawnia wymiar zewnętrzny i wewnętrzny. W wymiarze zewnętrznym dostrzegać trzeba jej poprzez globalne tendencje rozwojowe współczesnego świata i skutki z nich wynikające. W wymiarze zaś wewnętrznym - poprzez kryteria ogólnego poziomu cywilizacyjnego odniesionego do warstwy naukowo-technicznej, organizacyjnej, politycznej, społecznej, militamo-obronnej, ekonomicznej itd.

Zapewnienie bezpieczeństwa Polski w przyszłości rodzi cały szereg dyrektyw wobec gospodarczych podstaw obronności kraju podlegających ścisłym wpływom budowanej w naszym kraju gospodarki rynkowej. Obok dyrektyw płynących z zależności zewnętrznych kontaktów naszego kraju, istotną grupę stanowią te, które wiążą się z dyrektywami wynikającymi z wewnętrznego rozwoju kraju[236]. Tę ostatnią grupę sprowadzić można do trzech warstw:

---

[236]Por. *Polska 2025. Długookresowa strategia trwałego zrównoważonego rozwoju*, RzCSS-RM, Warszawa 2000.

- jako proces: będzie wówczas odwzorowywało procesy zachodzące w obszarze gospodarczym i politycznym w państwie;
- jako narzędzie (z punktu widzenia obronności): będzie postrzegane jako narzędzie realizacji założeń wynikających ze strategii obronnej.

Strategia obronna będzie w tym modelu postrzegana jako narzędzie realizacji założeń politycznych kształtowania bezpieczeństwa państwa i jako element procesu kształtowania tychże założeń.

Polityka występuje jako jeden z dwóch elementów pierwotnych tegoż modelu, który decyduje o niematerialnych składowych wejściowych bezpieczeństwa ekonomicznego i strategii obronnej, a także posiadająca duży wpływ na składowe materialne tychże elementów.

Gospodarka jest drugim elementem pierwotnym tegoż modelu, który decyduje o ilości i jakości materialnych składowych bezpieczeństwa ekonomicznego i strategii obronnej, a ponadto jest do pewnego stopnia weryfikatorem założeń tworzonych w obszarze polityki.

Ponadto elementami determinującymi postulowany model kształtowania bezpieczeństwa ekonomicznego zgodnie z wymaganiami stawianymi przez strategię obronną jest układ zewnętrzny i wewnętrzny. Pomiędzy którymi i poszczególnymi elementami oraz obszarami modelu zachodzą sprzężenia zwrotne i wymiana sygnałów. Posiada to duże znaczenie dla samego kształtu modelu, jak i obu układów. Im większą siłę może wygenerować model tym większy wpływ na formowanie się układów.

W modelu celowo pomija się problem przeważania określonego obszaru pierwotnego, gdyż będzie się to ujawniało w składowych wejściowych bezpieczeństwa ekonomicznego i strategii obronnej. Uzmysłowienie sobie istnienia pokazanych w modelu powiązań, ich głębokości, siły i wynikających stąd współzależności egzystencjalnych decyduje o podstawach a w efekcie o poziomie bezpieczeństwa państwa w ujęciu wielowymiarowym. Nie dostrzeganie tej problematyki może prowadzić do zachwiania równowagi, jakie te elementy i obszary starają się wypracować tj. uważają za naturalne. Rezultatem tego może być sztuczne osłabienia powiązań pomiędzy nimi oraz zerwania pomiędzy realiami gospodarczymi a potrzebami innych obszarów. Będzie to mogło odbywać się

tworząc różne obszary. Stąd też z punktu widzenia potrzeb rozwojowych, zaspokojenie potrzeb związanych z bezpieczeństwem jest dla gospodarki obciążeniem alternatywnym bezpieczeństwa w stosunku do innych potrzeb.

Rozmiary tego obszaru „C" obejmują skalę obciążenia gospodarki narodowej świadczeniami na rzecz bezpieczeństwa. Specyficzne elementy służące bezpieczeństwu to przykładowo:

- przemysł zbrojeniowy i infrastruktura obronna;
- zapasy i rezerwy w rozmiarach większych niż wymagają tego procesy techniczno-produkcyjne;
- utrzymywanie sił zbrojnych, pozamilitarnych elementów SOP itd.

Na tej podstawie można sformułować listę ***postulatów rozwojowych***[237]:

1. ***Postulat szybkiego rozwoju ekonomicznego.*** Wzrost gospodarczy powiększa ogólne rozmiary gospodarki, w tym także jej części tworzącej gospodarcze podstawy bezpieczeństwa. Dzięki temu może maleć relatywne obciążenie gospodarki świadczeniami na rzecz bezpieczeństwa (bez szkody dla SOP), a także rosną możliwości zaspokajania potrzeb obronnych w sytuacji kryzysowej.
2. ***Postulat mobilności.*** Odnosi się on do obszaru „podwójnego zastosowania". Ogólnie rzecz biorąc, chodzi o zapewnienie zdolności do zmiany celu zastosowania (przeznaczenia) części zasobów i strumieni produktów w warunkach narastania potrzeb SOP w pożądanym czasie i wielkości (proces mobilizacji).
3. ***Postulat zgodności struktury gospodarki z cywilnymi i militarnymi celami gospodarowania.*** Wypełnieniem tego wymogu będzie zdolność do zamiennego zaspokojenia potrzeb gospodarki obronnej albo konsumpcyjnych i rozwojowych potrzeb gospodarki.
4. ***Postulat wydzielenia w gospodarce wojennej części niezbędnej do przetrwania społeczeństwa i funkcjonowanie państwa*** (np. dzieci, chorzy, dobra kultury, administracja).

---

[237]Tamże, s.374.

- Pierwszej formułującej ogólne wymagania obronności wobec systemu kierowania gospodarczymi podstawami obronności, skoncentrowanej na: kierowaniu gospodarką obronną, dostosowaniu potrzeb obronności kraju do gospodarki narodowej, mobilizacji gospodarczej, militaryzacji gospodarki i zbrojeniach.
- Drugiej, obejmującej system gospodarki obronnej i koncentrującej uwagę na: przemyśle obronnym, rezerwach gospodarczych, infrastrukturze gospodarczo-obronnej, postępie naukowo-technicznym oraz międzynarodowej współpracy gospodarczej.
- Trzeciej, tworzącej system logistyki obronnej i koncentrującej uwagę na: zaspokojeniu materialnych potrzeb obronnych państwa oraz świadczeniach na rzecz obronności oraz zobowiązaniach sojuszniczych wynikających z pełnienia roli Państwa-Gospodarza.

Współzależności bezpieczeństwa i rozwoju gospodarczego kraju oraz związki tych problemów z obronnością kraju są powszechnie zaakceptowane. Potrzeby bezpieczeństwa coraz bardziej oddziaływają na przebieg procesów rozwojowych.

Dlatego też, konstruując model kształtowania bezpieczeństwa ekonomicznego, ze względu na wymagania strategii bezpieczeństwa, poszukiwać należy przesłanek określających potrzeby obronne państwa, a na ich podstawie pożądanych kierunków i proporcji rozwoju gospodarczego. Rozważania te dotyczyć muszą potrzeb obronnych i zdolności ich zaspokajania w różnych stanach bezpieczeństwa państwa.

Gospodarka narodowa jest źródłem siły obronnej państwa, dostarczając elementom systemu obronnego państwa potrzebne dobra i usługi. Ogólne zależności pomiędzy stanem gospodarki narodowej a możliwościami zaspokajania potrzeb związanych z bezpieczeństwem pokazują, że gospodarkę narodową rozpatrywać trzeba z jednej strony z punktu widzenia zdolności do zaspokojenia potrzeb związanych z zapewnieniem bezpieczeństwa państwa, a patrząc od strony potrzeb rozwojowych gospodarki bez uwzględniania wymogów bezpieczeństwa. Otrzymane w wyniku tego podziału obszary nie będą się ze sobą pokrywały,

- dostosowanie zdolności produkcyjnych poszczególnych zakładów do aktualnych i przewidywanych potrzeb odbiorców krajowych i zagranicznych;
- unowocześnienie rodzajów uzbrojenia poprzez pełniejsze wykorzystanie rodzimej myśli naukowo-technicznej oraz technologii zagranicznych;
- aktywizację działań proeksportowych;
- dotowanie wybranych gałęzi przemysłu obronnego, tak, aby utrzymać jego potencjał na poziomie umożliwiającym zaspokojenie zwiększonych potrzeb sił zbrojnych w przypadku wojny;
- wdrażanie do produkcji krajowych elementów kooperacyjnych uniezależniających wytwarzanie uzbrojenia i sprzętu wojskowego od dostaw importowych.

Oznacza to, że polski przemysł zbrojeniowy w perspektywie najbliższych lat będzie musiał przejść wiele zmian. Ich podjęciu i realizacji sprzyjać mają działania wspomagające ze strony państw NATO w ramach rozwoju współpracy wojskowej i gospodarczej.

Aktualny stan rezerw państwowych rodzi poważne zagrożenia dla systemu obronnego kraju, najbliższej przyszłości powinny zostać wypracowane koncepcje, a w ślad za nimi również dokonane zmiany systemu rezerw państwowych i gospodarowania nimi. W szczególności muszą zostać rozwiązane problemy dotyczące tworzenia i utrzymywania rezerw żywnościowych i paliw płynnych. Rezerwy przeznaczone na realizację potrzeb obronnych będą finansowane z budżetu państwa, zaś na potrzeby ogólnogospodarcze w systemie pozabudżetowym.

W związku ze wzrostem wymagań współczesnego pola walki rosnąć będą również wymagania wobec poziomu technicznego systemów uzbrojenia, zmuszając do wykorzystania zaawansowanych technologii. Pozyskanie ich będzie możliwe poprzez prowadzenie wspólnych badań oraz podejmowanie produkcji przez przedsiębiorstwa zainteresowane udziałem w programach zbrojeniowych.

Zakłada się, że uzyskanie wysokiej efektywności produkcji zbrojeniowej będzie możliwe dzięki wsparciu instytutów badawczych, funkcjonujących w ramach przedsiębiorstw i wyższych uczelni, którym za pośrednictwem KBN,

Z punktu widzenia bezpieczeństwa najważniejszą funkcją gospodarki narodowej jest tworzenie potencjału obronnego. Dlatego rozwój gospodarczy powinien być skorelowany z tworzeniem ekonomicznych warunków do efektywnego zaspokojenia potrzeb obronnych w zależności od intensywności zagrożeń bezpieczeństwa państwa.

Politykę bezpieczeństwa Polski przełomu XX i XXI wieku należy dostrzegać w wymiarze polityczno - militarnym, gospodarczym i cywilizacyjnym. Pierwszy z nich mimo założeń, iż nie ma obecnie zagrożeń wskazujących na możliwość zaistnienia napaści zbrojnej, musi zakładać możliwość ujawnienia się nacisków i presji o charakterze politycznym i gospodarczym - równie niebezpiecznych dla suwerenności i niepodległości naszego kraju. Drugi zaś gospodarczy kryje w sobie przede wszystkim imperatyw integracji kontynentalnej i regionalnej. Ściśle z nimi wiąże się wymiar cywilizacyjny sprowadzający się do swobodnego przepływu myśli, idei i informacji jako podstawy upowszechniania współczesnej myśli naukowej, kultury technicznej, nowoczesnego zarządzania i innych nośników postępu cywilizacyjnego.

Ważną stroną związków między polityką gospodarczo-obronną a strategią bezpieczeństwa państwa jest problem gospodarczych podstaw obronności kraju. Problemy kształtowania gospodarczych podstaw obronności kraju należą do tych, na których będzie skupiona w przyszłości zasadnicza uwaga polityki gospodarczo-obronnej państwa. Oznacza to w istocie rzeczy kontynuowanie dotychczasowego podejścia, chociaż bardziej uwzględniającego zmienność uwarunkowań rozwojowych kraju. Podobnie jak dotychczas, do spraw najważniejszych, wymagających koncentracji sił i środków, należeć będą: wzmacnianie kondycji przemysłu zbrojeniowego, zwiększenie rezerw państwowych, postęp naukowo-techniczny oraz zaspakajanie materialnych podstaw obronności.

Ważnym kierunkiem polityki gospodarczo-obronnej państwa jest wzmacnianie kondycji rodzimego przemysłu obronnego. Podniesienie konkurencyjności i innowacyjności produkcji specjalnej wymaga jednak jego gruntownej restrukturyzacji i oddłużenia. Koniecznym w związku z tym jest:

- przekształcenie państwowych przedsiębiorstw przemysłu obronnego w jednoosobowe spółki Skarbu Państwa;

Polityka gospodarczo-obronna mając wymiar polityki bezpieczeństwa państwa realizowana jest w trzech obszarach: politycznym, militarnym i gospodarczym. Dwa pierwsze decydują bezpośrednio o zdolności obronnej państwa natomiast trzeci tworzy materialne podstawy obronności.

Podstawą kształtowania rozwiązań w tych płaszczyznach i ich realizacji musi być obowiązująca strategia bezpieczeństwa państwa. Wypracowana w oparciu o aktualną sytuację społeczno-polityczną, stan gospodarki oraz wielkość potencjału obronnego kraju, a także wewnętrzne i zewnętrzne ich uwarunkowania. Oznacza to, iż polem zainteresowania polityki gospodarczo-obronnej państwa jest obszar gospodarki narodowej pełniący funkcję na rzecz bezpieczeństwa państwa.

Podstawowym zadaniem tej polityki jest kształtowanie gospodarczych podstaw obronności kraju, które realizują ogniwa gospodarczo-obronne funkcjonujące w ramach układu pozamilitarnego systemu obronnego państwa.

Rozpatrując problematykę bezpieczeństwa państwa należy stwierdzić, że jest ono kategorią wielowymiarową i dlatego nie może być realizowane tylko na jednej płaszczyźnie. Z tego powodu współcześnie obszar pojęcia bezpieczeństwa państwa rozszerzony jest poza tradycyjną sferę polityczno - militarną. Szerszy jest, bowiem zakres wartości podlegających ochronie. Najważniejsze z nich mieszczą się w sferach:

- politycznej;
- militarnej;
- ekonomicznej.

Są to najczęściej wymieniane sfery bezpieczeństwa państwa. Stąd można przyjąć, że polityka gospodarczo-obronna i strategia bezpieczeństwa państwa realizowana jest na tych samych płaszczyznach.

Podmiot, którym jest społeczeństwo zorganizowane w państwo, chroni zestaw wartości[238] wyrażonych racja stanu, interesami - przypisanych różnym sferom bytu narodowo-państwowego. Istnienie warunków ich realizacji oznacza, że państwo nie jest zagrożone, czyli jest bezpieczne.

---

[238]Wartości do których odwołuje się definiowanie bezpieczeństwa, wyprowadzone są z potrzeb ludzi, społeczeństw. Znajdują one swój wyraz w dążeniach a te z kolei są formułowane w postaci naczelnych wartości interesów.

państwo zlecać będzie dodatkowe opracowania ważnych dla obronności projektów zbrojeniowych, w oparciu o efekty przetargowe.

Budowa przyszłościowego, a podjętego obecnie, systemu obrony państwa wymaga zaspokojenia jego potrzeb we wszystkich jego elementach funkcjonalnych. W układzie militarnym proces ten zostanie skoncentrowany na zachowaniu gotowości bojowej i sprawności armii, co wymagać będzie ciągłego zasilania w nowoczesne uzbrojenie i sprzęt wojskowy, odtwarzania zapasów materiałowych, przeprowadzenia modernizacji sprzętu i uzbrojenia, intensyfikacji prac naukowo-badawczych oraz dokonania zmian w dyslokacji wojsk. Identycznymi być muszą zamierzenia dotyczące układu pozamilitamego i systemu kierowania obronnością. Całość tych przedsięwzięć ściśle uwarunkowana będzie rzeczywistym poziomem nakładów na armię.

Zaspokojenie potrzeb SZ RP w najbliższych latach musi zostać podporządkowana technicznej modernizacji armii, w celu dostosowania wyposażenia uzbrojenia i sprzętu wojskowego do możliwości prowadzenia obrony w wymiarze lądowo-powietrznym na dowolnym kierunku operacyjnym.

Dalszego doskonalenia wymaga także system kierowania gospodarką obronną. Skoncentrowane musi zostać ono w pierwszej kolejności na przedsięwzięciach legislacyjnych i organizacyjnych.

Wyznaczając postulaty polityki gospodarczo-obronnej wobec strategii bezpieczeństwa na najbliższe lata nieodzownym przedsięwzięciem staje się wypracowanie i przyjęcie „ustawy o powszechnym obowiązku obrony kraju". Obecnie obowiązująca nie przystaje do funkcjonującego ustroju społeczno-gospodarczego i nie stwarza warunków do sprawnego funkcjonowania systemu obronnego państwa. Nieodzowną sprawą jest także jak najszybsze, wyraźne określenie kompetencji naczelnych organów władzy państwowej w zakresie kierowania gospodarką obronną państwa.

Polityka gospodarczo-obronna jest częścią polityki państwa związanego z tworzeniem warunków i wykorzystaniem potencjału gospodarczego zgodnego ze strategią bezpieczeństwa państwa, traktowaną jako wypadkowa ogólnej strategii obronności państwa oraz strategii rozwoju gospodarczego kraju.

W istocie rzeczy zagrożenia, szanse i możliwości rozwojowe generowane są przez oba te obszary. W wymiarze zewnętrznym polityka gospodarczo-obronna Polski jest determinowana przez dwa wymiary, których postać wymaga podejmowania decyzji strategicznych, aby dostosować się o sytuacji międzynarodowej i wewnętrznej. Wyraża się to wykorzystaniem rodzących się szans i możliwości, które są tworzone przez inne podmioty środowiska międzynarodowego oraz przeciwdziałaniu zagrożeniom o charakterze gospodarczym, militarnym i politycznym. Prowadzona polityka gospodarczo-obronna powinna poddawać analizie zagrożenia kryzysowe z obszaru ekonomii i obronności, mające charakter regionalnych i ponadregionalnych zagrożeń o charakterze militarnym lub pozamilitarnym, które mogą wystąpić w bliskim, jak i dalszym otoczeniu naszego kraju i bezpośrednio odnosić się do naszego państwa. Wynika stąd, że polityka gospodarczo-obronna posiada wpływ na kształt strategii bezpieczeństwa w części dotyczącej wykorzystania potencjału gospodarczo-obronnego oraz występujących zagrożeń w sferze ekonomicznej. Utrzymanie, restrukturyzacja i modernizacja narodowego przemysłu obronnego stanowi ważną przesłankę realizacji strategii bezpieczeństwa RP. Zgodnie z Ustawą o wspieraniu restrukturyzacji przemysłowego potencjału obronnego i modernizacji technicznej Sił Zbrojnych RP „Strategia...” określa, że państwo jest zdecydowane utrzymywać potencjał polskiego przemysłu obronnego na poziomie gwarantującym bezpieczeństwo państwa.

W zakresie zagrożenia ekonomicznego w „Strategii” stwierdza się, że w dobie globalizacji, charakteryzującej się dużym stopniem wzajemnych powiązań ekonomicznych, gospodarka w coraz większym stopniu wpływa na kwestie związane z bezpieczeństwem państwa. Odnosi się to zarówno do potencjału gospodarczego państwa, jego stabilności makroekonomicznej i finansowej, jak i ilości środków przeznaczonych na obronność oraz do zdolności przemysłu obronnego. Zagwarantowanie świadczeń obronnych ze strony prywatnych przedsiębiorców prowadzących swoją działalność na terytorium Polski jest konieczna jako czynnik stanowiący między innymi o zapleczu logistycznym operacji wojskowych prowadzonych przez stronę polską.

Współczesne rozumienie bezpieczeństwa państwa stanowi szerokie spektrum wartości obejmujące:

- trwanie samego państwa w systemie międzynarodowym bez uszczerbku dla jego pozycji w różnych aspektach;
- realizację różnorodnych interesów (wartości egzystencjonalnych, rozwojowych i wyższego rzędu) społeczeństwa zorganizowanego w państwo.

Można je sprowadzić do dwóch poziomów:

- pewne minimum, którym jest fizyczne istnienie państwa i przetrwanie narodu (bezpieczeństwo jako zaspokojenie podstawowych potrzeb egzystencjonalnych - takich jak żywność i okrycie dla pojedynczych ludzi, którym odpowiada pojęcie dóbr podstawowych);
- ochronę już istniejącego stanu i możliwości rozwoju, które mogą być włączane po ich zaspokojeniu potrzeb podstawowych mogą inne potrzeby (np. rozwój, prestiż, dominacja, którym odpowiada pojęcie dóbr wyższego rzędu).

Bezpieczeństwo ekonomiczne wspólnie z bezpieczeństwem politycznym i militarnym stanowi część składową racji stanu państwa. Racja stanu nie jest ani jednoznacznie określona ani stabilna. Jest ona, bowiem definiowana przez różne siły polityczne w zależności od oceny sytuacji międzynarodowej, stanu gospodarki, nastrojów społecznych, własnego systemu wartości.

Racja stanu wymaga zagwarantowania bezpieczeństwa politycznego, militarnego i ekonomicznego lub podjęcia działań i użycia środków mających zapewnić lub przywrócić pożądany stan.

Rola polityki gospodarczo - obronnej w systemie bezpieczeństwa państwa wymaga wspierania jej ustawicznie aktualizowanymi analizami wewnętrznych i zewnętrznych uwarunkowań bezpieczeństwa państwa. Szczególnie odnosi się to do wymiaru politycznego, gospodarczego i militarnego bezpieczeństwa oraz do tych, które nabrały w ostatnich latach znaczenia we współczesnym świecie, tj. ekologicznego, społecznego i prawno-legislacyjnego.

Realne uwarunkowania kształtowania polityki gospodarczo-obronnej, rozpoznawane w wymiarze zewnętrznym i wewnętrznym.

- □ zapewnienia suwerenności narodowej;
- □ zapewnienia bezpieczeństwa państwa i jego obrony przed zagrożeniami zewnętrznymi.

Z celów ekonomicznych wynikają między innymi następujące zadania:

- pomnażanie bogactwa kraju przez optymalne wykorzystanie zasobów narodowych;
- powiększanie materialnych podstaw dobrobytu społeczeństwa.

Wskazane zadania są tożsame ze strategicznymi celami polskiej polityki bezpieczeństwa zawartymi w strategii bezpieczeństwa państwa. Kierowanie i zarządzanie w sytuacjach zagrożeń bezpieczeństwa państwa jest złożonym i trudnym zadaniem dla poszczególnych szczebli administracji państwowej (zarówno rządowej jak i lokalnej), którzy realizują swoje zadania przy pomocy powołanych na tych szczeblach zespołów (np. reagowania kryzysowego) i sieci stanowisk operacyjno-koordynacyjnych (tzw. centrów zarządzania kryzysowego).

Pośród problemów, które w obszarze bezpieczeństwa państwa nabierają szczególnej rangi, pojawił się problem pojmowania istoty i charakteru zagrożeń państwa, kierowania państwem w sytuacjach kryzysowych i związane z nim funkcje i zadania organów zarządzających z ich bazą techniczną oraz zasady i sposoby organizacji. Dla rozwiązania tych problemów zostały zdefiniowane pewne ustawy ustrojowe, szczególnie na poziomie terytorialnym oraz regulacje prawne definiujące zarządzanie w sytuacjach kryzysowych. Budowanie takiego systemu reagowania na wypadek szczególnych zagrożeń nie jest procesem łatwym. Szczególnie wtedy, gdy zarządzanie w sytuacjach kryzysowych będzie obejmować wszystkie aspekty zagrożeń i ich skutki (np. stan zagrożenia, konflikt lokalny, wojna, klęski żywiołowe, klęski ekologiczne itp.)

Dlatego zarządzanie państwem w sytuacjach szczególnych zagrożeń jest zadaniem dla poszczególnych szczebli administracji państwowej (zarówno centralnej jak i lokalnej), która realizuje swoje zadania przy pomocy powołanych na tych szczeblach zespołów reagowania kryzysowego i sieci stanowisk operacyjno-koordynacyjnych, tzw. centrów zarządzania kryzysowego. Szczególnego potraktowania wymaga system informacyjny (systemy teleinformatyczne), który powinien zapewnić stabilną i pewną komunikację pomiędzy organami zarządzania

Przeprowadzone rozważania upoważniają do stwierdzenia, że polityka gospodarczo-obronna i strategia bezpieczeństwa państwa posiadają wspólne obszary zainteresowania.

W centrum uwagi polityki gospodarczo-obronnej znajdują się procesy zachodzące w gospodarce obronnej ze szczególnym zwróceniem uwagi na:

a) określenie kierunków rozwoju gospodarczego z uwzględnieniem ogólnie określonych potrzeb obronnych; stosunków własności w sektorze obronnym gospodarki; zasad funkcjonowania przemysłu obronnego (wielkości, struktury, rozmieszczenia przestrzennego); zasad stosunków gospodarczych z zagranicą, zwłaszcza zaś w produkcji zbrojeniowej, wielkości, struktury i dyslokacji rezerw mobilizacyjnych; sposobów finansowania poszczególnych elementów systemu obronnego (sił zbrojnych rezerw mobilizacyjnych, infrastruktury obronnej itp.);
b) sterowanie poziomem mobilizacyjnej gospodarki obronnej;
c) inicjowanie i sterowanie: koordynacja prac naukowo-badawczych oraz przygotowanie kadr dla potrzeb obronnych.

Polityka gospodarczo-obronna państwa - jak wspomniano poprzednio - posiada wymiar polityki bezpieczeństwa państwa i jest realizowana na trzech wzajemnie powiązanych ze sobą obszarach: politycznym, militarnym i gospodarczym. Istniejące związki i zależności w obszarze bezpieczeństwa państwa wyraźnie wskazują na rolę polityki gospodarczo-obronnej państwa w procesach kształtowania jak i realizacji strategii bezpieczeństwa państwa. Politykę gospodarczo-obronna należy traktować, więc zarówno jako wyraz dociekań uogólniających, sprowadzających się do określenia celów, środków, metod i narzędzi realizacji przedsięwzięć państwa zmierzających do kształtowania, umacniania i utrzymania bezpieczeństwa państwa, jak również praktycznej realizacji tych celów przy wykorzystaniu w praktyce, w określonych warunkach, konkretnych jej środków, metod i narzędzi.

Strategia bezpieczeństwa państwa określa cele ustrojowo-systemowe i polityczne dla polityki gospodarczo-obronnej. Z tych celów wynikają zadania mające zapewnić respektowanie podstawowych wartości dla każdego narodu. Stanowi je zbiór działań na rzecz:

System informacyjny (łączności) zabezpieczający stanowiska kierowania i zarządzania kryzysami powinien być więc systemem elastycznym, umożliwiającym jego etapową rozbudowę oraz powinien zapewniać współpracę z istniejącymi już systemami: publicznymi i prywatnymi, z systemami specjalnymi oraz z infrastrukturami telekomunikacyjnymi państw NATO i systemami krajów sąsiednich (nie będących w konflikcie). Celowym jest więc tworzenie takiego systemu, który będzie składał się z infrastruktury:

- telekomunikacyjnej stacjonarnej i mobilnej;
- informatycznej;
- zarządzająco – kontrolnej;
- alarmowania i powiadamiania;
- logistycznej.

Ze względu na istniejące uwarunkowania w planowaniu, organizacji i wykorzystywaniu systemu telekomunikacyjnego (łączności), a zwłaszcza w sytuacjach kryzysowych, stawia się przed nim szereg specyficznych wymagań. ***Wymagania*** te zostały ujęte w następujących aspektach[239]:

1. ***Zapewnienia konsultacji i koordynacji w procesie planowania i wdrażania nowych różnorodnych systemów.***
2. ***Niezbędnego personelu i zarządzania.***
3. ***Technicznych aspektów systemu telekomunikacyjnego.***
4. ***Realizacji wymaganych usług telekomunikacyjnych.***

W każdym kraju jest powołany specjalny organ zarządzający do nadzorowania – wydatkowania przydzielonych nakładów na krajowe systemy telekomunikacyjne, co w efekcie zapewni bezprzerwową łączność krajową i międzynarodową w sytuacjach szczególnych zagrożeń, kryzysu i wojny. Nakłady te powinny zapewnić regularne konsultacje, koordynację niezbędnych przedsięwzięć oraz wymianę informacji pomiędzy krajami członkowskimi i wewnątrz Sojuszu. Operatorzy telekomunikacyjni muszą posiadać możliwie najaktualniejsze informacje odnośnie wymagań obronnych, ażeby zaimplementować je w nadzorowanej sieci w dopuszczalnych terminach. Dlatego

---

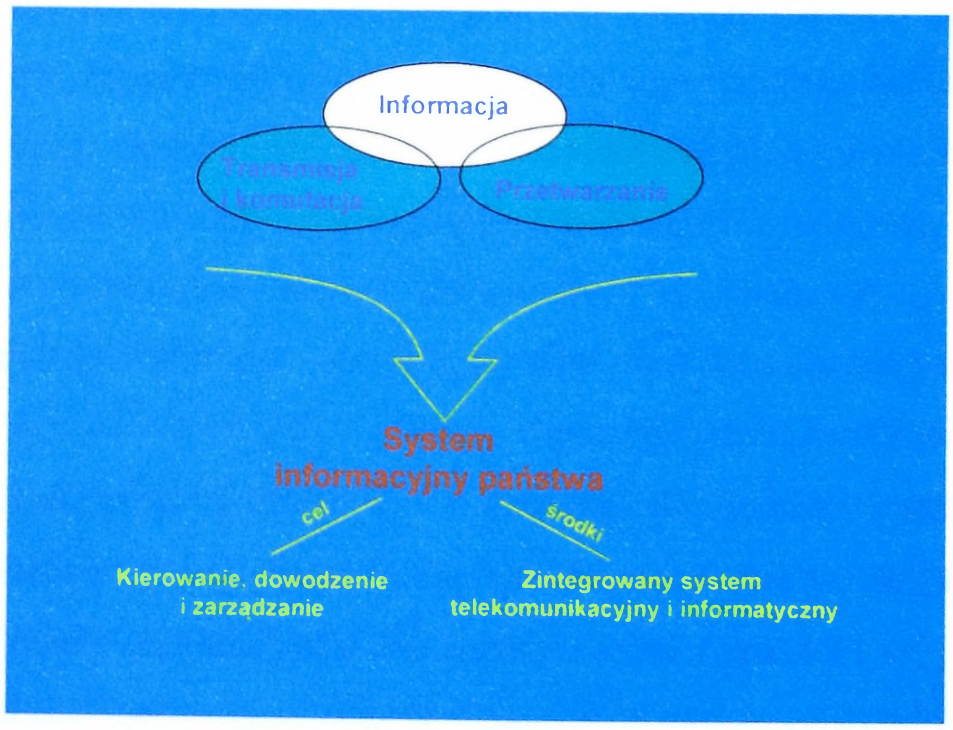
[239]Por. *System kierowania obronnością..., wyd. cyt.*, s. 134.

oraz podmiotami reagowania, od których zależy efektywność podejmowanych działań na zagrożonym terenie (Schemat 3.1.). Funkcjonowanie organów kierowniczych administracji państwowej w systemie zarządzania kryzysowego będzie możliwe w przypadku:

- stworzenia oraz zapewnienia warunków do ciągłego funkcjonowania systemu telekomunikacyjnego (stacjonarnego i mobilnego) włączonego w system ogólnokrajowy z określonymi punktami dostępu do systemu międzynarodowego (w tym z systemem koalicyjnym NATO);
- określenia i przyjęcia standardów w odniesieniu do systemów łączności, informatycznych, baz danych, map cyfrowych itp.;
- określenia respondentów w zakresie pozyskiwania i przekazywania informacji, w tym szczebla centralnego;
- określenia sposobów zbierania informacji z systemów monitorowania i wykrywania;
- określenia sposobów ostrzegania i alarmowania ludności (radiodyfuzja, telewizja itp.).

Schemat 3.1.

Atrybuty systemu informacyjnego państwa



Źródło: G. Różański, *Rola infrastruktury technicznej w zabezpieczeniu funkcjonowania systemów informacyjnych w stanach nadzwyczajnych,* w: Kierowanie obronnością w aspekcie wykorzystania środków najnowszej generacji, Materiały z konfer. nauk. Sz. Gen. WP, AON, Warszawa 2001, s. 57.

organizacyjne. Ich zadaniem jest zapewnienie utrzymania ciągłości kierowania oraz sprawnego przejścia gospodarki i sił zbrojnych ze struktury pokojowej na wojenną. W wielu krajach o rozwiniętych demokracjach struktury te są takie same lub zbliżone. System kierowania obronnością państwa, obok podsystemu militarnego i pozamilitarnego jest jednym z zasadniczych elementów systemu obronności. Jego rola polega na informacyjnym sprzężeniu poszczególnych elementów systemu obronności w jednolitą i sprawnie funkcjonującą całość. O jego efektywności decyduje nie tylko właściwy dobór kadr na kierownicze stanowiska i funkcje, ale i jego struktura gospodarcza, a przede wszystkim infrastruktura teleinformatyczna (telekomunikacyjna i informatyczna). Szczególnego potraktowania wymagają systemy teleinformatyczne, które muszą zapewnić stabilną i pewną komunikację pomiędzy organami zarządzania oraz podmiotami reagowania od których zależy efektywność podejmowanych działań na zagrożonym terenie[240].

Funkcjonowanie organów zarządzania w systemie zarządzania kryzysowego będzie możliwe w przypadku:

- stworzenia oraz zapewnienia warunków do ciągłego funkcjonowania systemu telekomunikacyjnego (stacjonarnego i mobilnego) włączonego w system ogólnokrajowy z określonymi punktami dostępu do systemu międzynarodowego (w tym z systemem koalicyjnym NATO);
- określenia i przyjęcia standardów w odniesieniu do systemów łączności, informatycznych, baz danych, map cyfrowych itp.;
- określenia respondentów w zakresie pozyskiwania i przekazywania informacji, w tym szczebla centralnego;
- określenia sposobów zbierania informacji z systemów monitorowania i wykrywania;
- określenia sposobów ostrzegania i alarmowania ludności (radiodyfuzja, telewizja itp.).

Tak, więc perspektywiczny system teleinformatyczny zabezpieczający kierowanie obronnością w stanach zagrożenia bezpieczeństwa państwa (np. przez centra zarządzania kryzysami) powinien być systemem elastycznym,

---

[240]Por. J. Paczocha, *Metodyka projektowania systemu telekomunikacyjnego dla potrzeb bezpieczeństwa państwa*, WS-O, AON, Warszawa 2004.

niezbędne są ciągłe konsultacje pomiędzy operatorami i właściwymi władzami krajowymi. Wielostronne konsultacje powinny zapewnić gwarancję uwzględnienia wymagań NATO w działaniach władz krajowych i operatorów telekomunikacyjnych mających na celu zapewnienie ciągłości świadczenia podstawowych, międzynarodowych usług telekomunikacyjnych.

W czasie sytuacji kryzysowych systemy telekomunikacyjne muszą być przygotowane na gwałtowne zmiany natężenia ruchu i zapewnić wymagane usługi wspomagające kierowanie działaniami obronnymi. W okresie kryzysu (zagrożenia wojennego), w przypadku podjęcia odpowiednich decyzji przez władze krajowe, operatorzy telekomunikacyjni powinni być przygotowani do wdrożenia (uruchomienia) wcześniej zaplanowanych zasobów telekomunikacyjnych na okres „W" Zasoby te powinny zapewnić – bezpieczną (utajnioną) wymianę informacji międzynarodowych (koordynacja kryzysu). W kraju powinny być zagwarantowane wymagane i wykwalifikowane zespoły ludzkie zdolne zająć się eksploatacją sieci telekomunikacyjnych w sytuacjach kryzysowych. Wyznaczony personel musi być przeszkolony np. dzięki uczestnictwu w specjalistycznych ćwiczeniach. Muszą być także zapewnione wystarczające i bezpieczne środki telekomunikacyjne dla powołanych na odpowiednich szczeblach Centrów Zarządzania Kryzysowego. Organy zarządzające muszą być przygotowane dla:

- właściwej organizacji i zapewnienia dodatkowych usług w tych obszarach, w których przewidywane są zintensyfikowane działania;
- wzmocnienia środków bezpieczeństwa i zwiększenie stanu osobowego odpowiedzialnego za ochronę przed aktami sabotażu, działaniami dywersyjnymi itp;
- uruchomienia rezerw, zapasów, zdolności produkcyjnych i możliwości napraw;
- informowania i instruowania ludności na temat dobrowolnych i obowiązkowych ograniczeń w zakresie korzystania z usług telekomunikacyjnych stosownie do bieżącej sytuacji.

W celu zapewnienia sprawnego funkcjonowania najwyższych organów władzy, administracji państwa i sił zbrojnych w czasie przechodzenia ze stanu pokojowego na wojenny, już w czasie pokoju tworzy się odpowiednie struktury

sobą w celu zapewnienia łączności właściwym abonentom specjalnym. Wykonywanie tego rodzaju czynności zależne jest od skali wdrożenia odpowiednich systemów sygnalizacji umożliwiających współpracę sieci międzynarodowych i w efekcie wysoką jakość transmisji. W niektórych sytuacjach konieczna może się okazać rozbudowa tych sieci pod kątem obsługi ruchu dodatkowego, generowanego przez abonentów specjalnych. W celu zagwarantowania użyteczności sieci specjalnych i ich łączy na potrzeby zestawiania połączeń w warunkach wojennych, systemy i łącza tych sieci muszą być maksymalnie uodpornione, by prawdopodobieństwo bezprzerwowej łączności było możliwie wysokie. Wymaga to zaimplementowania różnych tras przesyłania ruchu oraz zastosowania wielu dróg łączy obejściowych. Biorąc pod uwagę ograniczoną pojemność krajowych sieci specjalnych, kraje członkowskie NATO mogą wprowadzić kontrolę połączeń zewnętrznych przychodzących do sieci.

Podstawową cechą określającą stopień przydatności projektowanego systemu telekomunikacyjnego na potrzeby najwyższych organów władzy i administracji państwa jest możliwość hermetyzacji czyli zapewnienia najważniejszym abonentom priorytetowego dostępu do świadczonych usług. Cechą sieci hermetycznych jest to, iż tworzą one zamknięte systemy całkowicie niedostępne dla innych abonentów. Sieci takie, poprzez powszechne stosowanie urządzeń kryptograficznych, umożliwiają użytkownikom prowadzenie niejawnej korespondencji. Zaspokojenie ciągle rosnących potrzeb użytkowników, systemów łączności w zakresie usług teleinformatycznych, będzie możliwe poprzez wykorzystanie nowych technik i technologii telekomunikacyjnych. Technologie te zapewnią organom kierującym sytuacjami kryzysowymi niespotykane dotychczas możliwości usługowe dotyczące: szybkiej wymiany danych, transferu dużych zbiorów informacji, rozproszonego przetwarzania danych, wymiany danych w czasie rzeczywistym, przekazywania obrazów ruchomych, itp.

Mobilne systemy radiotelefoniczne posiadają możliwości łatwego i wygodnego ich zastosowania w różnych uwarunkowaniach operacyjnych. Podyktowane to jest głównie zgodnością standaryzacyjną z innymi systemami, elastycznością wyboru pasma częstotliwości (dla systemów trankingowych) oraz łatwością zastosowania w koniecznych miejscach funkcjonowania systemu.

umożliwiającym jego etapową rozbudowę oraz powinien zapewniać współpracę z istniejącymi już systemami: publicznymi i prywatnymi, z systemami specjalnymi oraz z infrastrukturami telekomunikacyjnymi państw NATO i systemami krajów sąsiednich (nie będących w konflikcie).

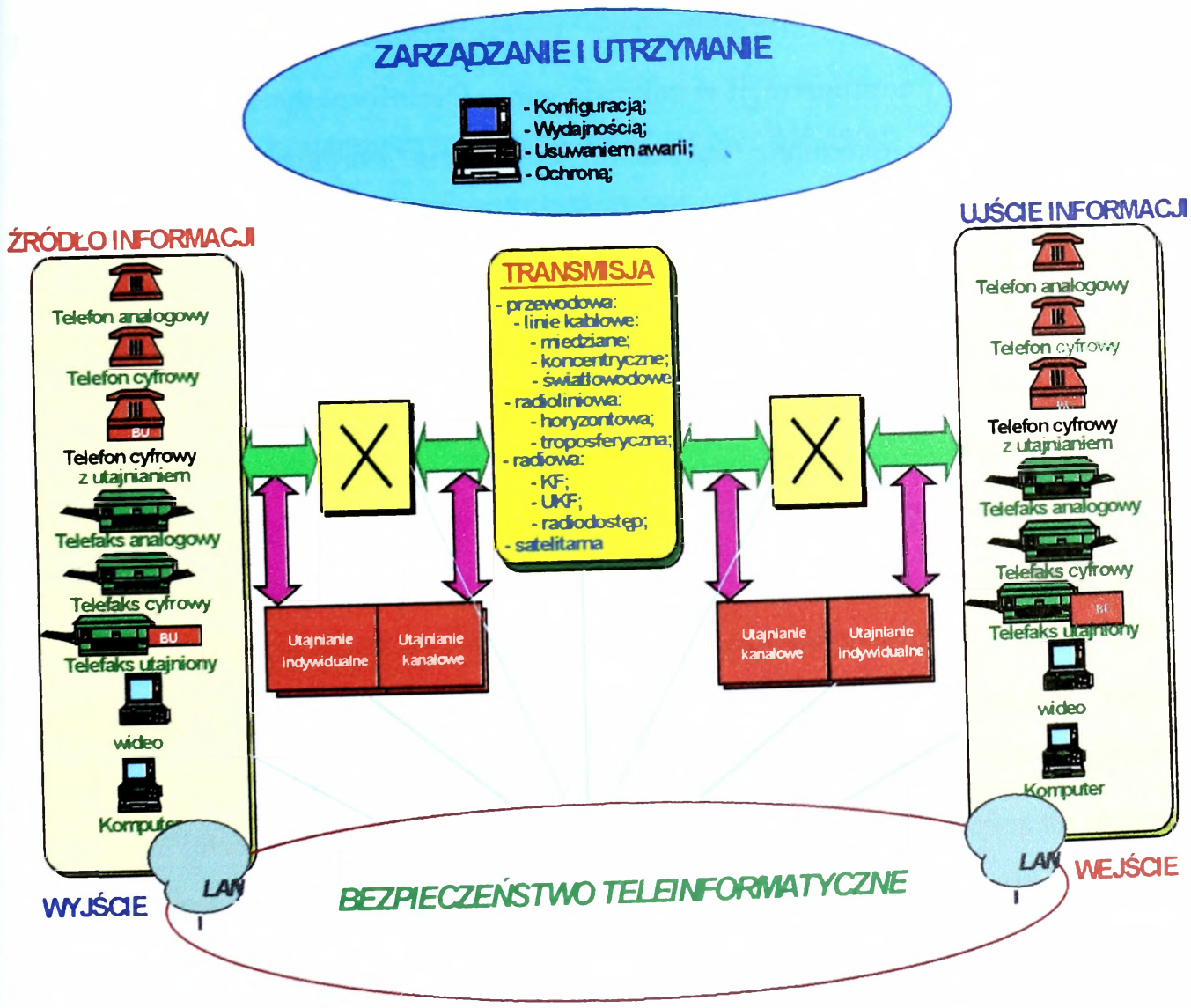
Sytuacje szczególnych zagrożeń bezpieczeństwa państwa wymagają podjęcia skutecznych działań w celu zapewnienia ciągłości świadczenia usług telekomunikacyjnych dla ludności oraz utrzymania dzierżawionych usług międzynarodowych. Szczególnie duże znaczenie ma zapewnienie łączności dyplomatycznej pomiędzy państwami członkowskimi NATO oraz łączności ważnej dla członków sojuszu w ramach struktur, a także pomiędzy sojuszem i innymi państwami. Łączność ta powinna umożliwić skuteczne działania na rzecz uniknięcia kryzysu, a jeśli działania te okażą się nieskuteczne, powinna umożliwić podejmowanie wysiłków na rzecz osiągnięcia pokoju. W czasie kryzysów i wojny konieczne jest zastosowanie odpowiednich środków kontroli, po to zwłaszcza, aby umożliwić podjęcie odpowiednich działań w zakresie zestawiania łączy bezpośrednich i obejściowych pomiędzy członkami sojuszu i innymi państwami. W tym kontekście środki kontroli oznaczają zarządzanie łączami i ruchem obsługiwanym przez te łącza. Na żądanie właściwych władz krajowych operatorzy telekomunikacyjni powinni stosować odpowiednie środki kontroli w odniesieniu do usług publicznych i dzierżawionych usług międzynarodowych. Rozwiązania tego rodzaju mogą doprowadzić do poszerzenia zwykłych funkcji zarządzania siecią sprawowanych w czasie pokoju.

W celu zagwarantowania skutecznego kontrolowania międzynarodowych usług telekomunikacyjnych, zarówno publicznych, jak i dzierżawionych, ważne jest, aby wszystkie kraje członkowskie NATO wprowadziły uzgodnione środki kontroli jednocześnie respektując przy tym odpowiednie rozporządzenia NATO. W celu zapewnienia wysokiego poziomu usług telekomunikacyjnych możliwe jest budowanie sieci specjalnych, wydzielonych z sieci publicznych na potrzeby władz krajowych w sytuacjach szczególnych zagrożeń, kryzysów międzynarodowych lub wojny. Krajowe sieci specjalne mają z reguły ograniczoną pojemność i możliwości obsługi ruchu telekomunikacyjnego. W czasie pokoju lub we wczesnej fazie kryzysu korzystne jest łączenie poszczególnych krajowych sieci specjalnych ze

Docelowy system łączności rozwijany na potrzeby bezpieczeństwa państwa do kierowania obronnością, przy zapewnieniu wysokiej niezawodności działania, powinien zapewnić ciągłość łączności oraz umożliwić bezpieczną wymianę informacji między poszczególnymi stanowiskami w postaci świadczenia wielu różnorodnych usług, a szczególnie multimedialnych umożliwiających przesyłanie różnego typu wiadomości i danych (Schemat 3.2.).

Schemat 3.2.

Elementy składowe systemu teleinformatycznego
na potrzeby kierowania bezpieczeństwem państwa



Źródło: W. Wojciechowski, M. Żochowski, *Koncepcja zarządzania infrastrukturą teleinformatyczną sił zbrojnych w stanach nadzwyczajnych,* w: Kierowanie obronnością w aspekcie wykorzystania środków najnowszej generacji, Materiały z konfer. nauk. Sz. Gen. WP, AON, Warszawa 2001, s. 66.

Wymagania najwyższych organów władzy, administracji państwowej i sił zbrojnych wobec telekomunikacji są szczególne. Zaliczyć do nich należy:

Urządzenia wykonane w nowych technologiach teleinformatycznych są podatne na zarządzanie, co sprawia, że można dokonywać rekonfiguracji systemu dopasowując go do określonych wymagań i potrzeb stanów nadzwyczajnych. Zakłada się przy tym, że systemy współpracujące i podległe mogą być wykonane w różnych technologiach np.:

- zgodnych z technologiami wykorzystanymi np. ISDN, ATM, TCP/IP;
- w technologii cyfrowej z modulacją „delta" (modulacją CVSD);
- w technice cyfrowej z modulacją PCM oraz usługami ISDN, ATM i itp.;
- w technice analogowej z systemem telekomunikacyjnym państwa i systemami resortowymi.

W ramach aktualnych tendencji rozwojowych systemu teleinformatycznego, wymieniane się trzy podstawowe grupy wymagań:

- trwałości – a więc zapewnienia odporności na zakłócenia, dużej niezawodności i żywotności, co wiąże się z budową sieci o strukturze siatkowej;
- skrytości - zapewnienia utajniania z wymaganą mocą kryptograficzną;
- mobilności – tzn. zachowania ciągłości łączności w czasie przemieszczania się stanowisk kierowania i dowodzenia.

Planowany system teleinformatyczny (łączności) powinien umożliwiać przesyłanie informacji do korespondentów w sposób bezpieczny. Reorganizacja systemu obronności państwa pociągać będzie za sobą jego przebudowę, polegającą na dynamicznej zmianie funkcji i aktywności poszczególnych stanowisk, dokonywana w celu dostosowania struktury kierowania obronnością państwa do aktualnej sytuacji stanu nadzwyczajnego, możliwości realizacyjnych i potrzeb, spowoduje potrzebę rekonfiguracji systemu łączności.

Kierunki rozwoju organizowanego systemu teleinformatycznego powinne uwzględniać i nadążać za dynamicznymi zmianami struktury organizacyjnej stanowisk kierowania i dowodzenia. Realizacja zadań stawianych systemowi kierowania obronnością państwa będzie integralnie związana z permanentną dynamiczną rekonfiguracją jego struktury. Rekonfiguracja ta polegać będzie głównie na zmianie funkcji poszczególnych stanowisk kierowania i dowodzenia spowodowanej aktualną sytuacją występujących zagrożeń.

3.2.1. Formuła sfery realnej modelu kształtowania bezpieczeństwa państwa

Zakres formuły sfery realnej modelu kształtowania bezpieczeństwa państwa wymaga zidentyfikowania oraz uporządkowania związanych z nią głównych kwestii stanowiących o jej istocie. Koniecznym i celowym jest określenie miejsca i roli gospodarki w systemie bezpieczeństwa państwa, istoty sfery realnej gospodarczych podstaw bezpieczeństwa państwa oraz ukazania problemów tworzenia i utrzymania gospodarczych podstaw bezpieczeństwa państwa.

Celem gospodarowania jest zaspokajanie występujących różnorodnych potrzeb w możliwie najpełniejszy sposób. Dotyczy to również potrzeb związanych z bezpieczeństwem. Dlatego też mając na uwadze ogół potrzeb społeczeństwa państwa, które ma zaspokoić gospodarka można umownie podzielić na dwie zasadnicze grupy:

- potrzeby konsumpcyjne i rozwojowe społeczeństwa;
- potrzeby związane z bezpieczeństwem.

W tym kontekście należy, chociaż bardzo ogólnie przybliżyć pojęcie gospodarki narodowej. W tradycyjnej ekonomii istniały dwa ściśle ze sobą powiązane pojęcia: gospodarstwa narodowego i gospodarki narodowej.

Pierwsze oznaczało ogół ludności i całość środków materialnych, znajdujących się w granicach danego kraju oraz system instytucji określających sposób dysponowania tymi środkami.

Drugie pojęcie odnosiło się do całości działalności danego gospodarstwa narodowego. Jeśli gospodarstwo narodowe stanowiło ramy rzeczowo-instytucjonalne, to gospodarka narodowa była całokształtem procesów, ukierunkowanych na tworzenie i podział bogactwa; mówiąc inaczej, była synonimem gospodarowania.

Opierając się na rozróżnieniu w rzeczywistości gospodarczej zasobów i procesów - opis gospodarki narodowej przedstawia się jako:

- gospodarstwa społecznego (narodowego) obejmującego różne elementy odpowiednio uporządkowane i pozostające w odpowiednich relacjach względem siebie;
- gospodarki narodowej w znaczeniu procesu gospodarowania.

W literaturze przedmiotu o ekonomii najczęściej mówi się o typach gospodarek,

- utrzymanie wyprzedzającej gotowości systemu w każdej sytuacji, a przede wszystkim w stanach nadzwyczajnych;
- zapewnienie bezpieczeństwa przekazywanych informacji i ochrony systemu;
- zapewnienie adaptacyjności i mobilności systemu;
- zintegrowanie rozwiązań technicznych w celu zapewnienia współdziałania wszystkich elementów podsystemów telekomunikacyjnego i informatycznego;
- uzyskanie efektywności ekonomicznej rozwiązań systemowych.

Realizacji przedstawionych wymagań i zadań powinny sprzyjać:

- ☐ jednoznacznie sformułowane i skoordynowane potrzeby organów władzy i administracji w zakresie usług teleinformatycznych;
- ☐ wyraźnie określone założenia techniczne i organizacyjne dotyczące wszystkich elementów systemu;
- ☐ możliwość wyboru najkorzystniejszych rozwiązań spełniających powyższe wymagania ogólne integrujące potrzeby użytkowników z uwzględnieniem ich specyfiki, np. sił zbrojnych, policji, straży pożarnej, urzędu celnego, itp.

Spełnienie tych wymagań będzie możliwe jedynie w systemie łączności wykorzystującym najnowsze techniki i technologie oraz zasady organizacji łączności, w którym wszystkie ogniwa (węzły komutacyjne) połączone ze sobą na zasadzie równorzędności tworzą strukturę niehierarchiczną, a stosowanie dynamicznego poszukiwania abonenta w sieci czyni taki system łączności odpornym na zniszczenia i podatnym na dynamiczną rekonfigurację całej sieci.

Perspektywiczny system łączności na potrzeby zapewnienia bezpieczeństwa i kierowania obronnością państwa, według przyjętych założeń, powinien stanowić zintegrowany pod względem organizacyjnym i technicznym zespół węzłów, traktów i linii łączności (stałych i rozbudowywanych według potrzeb oraz uzupełnianych doraźnie środkami polowymi), urządzeń komutacyjnych oraz końcowych, zapewniających korzystanie z niezbędnych usług telekomunikacyjnych wszystkim organom kierowania i dowodzenia funkcjonujących w ramach tego systemu.

kraju wobec powiązań z ugrupowaniami integracyjnymi i z gospodarką światową. Prezentowane w literaturze pojęcie gospodarowania jest dość spójne, pomimo pewnych różnic w akcentach i sposobie sformułowania. Część tych definicji akcentuje:

- problem rzadkości,
- inne akcentują sam proces gospodarowania.

W pierwszym ujęciu gospodarowanie definiowane jest jako konieczność dokonywania wyborów ekonomicznych, czyli decydowania, na co przeznaczyć stosunkowo rzadkie zasoby, którymi dysponuje określony podmiot, i jakie potrzeby za ich pomocą zaspokoić. Jednocześnie podkreśla się, że decyzje gospodarcze pociągają za sobą określone korzyści i koszty, co nakazuje dokonywanie optymalizacji efektów tych decyzji[243] .

Drugie - bardziej rozbudowane definicje podają, że gospodarowanie to świadoma i celowa działalność jednostek i zbiorowości ludzkich polegająca na realizacji faz gospodarowania (produkcji, podziale, wymianie lub obiegu, a także konsumpcji dóbr i usług)[244].

Status każdej gospodarki narodowej i przebieg procesu gospodarowania zależy od wielu czynników. Najbardziej wpływowymi są następujące czynniki [245]:

- geograficzny - czynnik geograficzny wyznacza położenie i obszar danego państwa;
- demograficzny - czynnik demograficzny (inaczej ludnościowy) wskazuje nie tylko na liczbę ludności, ale również jej podział według płci, wieku, poziomu wykształcenia, zawodu, liczby ludzi zawodowo czynnych oraz wielkości zatrudnienia;
- materialny - czynnik materialny charakteryzuje bogactwo narodowe danego kraju, wielkość jego majątku narodowego oraz dochodu narodowego;
- ustrojowy - czynnik ustrojowy wskazuje na charakter organizacji i funkcjonowania gospodarki.

---

[243]Por. M. Rekowski, *Wprowadzenie do mikroekonomii. Część I*, PWN, Poznań 1991, s. 6.
[244]Por. O. Lange, *Ekonomia polityczna, tom I i II,* PWN, Warszawa 1978, s. 20.
[245]Por: Z. Stachowiak, *Ekonomia*...wyd.cyt., s. 96.

takich jak nakazowa (planowa), wolnokonkurencyjna (jako model), i funkcjonujących w rzeczywistości gospodarkach mieszanych. Spotyka się także dość często odmienne rozumienie, które obok sposobu organizacji kładzie nacisk lub uwzględnia jej aspektu zasobowego. W tym ujęciu gospodarka narodowa to. całokształt wszystkich podmiotów, instytucji gospodarczych i przedsięwzięć o charakterze gospodarczym realizowanych w obrębie kraju[241]. Najbardziej użytecznym podejściem wydaje się ujmowanie gospodarki narodowej dwojako[242]:

- z jednej strony, jako względnie odosobniony makrosystem (lub podsystem) społeczny;
- z drugiej strony, jako całokształt zasobów i działalności prowadzonej w danym kraju w celu zaspokajania potrzeb.

Każde z tych podejść pozwala dostrzec inną stronę jej istoty, struktury oraz funkcjonowania. W obu ujęciach jest ona przy tym dostrzegana w skali makroekonomicznej.

W pierwszym rozumieniu - gospodarka narodowa, jako system względnie odosobniony, a więc jest jednocześnie częścią większego systemu, jakim jest społeczeństwo i państwo. Stanowi ona wyodrębniony i specyficzny element, chociaż wielostronnie powiązany z innymi częściami tego systemu. Składa się ona z określonych elementów, wzajemnie od siebie zależnych. Charakteryzuje się jednocześnie sprzężeniami zwrotnymi związków i zależności między elementami ją tworzącymi. Jako taka, jest ona zbiorem elementów powiązanych ze sobą łańcuchem oddziaływań przyczynowo-skutkowych.

W drugim rozumieniu - gospodarka narodowa rozpatrywana jako całokształt zasobów i działalności prowadzonej w sferze produkcji, podziału, obiegu (wymiany) i konsumpcji w danym kraju, widziana jest przede wszystkim, jako podstawa służąca zaspokajaniu potrzeb społeczeństwa. Patrząc zarówno z punktu widzenia teorii, jak i praktyki, dostrzegać trzeba w niej podstawowy zakres działalności gospodarczej. Jako taka, określa ona jednocześnie nieregionalny i nieodcinkowy charakter działalności gospodarczej lub wielkości ekonomicznych. Dostrzegać trzeba w niej równocześnie odrębność i suwerenność gospodarki danego

---

[241] *Słownik terminów z zakresu bezpieczeństwa...,wyd. cyt.,* s. 40.
[242] Por: Z. Stachowiak, *Ekonomia zarys podstawowych problemów*, WSZi I, AON, Warszawa 2000, s. 96.

przetwarzanie zasobów przyrody i informacji. W instytucjach gospodarczych, politycznych i społecznych ma miejsce jedynie przetwarzanie informacji.

Układ informacyjny należy określić jako otwarty zbiór sygnałów – wiadomości opisujących stany przekształcenia środowiska wewnętrznego systemu gospodarczego i jego otoczenia przyrodniczego (zewnętrznego). Do zbioru informacji wchodzą obok sygnałów – wiadomości na bieżąco pobieranych przez organizacje i instytucje również informacje będące zbiorami wiedzy o środowisku gospodarczym i przyrodniczym.

Układ etycznych norm postępowania jest zbiorem sygnałów regulacji zachowań ludzi względem siebie i środowiska przyrodniczego, na które składają się normy obyczajowe i prawne. Wśród norm etycznych postępowania wyróżnia się normy szczególne, stanowiące wartości podstawowe typu egzystencjalnego, których przestrzeganie określa postawy ludzi wobec siebie i środowiska przyrodniczego.

Układ kategorii obsługi więzi tworzą normy regulacji procesu gospodarczego, które są normami wyboru decyzji ekonomicznych. Wyróżnia się normy wyboru typu ekonomicznego i bezpośredniego. Ekonomicznymi normami regulacji są kategorie towarowo - pieniężne, wykształcone w historycznym rozwoju stosunków towarowych. Obsługują one układy poziomych więzi ekonomicznych między samymi organizacjami i instytucjami działalności gospodarczej. Normy bezpośrednie są kategoriami obsługi więzi między państwem i organizacjami i instytucjami gospodarczymi, które są więziami pionowymi.Identyfikując relacje pomiędzy gospodarką i bezpieczeństwem państwa zauważyć trzeba poglądy twórców nowoczesnej ekonomiki obrony stwierdzające, że problem bezpieczeństwa kraju w teorii może być uznany za jeden wielki problem ekonomiczny[247] - co wynika bezpośrednio z rzadkości zasobów.

Zasoby posiadane przez każdy kraj obecnie oraz przypuszczalne, dostępne w przyszłości, są w sposób konwencjonalny klasyfikowane przez ekonomistów, jako różnego rodzaju zasoby ziemi, pracy i kapitału. Mogą być one wykorzystane dla zaspokojenia wielu potrzeb kraju oraz jego obywateli, tj. dla bezpieczeństwa narodowego, podniesienia stopy życiowej, na ubezpieczenia społeczne,

---

[247]Por. C. J. Hitch, R. N. McKean, *Ekonomika obrony w erze jądrowej*, MON, Warszawa 1965, s. 26.

System gospodarczy jest organizmem społeczno-ekonomicznym charakteryzującym się:

- suwerennością terytorialną, odrębnością etniczną, językiem i kulturą;
- zdolnością do zaspokajania potrzeb (systemu), wchodzących w jego skład zbiorowości;
- zdolnością do trwania w rozwoju historycznym;
- zdolnością do zachowania suwerenności i odrębności;
- zarządzaniem odpowiednim do systemu;
- celowością działania.

Zorganizowanie systemu gospodarczego składa się z czterech układów, do których należą[246]:

- ☐ układ instytucjonalno-organizacyjny (typu blokowego);
- ☐ układ informatyczny;
- ☐ układ norm etycznych (postępowania);
- ☐ układ kategorii więzi między blokowymi elementami systemu.

Układ instytucjonalno-organizacyjny tworzą:

a) osoby fizyczne (pojedynczy ludzie);
b) organizacje działalności gospodarczej (firmy) instytucje gospodarcze;
c) instytucje polityczne i społeczne, a w ich zestawie instytucja o szczególnym znaczeniu, jaką jest państwo.

Organizacje gospodarcze i instytucje są subsystemami, czyli układami względnie odosobnionymi, zdolnymi do samoistnego bytu, posiadającymi wejścia i wyjścia, dla których otoczeniem jest bądź środowisko przyrodnicze i gospodarcze, bądź wyłącznie gospodarcze. Organizacje gospodarcze i instytucje posiadają swoją wewnętrzną strukturę.

Wewnątrz organizacji gospodarczej działają również instytucje, jako ich element blokowy, utrzymujący łączność z otoczeniem w drodze poboru informacji i reakcji na kategorie obsługi więzi i zachowania innych instytucji i organizacji oraz zmiany otoczenia przyrodniczego. W organizacjach gospodarczych zachodzi

---

[246]Por. R. Zieliński, *Alokacja zasobów w gospodarowaniu obronnym, Studium teoretyczne*, UŁ, Łódź 1997, s. 27.

W rozwoju gospodarczym wielu krajów przeważały zjawiska autarkiczne. Stopień współzależności ekonomicznej był niewielki. Nie istniała, więc potrzeba podejmowania szerszych przedsięwzięć (w takim zakresie jak obecnie) chroniących gospodarkę i jej segment ekonomiczno - obronny przed negatywnymi następstwami współzależności. Ponadto pomiędzy pokojowym okresem i wojną występował dość wyraźny rozdział. Oczywiście rozwiązywano wiele spraw /wiązanych z przygotowaniem do wojny w czasie pokoju, ale główne działania przypadały na okres mobilizacji gospodarczej i samej wojny.

Procesy rozwojowe - gospodarcze i technologiczne - doprowadziły do takiej sytuacji, w której pogłębiła się zależność pomiędzy pokojowym rozwojem gospodarczym a wojną, a jednocześnie wyraźnie wzrosła rola pokojowego rozwoju gospodarczego w rozwiązywaniu wielu zadań o charakterze mobilizacyjnym[40]. Sprawiają to takie zjawiska jak:

a) rewolucja w sferze uzbrojenia i zdolność rażenia nowoczesnej broni, które są związane rozwojem technologii (sił wytwórczych);
b) możliwość wystąpienia gwałtownej eskalacji napięć polityczno-militarnych i łącząca się z tym groźba, że nie będzie czasu na mobilizację gospodarczą, powoduje konieczność gromadzenia znaczniejszych rezerw o asortymencie wykraczającym poza uzbrojenie i wyposażenie sił zbrojnych.

Wagę tych kwestii podkreślają utrzymujące się w różnych regionach świata stany napięć, sprzeczności interesów, konflikty polityczne i regionalne konflikty zbrojne. W tej sytuacji naruszenie bezpieczeństwa ekonomicznego godzi bezpośrednio w system obronny.

Wykorzystanie narzędzi ekonomicznych w celach polityczno-militarnych - to problemy znane dobrze w historii całej naszej cywilizacji. Obejmują one szeroki zespół przedsięwzięć wykorzystywanych do realizacji celów polityczno - militarnych. Doceniano w pełni możliwość osiągania tych celów poprzez wpływ na gospodarkę[249].

Rola i znaczenie tego typu działań rosły w miarę postępującego wzrostu

---

[249]Tamże, s.13.

przyspieszenie stopy wzrostu gospodarczego itd.. Są to oczywiście konkurujące ze sobą cele. Ogólnie biorąc, im więcej zasobów poświęca się na bezpieczeństwo narodowe, tym mniej ich pozostaje np. na ubezpieczenia społeczne i na odwrót. Jest to, więc problem alokacji zasobów kraju pomiędzy różne przedsięwzięcia odpowiadające odmiennym celom.

Te kwestie są niezwykle istotne z punktu widzenia rozstrzygania podstawowych problemów ekonomicznych. Wiąże się to z przeniesieniem potrzeb z fazy postulacyjnej do fazy realizacyjnej. Sprowadzają się one do odpowiedzi na pytania:

- co wytwarzać, (produkować), jakie dobra i usługi?
- w jaki sposób je wytwarzać?
- dla kogo produkować, kto je otrzyma?

W tym kontekście, ważne jest rozpatrzenie relacji pomiędzy poziomem bezpieczeństwa państwa a gospodarką. Podstawowe znaczenie mają współzależności pomiędzy płaszczyznami bezpieczeństwa ekonomicznego (ogólnoekonomiczną i gospodarczo - obronną). Na tej podstawie można mówić o rozwoju potencjału ekonomicznego gospodarki w ogóle czy jej poszczególnych ogniw, ale równocześnie trzeba wskazać na ich znaczenie obronno - ekonomiczne (w tym wpływ na tworzenie i rozwój potencjału gospodarczo - obronnego). W ramach tych współzależności pokojowy rozwój gospodarki gwarantuje wzrost możliwości obronnych państwa i odwrotnie, wzrost możliwości obronnych gwarantuje dalszy pokojowy rozwój. Kwestię tą ujmuje Z. Kołodziejak stwierdzając, że ta zależność wynika ze ścisłego związku pomiędzy rozwojem sił wytwórczych i mocy ekonomicznej państwa (zespołu państw), a przygotowaniami do odparcia ewentualnej agresji. Zależność ta wskazuje niezbicie, że zarówno dla teorii obronno - ekonomicznej jak i praktyki nie może być sprawą obojętną problem bezpieczeństwa ekonomicznego[248].

Poprzednio bezpieczeństwo państwa pojmowano głównie w kategoriach polityczno - militarnych, złożoność tej problematyki była o wiele mniejsza. Poszczególne systemy gospodarcze były dość luźno ze sobą powiązane.

---

[248]Por. E. Frejtag Mika, Z. Kołodziejak, W. Putkiewicz, *Bezpieczeństwo...*,wyd. cyt., s. 11.

i militarnego oddziaływania w stosunkach międzynarodowych (np. sankcje gospodarcze, embargo na dostawy i handel).

Punktem wyjścia do określenia miejsca i roli gospodarki w systemie bezpieczeństwa państwa, powinny stać się możliwości realizacji zadań potencjału gospodarczego (rozpatrywanych w kontekście zdolności systemu gospodarczego do dostarczenia odpowiednich środków na te różnorodne zadania). Do nich należy także bezpieczeństwo. Dlatego istotnym zadaniem gospodarki jest wydzielenie niezbędnych środków dla realizacji i ochrony pozaekonomicznych interesów, (w tym poprzez wytwarzanie i dostarczanie dóbr publicznych). Inaczej mówiąc zadania związane z bezpieczeństwem obejmują różne płaszczyzny, spośród których najważniejsze mieszczą się w sferze: politycznej, militarnej i ekonomicznej.

Gospodarka, jak każdy system ma swoją specyficzną strukturę i opisywana jest często poprzez charakterystykę jej części składowych wyróżnionych na podstawie różnych kryteriów. Do najważniejszych spośród nich zaliczyć trzeba[250]:

- strukturę podmiotową;
- strukturę własnościową;
- strukturę prawno-organizacyjną;
- funkcjonalno-instytucjonalną(funkcjonalno-organizacyjną);
- strukturę produkcyjną (rzeczową) gospodarki (działową gałęziową, branżową, asortymentową i jakościową);
- strukturę zatrudnienia i kwalifikacji;
- strukturę stosowanych technologii.

Możliwości sfery realnej gospodarki można oceniać z dwóch stron:

- z pierwszej, od strony możliwości realizacji zadań gospodarczych (w tym politycznych i militarnych);
- z drugiej, od strony podatności na naciski zewnętrzne i zaburzenia wewnętrzne.

Gospodarka umożliwiająca osiąganie celów politycznych może być wrażliwa

---

[250]Por. Z. Stachowiak, *Ekonomia* ...wyd. cyt., s. 36.

współzależności i zależności ekonomicznej oraz uzależniania się zjawisk wojennych od czynnika ekonomicznego. Poczynania te, zaliczane do wojny gospodarczej, szczególnie szeroko wykorzystywane są po II wojnie światowej, zwłaszcza w okresie zimnej wojny i embarga wobec byłych krajów, wobec byłych krajów socjalistycznych przez USA i inne państwa NATO. Było ono jednym z najbardziej i drastycznych i powtarzalnych objawów wykorzystywania narzędzi ekonomicznych w celach polityczno-militarnych. Zmianie ulegają tylko ich formy w zależności od stanu stosunków międzynarodowych. Przez wiele lat wywoływały one wiele trudności gospodarczych - bowiem:

- wymuszały tendencje samowystarczalności gospodarczej narodu;
- powodowały niekorzystne zmiany strukturalne w gospodarkach;
- pogłębiały ekstensywne formy rozwoju;
- utrudniały wykorzystanie możliwości, jakie niosła z sobą rewolucja naukowo-techniczna i powodowały inne następstwa.

W ostateczności działania te wraz a zespołem innych poczynań spowodowały upadek systemu socjalistycznego na kontynencie europejskim. Jest rzeczą oczywistą, że system ten sam w sobie był niesprawny. Mógł jednak jeszcze trwać. To działalność Zachodu w tym m.in. wymienione formy przyspieszyły ten proces.

Współcześnie kwestie gospodarcze w ogólnej strukturze bezpieczeństwa państwa nabierają jeszcze większego znaczenia. W ostatnich latach uznanie dla gospodarczych podstaw bezpieczeństwa inaczej ekonomicznego wymiaru bezpieczeństwa wyraźnie wzrosło z następujących powodów:

- pierwszy to wyraźny spadek zagrożenia militarnego w świecie, jaki nastąpił po rozpadzie Układu Warszawskiego i Związku Radzieckiego;
- drugi związany jest z uznaniem wysokiej efektywności środków gospodarczych (wojny gospodarczej) w zimnej wojnie między blokiem państw skupionych wokół ZSRR, a państwami skupionymi wokół USA.

Spadek zagrożenia militarnym konfliktem globalnym i dotkliwość skutków zastosowania środków wojny gospodarczej spowodował, że współzależności ekonomiczne stały się ważnym (i wygodnym) narzędziem politycznego

wewnętrznej i procesów internacjonalizacji życia gospodarczego oraz wchłaniały nowinki techniczne i organizacyjne. Kraje tak postępujące korzystały z dostępu do rynków międzynarodowych czerpały korzyści z rosnącej skali wymiany międzynarodowej i zapewniły zdrowie swoim gospodarkom dzięki poddaniu się regułom międzynarodowej konkurencji. Natomiast kraje, które opierały się tym zmianom dyktowanym przez otoczenie, traciły konkurencyjność i zdolności rozwojowe, redukując tym samym własne bezpieczeństwo ekonomiczne. Takimi były kraje Europy Środkowo - Wschodniej i największe kraje Ameryki Południowej, chociaż każda z tych grup z innych względów.

Ponieważ występują problemy z określeniem zdolności potencjału gospodarczego, dlatego należy znaleźć odpowiednie narzędzia, które pozwolą go zidentyfikować i oceniać jego możliwości ocenić jego możliwości wykonania zadań wynikających z bezpieczeństwa ekonomicznego.

Dotychczasowe rozważania dają podstawę do podjęcia próby określenia istoty sfery realnej gospodarczych podstaw bezpieczeństwa państwa. Tworzą ją dostępne gospodarcze i gospodarczo - obronne zasoby i procesy materialne (fizyczne), przydatne do kształtowania bezpieczeństwa państwa w jego różnych wymiarach, niezależnie od ich bieżącego wykorzystania. Jej uporządkowany obraz pozwala na wyraźne dostrzeżenie struktury sfery realnej gospodarczych podstaw bezpieczeństwa państwa.

Sfera realna gospodarczych podstaw bezpieczeństwa występować będzie w ramach bilansów dóbr finalnych i pośrednich, powiązań kooperacyjnych, poziomu i struktury rezerw i zapasów. Mogą one uwzględniać wewnętrzne i zewnętrzne źródła zaopatrzenia i zbytu, dostępność w określonym czasie, itp. Wyrażają potrzeby bezpieczeństwa państwa lub jego segmentów o charakterze pierwotnym (surowcowo-energetycznym, żywnościowym itd.) i wtórnym (kapitału rzeczowego, odpowiedniego sprzętu i uzbrojenia, technologii oraz w zakresie infrastruktury techniczno -ekonomicznej i logistyki). W sferze realnej gospodarczych podstaw bezpieczeństwa państwa zawarta jest jej immanentna wewnętrzna sprzeczność. Wynika to z faktu, że na gruncie gospodarki typowa sprzeczność występuje pomiędzy warunkami i potrzebami bezpieczeństwa

na wpływy otoczenia. Za podstawowy warunek osiągania celów społeczno - ekonomicznych często uważa się posiadanie odpowiedniego potencjału gospodarczego, czyli zasobów tworzących sferę realną[251]. Z punktu widzenia nauk politycznych, ekonomiczny filar bezpieczeństwa państwa jest oceniany najczęściej poprzez pryzmat możliwości realizacji zadań potencjału gospodarczego. Jednak określenie, co oznacza „odpowiedni potencjał gospodarczy zapewniający bezpieczeństwo ekonomiczne i polityczne", nastręcza także trudności.

Odpowiedni potencjał gospodarczy może wyrażać się wysokim poziomem ilościowym zasobów produkcyjnych (czynników produkcji). Rozmiary tak pojętego potencjału gospodarczego mają znaczenie dla bezpieczeństwa państwa, ponieważ tworzy możliwości osiągnięcia wysokiego poziomu zaspokojenia materialnych potrzeb bezpieczeństwa. Duży potencjał oznacza także możliwość oddziaływania na otoczenie i mniejszą podatność na wpływy zewnętrzne.

Jednak samo ich posiadanie nie określa „wagi" gospodarki w układzie regionalnym i światowym ani poziomu zaspokojenia potrzeb społeczeństwa. Współcześnie istnieje wiele „dużych krajów" o dużych zasobach siły roboczej, zasobach naturalnych, ziemi uprawnej i produkcyjnych środków trwałych, ale ich udział w światowym czy regionalnym PKB jest wyraźnie mniejszy od udziału posiadanych zasobów.

Ważniejsze znaczenie ma jednak struktura i konkurencyjność gospodarki. W tym ujęciu duży potencjał oznacza wysoką sprawność i wydajność gospodarki. To kraje mające dużą przewagę mogą „dyktować warunki" uzależnionemu od siebie gospodarczo partnerowi. Gospodarka sprawna i efektywna tworzy także warunki do pełniejszego zaspokajania różnorodnych aspiracji własnego społeczeństwa.

Z punktu widzenia bezpieczeństwa ekonomicznego istotne znaczenie ma zdolność gospodarki do trwania i rozwoju w zmieniającym się otoczeniu - czyli adaptacyjność potencjału gospodarczego. Z pośród współczesnych gospodarek sukces osiągnęły tylko te, które nadążały najszybciej za zmianami struktury

---

[251]Por. A. Lubbe, *Bezpieczeństwo ekonomiczne*..., wyd. cyt., s. 64.

gospodarczej z zagranicą lub z partnerami, od których mogą płynąć zagrożenia (a w rezultacie zmniejszenie uzależnienia od wymiany zagranicznej). Wzrost bezpieczeństwa ekonomicznego wynikający ze zmniejszenia uzależnienia od zagranicy rodzi nowe zagrożenia dla rozwoju gospodarczego, ponieważ powoduje to wyższe koszty produkcji a także mniejsze możliwości rozwoju i podnoszenia poziomu życia obywateli.

Fakt istnienia zasobów nie oznacza jednak, że przeciwdziałania zadziałają automatycznie (zagrożenia zostaną samoczynnie zneutralizowane). Po to, aby gospodarka aktywnie przeciwstawiła się zagrożeniom bezpieczeństwa państwa, konieczne jest istnienie mechanizmu, który przekształci te zasoby w strumienie przeciwdziałań. W praktyce (także innych dziedzin, np. militarnej) znaczenie mają tylko te zasoby, które w określonej perspektywie (np. czasu spodziewanego konfliktu) dadzą się wykorzystać, czyli uruchomić.

Kształtowanie i utrzymanie bezpieczeństwa państwa wymaga od gospodarki narodowej, a konkretnie od gospodarczych podstaw bezpieczeństwa państwa, nadania jej cech, które by sprzyjały urzeczywistnianiu tego stanu. Sprowadzają się one do pozyskania przez GPB cech określanych jako „odporność"[252] i „żywotność"[253].

O odporności i żywotności gospodarczych podstaw bezpieczeństwa państwa stanowią:

- z jednej strony siła potencjału gospodarczego państwa - tj. jego wielkość, struktura, efektywność wykorzystania, nowoczesność;
- z drugiej strony -jego wrażliwość na wpływy zewnętrzne.

Problem odporności i żywotności gospodarczej w skali makroekonomicznej, to także problem strategii wyboru dokonywanej w warunkach dużej niepewności co do przyszłości oraz w warunkach różnych sprzeczności. Ze względu na pożądane cechy gospodarki narodowej, musi się ona orientować nie na autarkię gospodarczą tj. nie na zamykanie się we własnych granicach i skazywanie się na wytwarzanie wszystkiego lub niezbędnego w danych warunkach - często jakościowo gorszego niż

---

[252]Przez odporność gospodarczą należy rozumieć stopień uległości gospodarczej wobec podejmowanych działań wojny ekonomicznej.

[253]Przez żywotność gospodarczą należy rozumieć stopień zdolności gospodarki do przeciwstawiania się i przezwyciężania warunków związanych z wojną gospodarczą.

ogólnoekonomicznego a bezpieczeństwa polityczno – militarnego,

Bezpieczeństwo ekonomiczne nie może być porównywane z bezpieczeństwem polityczno - militarnym. Wynika to z faktu, że gospodarka w pełni bezpieczna musi być stagnacyjna, a więc niebezpieczna. Natomiast dla sfery polityczno - militarnej konieczna jest stabilizacja i pewność. Stąd też środki konieczne dla tej sfery bezpieczeństwa państwa muszą być pewne, przygotowane. Nie mogą więc podlegać bezpośrednio regułom rynkowym. Nie mają tu zastosowania wprost reguły ekonomicznej efektywności. Cele tego bezpieczeństwa, wartości i racja stanu nie mają, bowiem wymiaru ekonomicznego. Reguły efektywności w tej sferze wyznaczone są, bowiem pewnym poziomem wystarczalności, a efektywność ekonomiczna będzie odnoszona do takich wariantów użycia środków, które minimalizować będą nakłady na osiągnięcie danego celu politycznego lub militarnego. Zastosowanie w odniesieniu do czystych dóbr publicznych mają kryteria polityczne a nie ekonomiczne. Poddanie regułom rynkowym (tj. konkurencji i niestabilności) sektorów gospodarki służących bezpieczeństwu może pozbawić je zdolności do dostarczania koniecznych środków a nawet doprowadzić do likwidacji istotnych z punktu widzenia bezpieczeństwa segmentów, np. wytwarzających i dostarczających narzędzia bezpieczeństwa polityczno - militarnego.

Sprzeczność pomiędzy bezpieczeństwem polityczno - militarnym a ekonomicznym polega nie tylko na różnych sposobach ich realizacji (relacje: stabilność <==> konkurencja). Odpowiednie środki na maksymalizowanie bezpieczeństwa militarnego czy politycznego zabierają środki na konsumpcję lub/i na rozwój/inwestycje. I odwrotnie: np. maksymalizowanie konsumpcji dóbr prywatnych może ograniczyć lub nawet uniemożliwić dostarczanie dóbr publicznych, w tym bezpieczeństwa narodowego.

Kolejnym przykładem jest sprzeczność pomiędzy koniecznością strukturalnego zaangażowania w międzynarodową wymianę gospodarczą, a dążeniem do uniezależnienia się od oddziaływania zaburzeń występujących na rynkach zewnętrznych na wewnętrzną sytuację gospodarczą. Kraj znajdujący się w sytuacji zagrożenia konfliktem gospodarczym lub militarnym może zwiększyć swoje bezpieczeństwo ekonomiczne poprzez ograniczenie swojej wymiany

termin ten dotyczy kluczowej sprawy, jaką jest sposób działania, czy też model funkcjonowania (zarządzania). W szerokim ujęciu chodzi tu o system kierowania tymi procesami.

Można wyróżnić - podobnie jak to ma miejsce w całej gospodarce - sferę regulacji (funkcjonalną) i sferę realną. Obejmują one odpowiednio procesy informacyjno-decyzyjne i materialne. Każda z tych sfer posiada własną strukturę organizacyjną, na którą składa się system podmiotowy i system powiązań między tymi podmiotami. Pierwsza z tych sfer prowadzi działalność regulacyjną, czyli oddziałuje na podmioty różnego typu narzędziami w celu wywołania pożądanego stanu lub procesu w gospodarce. Natomiast druga - co wskazano we wcześniejszych rozważaniach - prowadzi działalność głównie w sferze realnej, dostarczając dóbr i usług przydatnych do użycia i tworzących gospodarcze podstawy bezpieczeństwa państwa.

Istotą sfery funkcjonalnej bezpieczeństwa państwa jest to, że zadania dla gospodarki ustalane są przez centralne organy władzy ustawodawczej i wykonawczej państwa, a realizują je wszystkie podmioty administracji państwowej, samorządowej i gospodarczej. Skupiając się na sferze regulacji tych procesów należy zwrócić uwagę na ich zhierarchizowane struktury, przy występowaniu silnych i wzajemnych powiązań. Ogólnie da się wydzielić trzy główne organy państwa, które realizują różnorodne funkcje, są to:

- organy centralne, które podejmują decyzje, określają cele i dokonują strategicznych wyborów;
- organy sztabowe, które przetwarzają informacje i dokonują projekcji zjawiska;
- organy obserwacyjno-kontrolne, które gromadzą i porządkują informacje oraz dokonują audytu zgodnie z zaleceniami odpowiednich organów ustawodawczych.

Zgodnie z tak ujętymi funkcjami, najwyższym i najważniejszym szczeblem w sprawach bezpieczeństwa narodowego są:

- władza ustawodawcza, urząd prezydenta sprawujący ogólne kierownictwo w dziedzinie bezpieczeństwa narodowego i ponoszący główną odpowiedzialność za jego stan;

gdzie indziej, ale na kompromis gospodarczy polegający na wyznaczaniu pewnego stanu samowystarczalności, uznanego za wystarczający dla zapewnienia bezpieczeństwa państwa. Istotny wpływ na żywotność gospodarczych podstaw bezpieczeństwa danego kraju ma jej struktura. Im będzie ona bardziej nowoczesną, tym istotniejsza będzie jej rola korygująca. Im natomiast będzie ona bardziej przestarzała, tym mniej będzie ona odporną i żywotną. Oceny w tym względzie zawsze są i będą wypadkową poziomu gospodarczego danego kraju i krajów stanowiących zagrożenie dla niego. Problem odporności i żywotności polega na:

- z jednej strony na przygotowaniu gospodarki do rozwoju poprzez:
  - dywersyfikację gospodarki narodowej;
  - podjęcie działań zmierzających do ukształtowania bezpiecznych międzynarodowych stosunków ekonomicznych,
- z drugiej zaś strony na przygotowaniu gospodarki do:
  - przetrwania i przezwyciężenia destruktywnych działań przeciwnika;
  - odtworzenia naruszonych podstaw działania gospodarki.

Cechą charakterystyczną odporności i żywotności gospodarczych podstaw bezpieczeństwa, jako warunku kształtowania i utrzymania bezpieczeństwa państwa jest to, że poddać go weryfikacji mogą nie tylko przedsięwzięcia wojny ekonomicznej, lecz także trudności ekonomiczne i finansowe kraju, a nawet klęski ekologiczne czy żywiołowe jak i udział w międzynarodowych misjach stabilizacyjnych czy pokojowych.

3.2.2. Formuła sfery funkcjonalnej modelu kształtowania bezpieczeństwa państwa

Formuła sfery funkcjonalnej (regulacyjnej) wymaga przypomnienia podstawowych wiadomości związanych z jej istotą, wskazania zasadniczych organów państwa tej sfery, określenia kompetencji organów władzy i administracji publicznej w tym zakresie oraz skupienia wagi na możliwych narzędziach i instrumentach oddziaływania podmiotów sfery regulacji na kształtowanie systemu gospodarczych podstaw bezpieczeństwa państwa, a także omówienia współdziałania i roli Sojuszu NATO oraz Unii Europejskiej w kształtowaniu tych procesów. W literaturze przedmiotu, że regulacja (funkcjonowanie) to ujmowanie czegoś w pewne przepisy, normy, porządkowanie, normowanie. Wynika z tego, że

centralnym i sztabowym. Gromadzone i przetwarzane dane są podstawą wykonywania funkcji kontrolnych w sensie porównania stanu rzeczywistego ze stanem pożądanym czy też i określonym.

Przez system kierowania gospodarką obronną rozumie się wszystkie organy centralne w państwie odpowiadające za realizację zadań gospodarczo-obronnych, powiązane informacyjnie i pozostające w ustanowionych prawnie relacjach kompetencyjnych, wraz z aparatem wykonawczym (administracyjnym, sztabowym, organizacyjnym) oraz konieczną infrastrukturą. System ten działa w gospodarce pokojowej i jest przygotowany do odpowiedniego rozwinięcia na czas zewnętrznego zagrożenia bezpieczeństwa państwa i wojny. Zadania kierowania gospodarką obronną uwzględniać jednak powinny właściwości jej funkcjonowania w dwóch innych stanach gotowości obronnej państwa: okresu pokoju i stanach szczególnych zagrożeń państwa.

Kierowanie obronnością państwa jest to celowa działalność wszystkich organów władzy i administracji państwowej, samorządowej i gospodarczej zmierzająca do utrzymania określonego potencjału obronnego w czasie pokoju oraz zapewniająca prawną realizację tych zadań w okresie zagrożenia i wojny. Kierowanie, rozumiane jako funkcja systemu obronności państwa, jest rodzajem więzi informacyjnych i decyzyjnych, jakie zachodzą między określonymi elementami systemu obronności.

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

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

- □ urząd premiera i rząd odpowiedzialny za realizację zadań w zakresie bezpieczeństwa państwa wraz z terenowymi organami administracji państwowej.

Do kompetencji tych organów należy określanie celów w zakresie bezpieczeństwa państwa wraz z wyborem sposobów ich osiągania w ramach posiadanych kompetencji. Ponadto posiadają uprawnienia do inicjatywy ustawodawczej jak również odpowiednie narzędzia rynkowe i administracyjne, które stymuluj ą podległe podmioty w pożądanym obszarze i kierunku. Oznacza to, że tworzą one określoną politykę państwa.

Obszarem kompetencji regulacyjnych tych ogniw jest całość państwa i jego stosunków z otoczeniem zewnętrznym, chociaż różnie rozkładają się akcenty w zakresie kształtowania bezpieczeństwa. Należy podkreślić, że stosowanie narzędzi regulacji powoduje odpowiednie zmiany, zarówno w sferze realnej jak i w sferze regulacji. Te skutki powinny być zauważone przez organy obserwacyjne dające początek nowemu cyklowi sprawnego kierowania gospodarczymi podstawami bezpieczeństwa państwa.

Na szczeblu centralnym, oprócz tego istnieją instytucje i urzędy wykonujące funkcje sztabowe na podstawie, których podejmowane są decyzje stanowiące w sprawach bezpieczeństwa. Do ich kompetencji należy: analiza i ocena gospodarczych podstaw bezpieczeństwa państwa; przygotowanie wariantów skutecznego przeciwdziałania destrukcyjnemu oddziaływaniu na potencjał gospodarczy; przewidywanie skutków dla bezpieczeństwa państwa różnego rodzaju decyzji społeczno-gospodarczych. Takim typowym organem sztabowym administracji w odniesieniu do gospodarki narodowej jest Rządowe Centrum Studiów Strategicznych.

Mając na uwadze organy obserwacyjno-kontrolne należy wymienić przede wszystkim takie instytucje działające w naszym kraju jak: Główny Urząd Statystyczny; Najwyższą Izbę Kontroli; agencje wywiadu, agencję bezpieczeństwa wewnętrznego oraz dyplomację. Organy te zgodnie z przypisaną im rolą zbierają informacje o wszystkich elementach wywierających wpływ na stan bezpieczeństwa kraju, toczących się w nich procesach i relacjach. Zebrane informacje są odpowiednio porządkowane, agregowane oraz przedkładane odpowiednim organom

Z tego wynikają obowiązki i uprawnienia oraz określone miejsce i rola poszczególnych organów w całym systemie kierowania obronnością państwa. Sprawy te są ogólnie uregulowane w Konstytucji RP. Bardziej szczegółowe uregulowania znajdują się w ustawach dotyczących urzędów państwowych, w tym również w ustawie o urzędzie ministra obrony narodowej, aktach prawnych uchwalanych przez Radę Ministrów oraz w dotychczas obowiązujących uchwałach Komitetu Obrony Kraju. Zgodnie z postanowieniami zawartymi w wyżej wymienionych aktach poszczególne organa sprawują określone funkcje w kierowaniu obronnością Rzeczpospolitej Polskiej w czasie pokoju. Szczegółowe zadania dla poszczególnych pozamilitarnych ogniw systemu obronnego państwa ustalają właściwe organy władzy i administracji państwowej drogą aktów prawnych.

Parlament jest organem stanowiącym prawo, w tym również prawo dotyczące bezpieczeństwa i obronności państwa. Parlament jest dwuizbowym organem władzy ustawodawczej tj. Sejmu Rzeczpospolitej Polskiej i Senatu Rzeczpospolitej Polskiej. Sejm Rzeczpospolitej Polskiej, uchwala każdego roku wysokość środków na bezpieczeństwo i obronę państwa w ramach ustawy budżetowej, jak również inne regulacje ustawowe dotyczące problematyki bezpieczeństwa i obronności państwa oraz kontroluje ich stosowanie. Senat Rzeczpospolitej Polskiej dzieli z Sejmem wykonywanie funkcji ustawodawczej, włącznie z uchwaleniem wysokości wydatków na bezpieczeństwo i obronę państwa. Parlament w głównej mierze, decyduje o wielkości potencjału obronnego państwa utrzymywanego w czasie pokoju. Wszelkie decyzje dotyczące bezpieczeństwa i obronności państwa powodują określone skutki głównie ekonomiczne i gospodarcze, a nieraz także polityczne i inne. Stąd, w tych sprawach, szczególnie w czasie pokoju ściśle przestrzega się przyjętych procedur legislacyjnych.

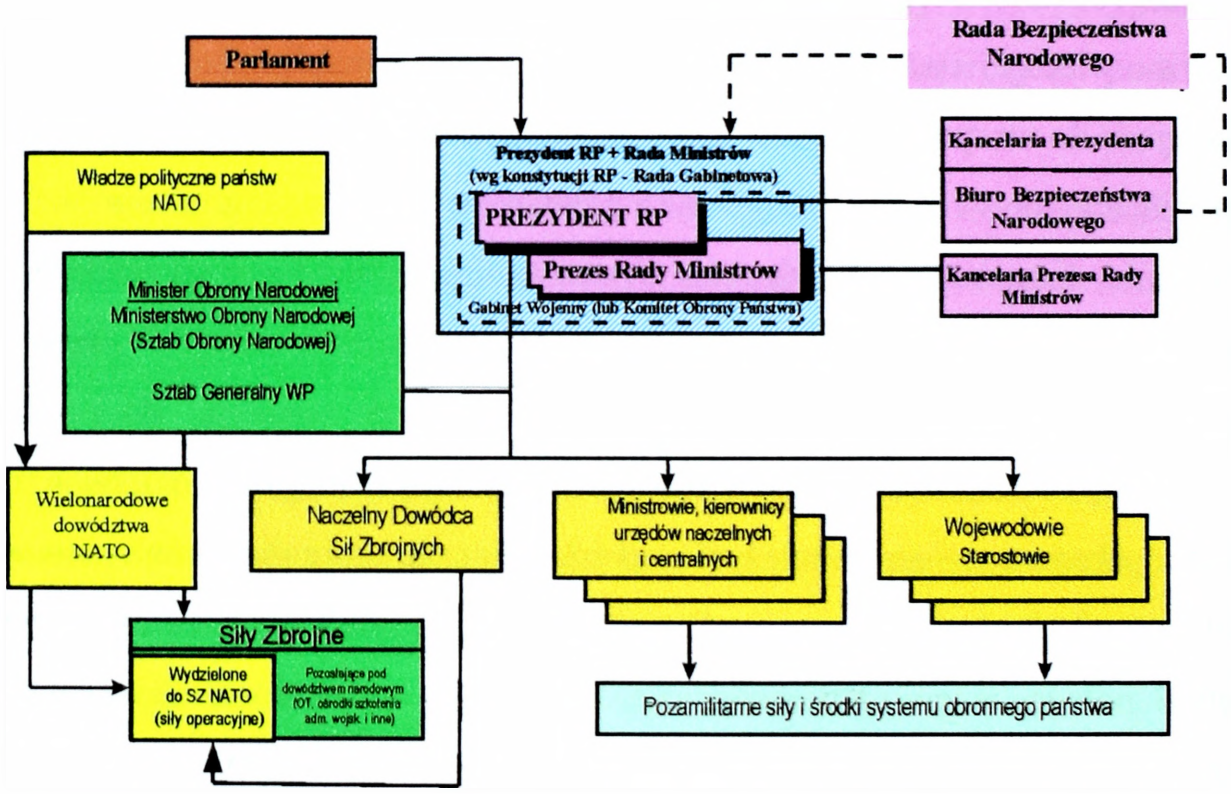
Projekty ustaw dotycząca obronności (mogą je wnosić tylko organa posiadające prawo inicjatywy ustawodawczej) niezależnie od opinii Komisji Sejmowej i Senackiej zawsze są opiniowane przez Radę Ministrów. Rząd każdorazowo, w takich sprawach, obowiązany jest przedstawić parlamentowi skutki, jakie może spowodować przyjęcie określonej ustawy. Dopiero po

odpowiedzialne za bezpieczeństwo kraju i brały czynny udział w procesie kierowania jego obronnością[254].

System kierowania państwem w systemie obronności państwa, opiera się w zasadzie na liniowej strukturze. Polega na tym, że przy każdej osobie funkcyjnej (decydencie) działa komórka organizacyjna (lub zespół) wykonująca czynności o charakterze przygotowawczym i organizacyjnym. Nie zwalnia to jednak osoby funkcyjnej (decydenta) od osobistego podejmowania decyzji i od konsekwencji z tego wynikających. Ogólne powiązania informacyjno - decyzyjne pomiędzy najwyższymi organami władzy ustawodawczej i wykonawczej oraz administracji państwa, jak również podsystemu niemilitarnego z jego siłami i środkami, a także militarnego z uwzględnieniem obecności w NATO (Schemat 3.3.).

Schemat 3.3.

Kierowanie obronnością państwa (Wariant)



Źródło: Opracowanie własne na podstawie materiałów Sz. Gen. WP.

W kierowaniu obronnością obowiązują podobne zasady jak w każdym rodzaju kierowania. Szczególnie ważna, ze względu na omawiany problem, jest zasada precyzyjnego określenia kompetencji organów w zakresie kierowania.

---

[254]Por. B. Tarasiuk, A. Czarniecki, W. Suwiński, *Kierowanie obronnością państwa w czasie pokoju, kryzysu i wojny*. AON, Warszawa 1998, s. 34.

i przedstawione zadania powinna spełniać Rada Bezpieczeństwa Narodowego, która ma zstąpić Komitet Obrony Kraju. Obok Komitetu Obrony Kraju w proces przygotowań obronnych jest zaangażowana Rada Ministrów, głównie w sferze wydawania przepisów wykonawczych regulujących powinności podmiotów gospodarczych oraz obywateli. Należy tu zaznaczyć, że jest to sprzeczne z nową Konstytucją, która zadania te powierza Radzie Ministrów.

Rada Ministrów jest głównym organem wykonawczym w dziedzinie działalności państwa. Realizuje ona politykę wewnętrzną i zagraniczną Rzeczypospolitej Polskiej. Do jej szczególnych obowiązków należy zapewnienie wykonania ustaw, w tym również ustaw dotyczących obronności, zapewnienie bezpieczeństwa zewnętrznego i wewnętrznego państwa oraz porządku publicznego, sprawowanie ogólnego kierownictwa w dziedzinie obronności kraju, zawieranie umów międzynarodowych, wymagających ratyfikacji oraz zatwierdzenia i wypowiadania innych umów międzynarodowych. Rada Ministrów, poprzez ministrów i wojewodów, kieruje realizacją zadań obronnych, koordynuje, kontroluje i nadzoruje prace wszystkich organów administracji rządowej. Przysługuje jej prawo inicjatywy ustawodawczej (Załącznik 1.).

Prezes Rady Ministrów kieruje pracami Rady Ministrów, kontroluje i koordynuje prace członków Rady Ministrów, jest zwierzchnikiem służbowym pracowników administracji rządowej i korpusu służby cywilnej, posiada uprawnienia występowania z wnioskiem do Rady Ministrów o uchylenie rozporządzenia lub zarządzenia ministra. Wewnętrznym organem rządu w sprawach bezpieczeństwa i obronności państwa jest Komitet Spraw Obronnych Rady Ministrów (KSORM). Do jego głównych zadań należy koordynowanie działań organów administracji państwowej w zakresie obronności w celu przygotowania stosownych projektów i aktów normatywnych. Konkretne sprawy po rozpatrzeniu przez KSORM kierowane są do Rady Ministrów lub właściwego ministra, gdzie podejmuje się stosowne decyzje.

Ministrowie (kierownicy urzędów centralnych) kierują określonym działami administracji rządowej, odpowiedzialni są za realizację zadań obronnych przez podległe i nadzorowane jednostki organizacyjne, w ramach powszechnego obowiązku obrony. W strukturze organizacyjnej w bezpośrednio podległych im

zaopiniowaniu projektu ustawy przez rząd, dalsze procedury legislacyjne są identyczne jak dla innych ustaw uchwalanych przez Parlament. Specjalistycznymi organami parlamentu w sprawach obronności są Senacka i Sejmowa Komisja Obrony Narodowej. Zgodnie z postanowieniami określonymi w Konstytucji RP Sejm decyduje w imieniu RP o stanie wojny i o zawarciu pokoju. Natomiast parlament bezpośrednio w kierowaniu obronnością nie uczestniczy, gdyż nie posiada on jak i jego komisje uprawnień wykonawczych.

Prezydent Rzeczypospolitej Polskiej, zgodnie z zapisami Konstytucji RP, stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium. Jako reprezentant państwa w stosunkach zewnętrznych ratyfikuje i wypowiada umowy międzynarodowe, o czym ma obowiązek powiadomić Sejm i Senat. Jest on najwyższym zwierzchnikiem Sił Zbrojnych Rzeczypospolitej Polskiej. W sprawach szczególnej wagi może zwołać Radę Gabinetową (jest to Rada Ministrów obradująca pod przewodnictwem Prezydenta RP), z tego uprawnienia nie wynikają dla Prezydenta RP dodatkowe kompetencje. Radzie Gabinetowej nie przysługują kompetencje Rady Ministrów, chociaż jej postanowienia mogą mieć istotny wpływ na decyzje Rady Ministrów.

Prezydent uczestniczy w ustanawianiu prawa, w tym również prawa w ziedzinie obronności (posiada on prawo inicjatywy ustawodawczej, prawo veta i podpisuje ustawy). Organem doradczym Prezydenta RP w zakresie wewnętrznego i zewnętrznego bezpieczeństwa państwa jest Rada Bezpieczeństwa Narodowego. O jej składzie i trybie powoływania decyduje Prezydent RP.

Komitet Obrony Kraju, zgodnie z dotychczas obowiązującą ustawą o powszechnym obowiązku obrony, jest organem właściwym w sprawach obronności i bezpieczeństwa państwa, posiadającym bardzo szerokie kompetencje w zarządzaniu i administrowaniu obronnością. W świetle obowiązujących ustaleń prawnych organem organizacyjnym, nadzorującym i kontrolującym proces przygotowań obronnych jest nadal Komitet Obrony Kraju. W toku sprawowania swoich funkcji Komitet wydał szereg przepisów (uchwał i wytycznych) określających zakres przygotowań obronnych i zasady ich prowadzenia, a także ustalił bezpośrednich przedsięwzięć obronnych i zasady ich prowadzenia, a także ustalił bezpośrednich wykonawców przedsięwzięć obronnych. Funkcję

obronnością państwa zależy od jednoznaczności zakresu obowiązków i odpowiedzialności jego poszczególnych ogniw i osób funkcyjnych. Do realizacji zadań w dziedzinie bezpieczeństwa narodowego, kierowania systemem obronnym, w tym jego podsystemem niemilitarnym, państwo przeznacza różne siły i środki, które to ujęte w odpowiednią strukturę funkcjonalną składają się na systemy bezpieczeństwa i obronny kraju.

Problemem o zasadniczym znaczeniu w procesie kierowania jest walka o czas. Najkorzystniejsza decyzja umożliwiająca, w warunkach określonych stanów nadzwyczajnych np. zagrożeń, wykorzystanie sił i środków powinna wynikać nie tylko z intelektualnych predyspozycji organów kierowniczych, ich doświadczenia i wiedzy, ale przede wszystkim powinna opierać się na rzeczowych kalkulacjach i ocenach prawdopodobnych rezultatów. Szybkość przekazywania informacji od organów kierowniczych do wykonawców oraz stopień ich wiarygodności są podstawowymi czynnikami, które decydować będą o efektywności podjętych działań i przedsięwzięć. Rola informacji w kierowaniu podczas różnych zagrożeń obszaru kraju nieprzerwanie ulega istotnemu przewartościowaniu, a rozwijające się systemy łączności stają się jednym z podstawowych atrybutów stanowiących wkład w przyszłe społeczeństwo informacyjne.

Całokształt kierowania problematyką niemilitarną jest procesem decyzyjno - informacyjnym. System informacyjny sprzęga w jedną spójną całość wszystkie pozostałe elementy składowe systemu kierowania obroną państwa. Obejmuje on siły i środki zdobywania, przetwarzania i przesyłania informacji we wszystkich elementach systemu obronnego państwa w tym i podsystemu niemilitarnego. Doświadczenia ostatnich wojen i konfliktów zbrojnych potwierdzają, że o ile dawniej głównymi obiektami ataku były przede wszystkim systemy rażenia, to współcześnie coraz bardziej stają się nimi systemy kierowania, dowodzenia i łączności. System kierowania obejmuje, więc swoim zasięgiem wzajemnie powiązane informacyjnie organa kierowania, techniczne środki kierowania oraz stanowiska kierowania. Infrastrukturę techniczną systemu kierowania obronnością kraju stanowią stanowiska pracy osób funkcyjnych organów kierowania, rozmieszczone w dotychczasowych miejscach pracy, wyposażone w odpowiednie

urzędach występują specjalistyczne komórki ds. obronności, tworzą je departamenty lub biura spraw obronnych. Poszczególne resorty w swojej strukturze posiadają terenowe organa administracji specjalnej. W strukturze organów administracji specjalnej są etatowi pracownicy ds. obronnych.

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

Obecnie w sytuacji, członkostwa w NATO, wydzielone siły operacyjne podlegają pod wielonarodowe dowództwo Paktu Północnoatlantyckiego, natomiast pozostałymi siłami, poprzez dowództwa rodzajów sił zbrojnych, dowodzi Minister Obrony Narodowej.

Wojewoda (starosta) jako przedstawiciel Rady Ministrów w województwie (powiecie) kieruje realizacją zadań obronnych na obszarze województwa (powiatu). Do jego obowiązków należy:

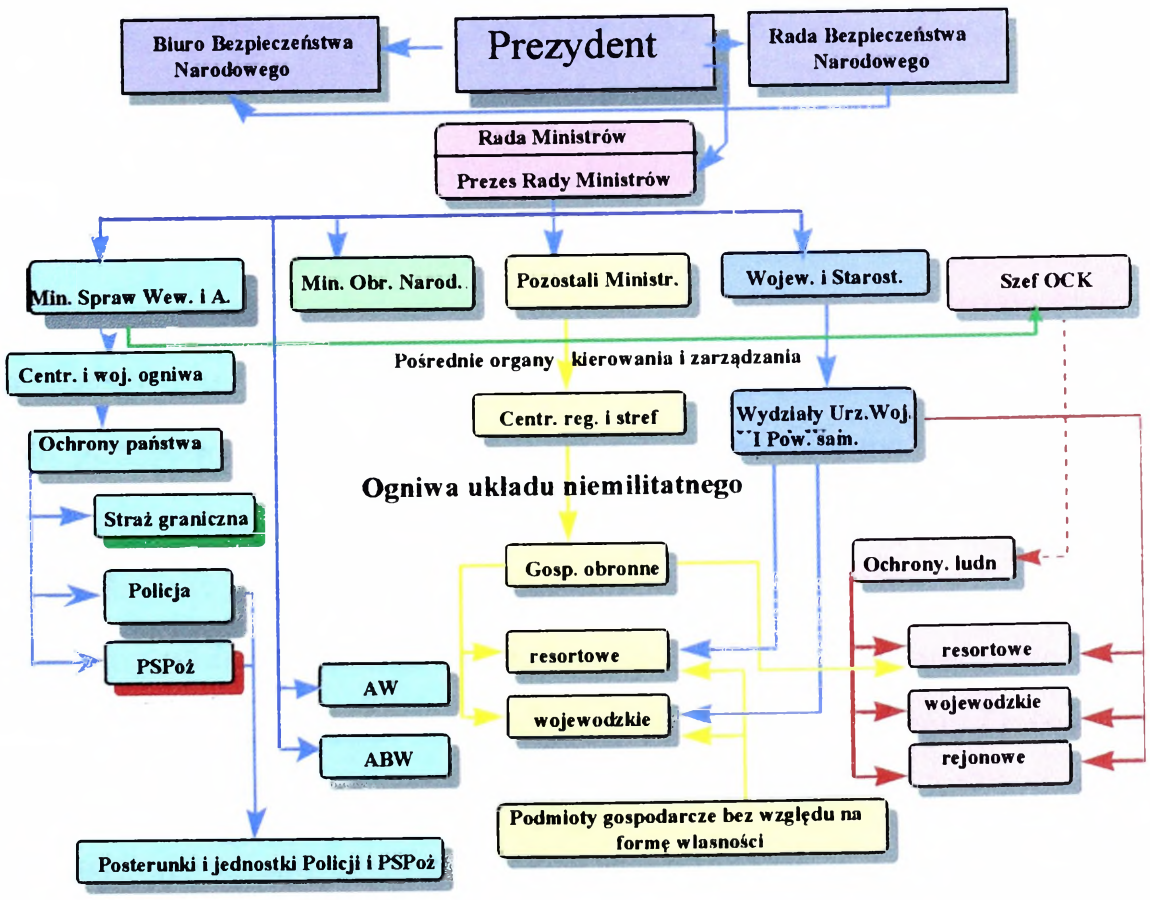
- koordynowanie i kontrolowanie działalności administracji rządowej działającej na obszarze województwa w zakresie zgodności z polityką rządu;
- zapewnienie współdziałania jednostek organizacyjnych działających na obszarze województwa w zakresie porządku publicznego, a także zapobiegania klęskom żywiołowym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

Wojewodzie (staroście) jako szefowi Obrony Cywilnej Województwa (powiatu) bezpośrednio podporządkowany jest Wydział Zarządzania Kryzysowego, Ochrony Ludności i Spraw Obronnych. Sprawność systemu kierowania

utrzymywanego w czasie pokoju. Prawidłowe spełnianie tych funkcji warunkuje stan prawny w państwie, precyzyjny podział kompetencji oraz przydzielone na obronność środki finansowe. Podsystem niemilitarny swoim działaniem obejmuje wszystkie dziedziny związane z gospodarką obronną państwa[257]. Miejsce i rolę poszczególnych elementów niemilitarnego systemu wyznaczają spełniane przez nich zadania na rzecz sił zbrojnych i obronności kraju. W studiowanej literaturze przedmiotu podaje się, że do centralnych organów bezpośrednio uczestniczących w procesie kierowania podsystemem niemilitarnym wliczane są elementy następujących jednostek, komórek organizacyjnych: Biura Bezpieczeństwa Narodowego, Rady Bezpieczeństwa Narodowego, Rady Ministrów, Komitetu Spraw Obronnych Rady Ministrów itp.

Schemat 3.4.

Struktura niemilitarnych ogniw kierowania



Źródło: Opracowanie własne na podstawie materiałów Sz. Gen. WP.

---

[257]Por.L. Sawicki, *Przygotowanie organizacyjno-mobilizacyjne układu pozamilitarnego systemu obronnego państwa,* AON. Warszawa 1998, s. 17.

techniczne środki, w tym głównie środki łączności i informatyki, tworzące stanowiska kierowania lub dowodzenia odpowiedniego szczebla systemu.

W czasie pokoju, stanowiska kierowania są rozmieszczone w stałych miejscach pracy. Za przygotowanie stanowisk kierowania prezydenta, premiera, Agencji Wywiadu i Agencji Bezpieczeństwa Wewnętrznego oraz innych stanowisk kierowania w podsystemie niemilitarnym odpowiada minister spraw wewnętrznych i administracji. Natomiast za stanowiska kierowania województw odpowiadają wojewodowie. Każde ze stanowisk powinno mieć stworzone warunki do pracy, odpowiednio zapewnioną łączność, a także zabezpieczenie bytowe i materiałowo - techniczne. Stanowiska kierowania określonych szczebli - w zależności od potrzeb ich osób funkcyjnych - wyposażone są w urządzenia końcowe łączności i informatyki o różnych możliwościach świadczonych usług.

W czasie pokoju w procesie kierowania uczestniczą naczelne oraz centralne organa władzy i administracji rządowej, wojewódzkie, powiatowe (regionalne) organa administracji rządowej, organa samorządu terytorialnego, kierownicy podmiotów gospodarczych, instytucji i organizacji zobowiązanych do realizacji zadań obronnych, a także organa dowodzenia sił zbrojnych funkcjonujące w strukturach czasu pokoju. Wyjątkową odpowiedzialnością obciążone są naczelne organa polityczne.

Głównym organem zarządzającym i wykonawczym podsystemu niemilitarnego jest rząd RP i Rada Ministrów (Schemat 3.4.). Szczeblem realizacyjnym w tym systemie są ministrowie, wojewodowie, starostowie i samorząd terytorialny[255]. Szef Obrony Cywilnej Kraju jest powoływany przez Prezesa Rady Ministrów na wniosek ministra spraw wewnętrznych i administracji, który swoją decyzją[256] powołał i określił strukturę organizacyjną Urzędu Zarządzania Kryzysowego i Ochrony Ludności. Do ich kompetencji należy ocena potencjalnych zagrożeń oraz określenie środków zaradczych stosownie do zagrożeń i możliwości państwa. Ściśle z tym związany jest wybór odpowiedniej strategii działania, co w konsekwencji wiąże się z wielkością potencjału obronnego państwa

---

[255]Por. R. Kulczycki, E. Piedziuk, J. Wojnarowski, *Model systemu obronnego państwa.* AON, Warszawa 1994, s.21.

[256]Decyzja nr 2 ministra spraw wewnętrznych i administracji z 4 stycznia 1997r.

techniczne umożliwiające w sposób tajny uzyskiwanie informacji oraz utrwalanie śladów i dowodów.

Struktura organizacyjna policji jest dostosowana do obowiązującego podziału administracyjnego kraju. Centralnym organem administracji państwowej, właściwym w sprawach ochrony bezpieczeństwa obywateli oraz utrzymania bezpieczeństwa i porządku publicznego, jest Komendant Główny Policji, podległy bezpośrednio Ministrowi Spraw Wewnętrznych i Administracji. Natomiast terenowymi organami są: - komendanci wojewódzcy Policji; - komendanci powiatowi Policji; - komendanci komisariatów Policji. Podległe Komendantowi Głównemu pododdziały prewencji, realizują zadania policyjne na korzyść określonych województw i pozostają w dyspozycji komendantów wojewódzkich, jak również wszystkich ośrodków szkolenia Policji.

Znaczne siły i środki Policji są angażowane do walki ze zorganizowaną przestępczością głównie o charakterze terrorystycznym i mafijnym. W wypadku zaistnienia kryzysu lub wybuchu wojny Policja, działając w obecnie funkcjonującym układzie strukturalnym, z uwagi na rozległość i różnorodność zadań, może nie wywiązać się z nałożonych na nią obowiązków.

Intensywność ruchu granicznego oraz tendencja do ułatwień w poruszaniu się przez terytoria poszczególnych państw spowodowały zagrożenia występowaniem sytuacji niebezpiecznych w strefach nadgranicznych oraz wewnątrz państwa. Szczupłe siły Straży Granicznej, odczuwające braki w uzbrojeniu i wyposażeniu, nie zapewniają już obecnie skuteczności przeciwdziałania przestępczości przygranicznej. W wypadku zaistnienia kryzysu lub wojny Straż Graniczna w strefach przygranicznych z państwami nie będącymi stronami konfliktu nie jest w stanie przy obecnym jej kształcie strukturalno - funkcjonalnym poradzić sobie z realizacją ustawowych zadań.

Zadania obronne spoczywają na wszystkich ogniwach systemu obronnego państwa, jak również na organizacjach społecznych, politycznych i gospodarczych. Należy dodać, że stan i możliwości układu niemilitarnego uzależnione są w głównej mierze od wielkości potencjału gospodarczo-obronnego, przygotowania kierowniczej kadry oraz jej przekonania, co do konieczności świadczeń na rzecz obronności.

Można stwierdzić, że kierowanie elementami podsystemu niemilitarnego ograniczone jest:

- od góry - organami naczelnej władzy państwowej: ustawodawczej, wykonawczej, sądowniczej;
- od dołu - przedstawicielami władzy wykonawczej na poziomie: poszczególnych ministerstw, dowódcy sił zbrojnych, wojewodów, starostów, burmistrzów, kierowników ważniejszych nadzorowanych jednostek organizacyjnych wykonujących zadania obronne.

Skuteczność kierowania podsystemem niemilitarnym a zwłaszcza jego sprawność zależy, w dużej mierze od stopnia przygotowania infrastruktury technicznej stanowisk kierowania oraz od posiadanych środków i podsystemów łączności, które zapewniają powiązanie wszystkich elementów podsystemu niemilitarnego.

Przemiany ustrojowe, jakie dokonały się w Polsce po 1989 roku, spowodowały wzrost zagrożeń wewnętrznych, w tym wzrostu przestępczości. Obecnie funkcjonujące struktury resortu spraw wewnętrznych i administracji (tworzące ogniwa ochrony państwa) nie zawsze zapewniają utrzymanie porządku publicznego i wewnętrznego. W przypadku kryzysu lub wojny sytuacja ta może ulec dramatycznemu zaostrzeniu.

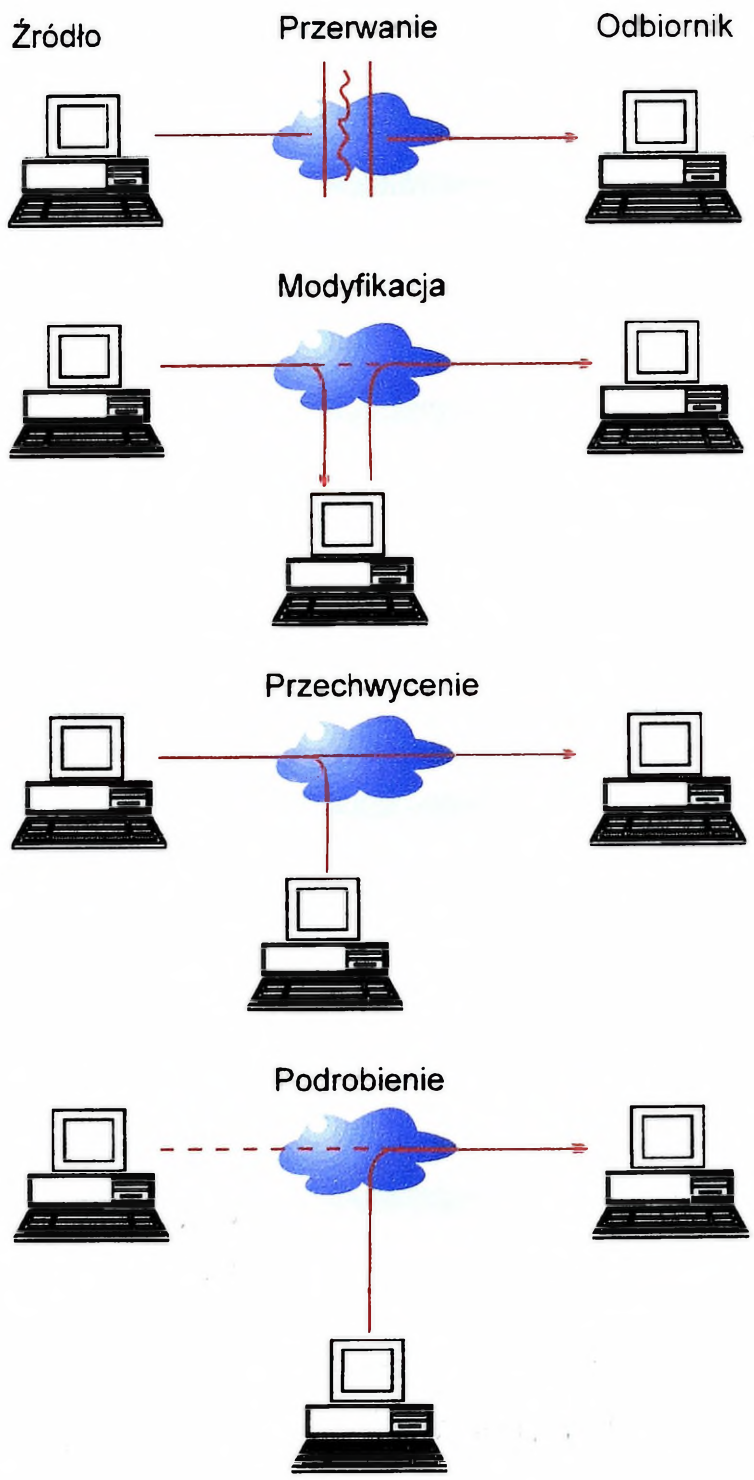
Należy zauważyć, że nałożony na ABW ustawowy obowiązek ochrony bezpieczeństwa państwa nie jest możliwy do realizacji jedynie przez tę instytucję. Urząd głównie pozyskuje informacje o zagrożeniach: sam im przeciwdziała tylko częściowo, a większość informacji służy do podejmowania właściwych działań przez inne organa państwa: polityczne, gospodarcze, wojskowe, ekologiczne, sprawiedliwości i bezpieczeństwa wewnętrznego.

Funkcjonariusze ABW w celu rozpoznania, zapobiegania i wykrywania przestępstw powinni wykonywać czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze, a w celu zapobieżenia bądź wykrycia zbrodni godzących w porządek konstytucyjny, bezpieczeństwo i obronność państwa, a także zbrodni ściganych na mocy umów i porozumień międzynarodowych funkcjonariusze ci powinni mieć prawo kontrolować korespondencję oraz stosować różne środki

Atak pasywny to szeroko rozumiany podsłuch lub podgląd w celu zdobycia informacji niejawnej i/lub analiza ruchu w sieci dla zlokalizowania ważnych obiektów i stanowisk kierowania. Jest on najczęściej etapem przygotowawczym do wykonania ataku aktywnego na system.

Schemat 3.6.

Ataki na bezpieczeństwo w sieciach teleinformatycznych



Atak aktywny dąży do modyfikowania strumienia informacji lub tworzenia fałszywych informacji. W działaniach tych mieszczą się: podszywanie się pod osobę uprawnioną i blokowanie działania. Rezultatem skutecznego ataku na system

3.2.3. Systemy osobowego i kryptograficznego zabezpieczenia infrastruktury telekomunikacyjnej w modelu kształtowania bezpieczeństwa ekonomicznego państwa

W ostatnich latach nastąpił w Polsce gwałtowny rozwój infrastruktury telekomunikacyjnej. Sytuacja ta umożliwiła szerokie wykorzystywanie w procesach zarządzania i kierowania nowoczesnych technik przekazu i przetwarzania informacji. Znaczenie obiegu informacji w instytucji państwowej, przedsiębiorstwie, organizacji militarnej, czy też koncernie działającym w sieci teleinformatycznej, porównać można do znaczenia krwioobiegu w organizmie ludzkim. Każda organizacja dysponująca informacjami, wykorzystuje do ich przechowywania, przetwarzania i przesyłania systemy teleinformatyczne (Schemat 3.5.). Pojawiło się szereg niebezpieczeństw, spowodowanych przejęciem kontroli nad informacją nie tylko przez nieuprawnione działanie w sieci teleinformatycznej jej użytkowników lub pojedyncze osoby, ale również przez zorganizowane grupy o nastawieniu antyspołecznym i antypaństwowym. Potencjalne możliwości nieuprawnionego działania w sieci teleinformatycznej jej użytkowników lub osób nie będących jej użytkownikami nazywane są zagrożeniami. Zagrożenia mogą występować przypadkowo lub być skutkiem działania celowego. Działania celowe, nazywane atakiem na system (Schemat 3.6.), mogą być realizowane bez aktywnego oddziaływania - atak pasywny lub z oddziaływaniem na system atak aktywny.

Schemat 3.5.

Uproszczony schemat ochrony danych w sieci teleinformatycznej



Atak pasywny polega na podsłuchiwaniu (szeroko pojętym) i monitorowaniu przesyłanych informacji. Celem ataku pasywnego może być dążenie do ujawnienia treści wiadomości lub uzyskanie informacji o samym ruchu informacji.

informacji niejawnych, a działając w sposób aktywny może spowodować zniszczenie zasobów informacji i zdezorganizowanie funkcjonowania sieci.

Funkcje zaimplementowane w urządzeniach utajniających powinny realizować wiele różnych zadań kryptograficznych. Dla poprawnej pracy tych urządzeń niezbędne jest dostarczenie określonej ilości danych kluczowych, ich wymiana w określonym czasie i bieżący nadzór nad eksploatacją. Funkcje te możliwe są do zrealizowania przez odpowiednie zaprojektowanie i wykonanie urządzeń utajniających.

Specyfika eksploatacji sieci teleinformatycznej powoduje występowanie szeregu czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji. Poznanie ich pozwala prawidłowo projektować strukturę systemu, oraz konstrukcję i funkcje urządzeń.

Do czynników sprzyjających powstawaniu zagrożeń bezpieczeństwa informacji zaliczyć należy:

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

Zagrożeniami bezpieczeństwa informacji mogą być występujące czynniki i elementy składowe systemu:

- ujawniająca emisja elektromagnetyczna komputerów, terminali i aparatury kanałowej oraz wrażliwość tych elementów na zakłócenie elektromagnetyczne;
- możliwość zdalnej penetracji zasobów informatycznych systemu;

może być zmiana jego stanu i sposobu działania. Istnieją różne metody zablokowania systemu teleinformacyjnego. Jedną z najprostszych do przeprowadzenia metod jest atak polegający na tak silnym przeciążeniu działania systemu wówczas praca w nim okazuje się niemożliwa.

Ten rodzaj sabotażu może sparaliżować pracę organizacji w takim stopniu, że nie będzie ona mogła normalnie funkcjonować. Napastnik zaleje system falą komunikatów, listów elektronicznych, połączeń modemowych i żądań usług sieciowych w tak dużym stopniu, że system nie będzie praktycznie robił nic poza próbami wykonania tych wszystkich zleceń. Bardziej wyrafinowane ataki polegają na przekierowywaniu żądań usług systemu w inne, zupełnie niewłaściwe miejsca.

Znany jest przykład takiego przeprogramowania połączeń modemowych, że każde połączenie było kierowane na przypadkowy błędny numer. Szczególną bolączką jest fakt, że ochrona przed blokadą usług systemu jest bardzo trudna – w praktyce wiąże się z izolowaniem systemu od otoczenia sieciowego. Zagrożenia atakiem występują, gdy istnieją możliwości:

1. Nieuprawnionego dostępu do przechowywanych, przetwarzanych lub przesyłanych informacji niejawnych bez oddziaływania na system;
2. Nieuprawnionego oddziaływania na system, których wykorzystanie może powodować:
   - zmiany w funkcjonowaniu sieci telekomunikacyjnej, w tym przerwanie lub czasowe zablokowanie realizowanych usług;
   - dostęp do przesyłanych, przetwarzanych lub przechowywanych informacji;
   - zniszczenie informacji lub innych zasobów;
   - fałszowanie lub nieuprawnioną modyfikację informacji;
   - dezinformację.

Chcąc jednak uzyskać kryptograficznie bezpieczny i spójny system teleinformatyczny (łączności), należy oprócz eksploatacji tych urządzeń zrealizować szereg przedsięwzięć organizacyjno - technicznych. Eksploatacja sieci teleinformatycznej (łączności) bez systemu ochrony informacji może umożliwić przeciwnikowi (wykorzystującemu istniejące luki w systemie ochrony) dostęp do

Podsystem ten powinien być modyfikowalny. Do budowy podsystemu ochrony informacji należy stosować środki techniczne, programowe i administracyjno – organizacyjne. Użytkownikom należy zostawić swobodę w stosowaniu dodatkowych środków ochrony ich własnej informacji pod warunkiem, że uzyskają odpowiedni atest. Przy projektowaniu i wdrażaniu podsystemu ochrony należy uwzględnić koszty jego budowy i eksploatacji.

Ochrona informacji w sieciach teleinformatycznych obejmuje aspekty zabezpieczania fizycznego, organizacyjnego, przesyłania i przetwarzania danych. Jeśli informacja przesyłana między elementami sieci jest utajniana, lecz nie ma fizycznych ograniczeń w dostępie do systemu, to utajnianie może okazać się bezcelowe. W sieci teleinformatycznej ochrony wymagają:

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

Dla elementów tych istnieją następujące zagrożenia:

- zniszczenie informacji i/lub innych zasobów (nieświadome lub złośliwe);
- fałszowanie lub modyfikacja informacji;
- kradzież, usunięcie lub zgubienie informacji;
- ujawnienie informacji niejawnych;
- przerwanie usługi;
- zmiana uprawnień.

Środki ochrony, zmniejszające ryzyko uzyskania dostępu do danych przez osoby nieupoważnione, ogólnie można podzielić na dwie kategorie: ograniczenie dostępu do zasobów systemu zgodnie z ustaloną polityką ochronną instytucji lub organizacji oraz kodowanie informacji (utajnianie) za pomocą metod kryptograficznych.

Przyszli użytkownicy systemów, urządzeń czy też oprogramowania, które mają służyć do przechowywania, przetwarzania i przesyłania informacji o charakterze niejawnym, muszą mieć pewność, że wyrób który zamierzają kupić spełnia wymagania bezpieczeństwa teleinformacyjnego. Wiara w werbalne

- dołączanie podsłuchowych urządzeń rejestrujących;
- dołączanie niesankcjonowanych terminali;
- nielegalne wykorzystanie terminali użytkowników;
- stosowanie nielegalnego oprogramowania;
- czynniki losowe - zaniki napięcia, przesłuch, błędy w komutacji, zakłócenia w transmisji, powodzie, pożary;
- awarie urządzeń;
- niesolidność personelu wywołana niedoszkoleniem, bezmyślnością lub spowodowana szantażem.

W systemie teleinformatycznym eksploatowanych jest szereg różnych urządzeń i kanałów. Elementy te tworzą kilka podstawowych, zasadniczych podsystemów teleinformatycznych. W każdym z tych podsystemów występuje potrzeba określenia jednoznacznych i ścisłych wymagań dotyczących ochrony kryptograficznej. Do podsystemów tych zaliczyć należy:

- ☐ podsystem telekomunikacyjny;
- ☐ podsystem informatyczny;
- ☐ podsystemu kierowania i zarządzania siecią łączności;
- ☐ podsystem dystrybucji.

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

Podsystem ten powinien spełniać następujące wymagania:

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

strategicznym zajmowała się Rada Ministrów[259], a także Ministerstwo Obrony Narodowej[260]. W opracowanych dokumentach kompetencje w zakresie bezpieczeństwa informacyjnego zostały powierzone Agencji Bezpieczeństwa Wewnętrznego. ABW powstała ze struktur UOP, pracuje aktualnie nad kompleksową strategią ochrony bezpieczeństwa teleinformatycznego, gdyż do jej ustawowych zadań należy m.in. zapewnienie bezpieczeństwa systemów i sieci teleinformatycznych, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową lub służbową.

Zadania ABW w tym zakresie realizuje wyspecjalizowany zespół Departamentu Bezpieczeństwa Teleinformatycznego zwany Jednostką Certyfikującą. Pod wpływem nadchodzących z USA doniesień o atakach na sieci rządowe, od lat dziewięćdziesiątych, w Polsce podjęto zagadnienie ochrony dostępu do danych gromadzonych przez służby publiczne. Sukcesywnie były prowadzone prace nad stworzeniem projektu regulacji prawnych, w randze ustawy bądź rozporządzenia.

Najważniejszymi regulacjami prawnymi dla środowiska teleinformatycznego, które weszły w życie w minionych latach, są ustawy:

- Ustawa o łączności z dnia 23 listopada 1990 r.[261];
- Ustawa z dnia 29 grudnia 1992 roku o radiofonii i telewizji[262];
- Rozporządzenie Ministra Łączności z dnia 31 maja 1993 roku w sprawie określania systemów telekomunikacyjnych, zakładanych i użytkowanych na terytorium Rzeczpospolitej Polskiej[263];
- Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych[264];

---

[259]Por. *Rozporządzenie Prezesa Rady Ministrów* z dnia 9 września 2002 r. w sprawie wymiany informacji istotnych dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczypospolitej Polskiej, „Dz. U." 2002 nr 150, poz. 1234.

[260]Por. Decyzja nr 182/MON z dnia 6 października 2000 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (dokument wewnętrzny).

[261]Por. *Ustawa o łączności z dnia 23 listopada 1990 r.*, Dz. U. 1990 nr 117, poz. 564.

[262]Por. *Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji* Dz. U. 1993 nr 7, poz. 34.

[263]Por. *Rozporządzenie Ministra Łączności* z dnia 31 maja 1993 roku w sprawie określania systemów telekomunikacyjnych, zakładanych i użytkowanych na terytorium Rzeczpospolitej Polskiej, Dz. U. 1993 nr 63, poz. 302.

[264]Por. *Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych*, Dz. U. 1994 nr 24, poz. 83.

zapewnienia producentów czy dealerów o bezpieczeństwie teleinformacyjnym tej kategorii wyrobów jest niewystarczająca.

Użytkownik powinien polegać na wynikach formalnej i bezstronnej oceny, dokonanej przez uprawniony do tego organ. Ocena wyrobu wymaga dobrze zdefiniowanego kryterium oceny zabezpieczenia oraz istnienia jednostki certyfikującej, uprawnionej do wydania potwierdzenia, że oceny dokonane przez laboratorium badawcze zostały przeprowadzone właściwie. Ocena możliwości zabezpieczających systemu może być rozpatrywana jako część większej formalnej procedury przyjęcia systemu teleinformatycznego do stosowania w konkretnym środowisku.

Obecnie na zagrożenia procesów informacyjnych i infrastruktury teleinformatycznej najbardziej narażone są wysoko rozwinięte wielkie państwa, ale również kraje takie jak Polska, mogą spodziewać się potencjalnego ataku.

Kompleksowa ochrona informacji w sieciach teleinformatycznych obejmuje:

- aspekt prawny;
- zabezpieczenia fizyczne i organizacyjne;
- ochronę przed emisją ujawniającą;
- ochronę kryptograficzną.

Z oceny krajowych specjalistów i ekspertów wynika, że zagrożenia dostępu do sieci teleinformatycznej i naruszenia poufnych danych - w tym chronionych ustawą danych osobowych – nie spotykają się z właściwym zrozumieniem ze strony instytucji i podmiotów gospodarczych, które często traktują stały monitoring informacyjny jako dodatkowy, zbędny wydatek. Tak błędnie pojmowana oszczędność może przynieść katastrofalne skutki podczas zagrożeń, pomimo, że spektrum środków ochrony systemów i sieci jest coraz większe oraz tańsze.

Zagadnienia ochrony informacji w polskiej strategii bezpieczeństwa były przedmiotem analizy, już w latach osiemdziesiątych. W Akademii Sztabu Generalnego Wojska Polskiego powstawały prace omawiające znaczenie systemów informacyjnych w siłach zbrojnych[258]. Problemem obiegu informacji o znaczeniu

---

[258]Por. S. Koziej, *Rajdy bojowe,* Warszawa 1987; S. Koziej, *Teoria sztuki wojennej*, Warszawa 1993.

- Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa[275].

Inne zalecenia specjalistów z zakresu ochrony informacji zostały włączone sektorowych dokumentów m.in.: przepisów o rachunkowości, o ochronie danych osobowych, w prawie bankowym i ustawie o ochronie informacji niejawnych.

Na podstawie dokonanej analizy doświadczeń NATO i USA, w roku 2002 przyjęto wypracowaną przez MSWiA definicję polskiej infrastruktury krytycznej, uzgadniając, że narodowa strategia skupiona będzie wokół kategorii „bezpieczeństwa teleinformatycznego". Za infrastrukturę krytyczną państwa uznano „obiekty i urządzenia oraz służby odpowiedzialne za ich ochronę, systemy sieci teleinformatycznej istotne dla bezpieczeństwa ekonomicznego i dobrobytu państwa oraz jego efektywnego funkcjonowania"[276]. Z definicji tej wynika, że wymienione gałęzie gospodarki narodowej, mieszczą się w ramach infrastruktury krytycznej, nazywanej „obszarami informacji szczególnie wrażliwej z punktu widzenia bezpieczeństwa państwa"[277].

Ochroną infrastruktury krytycznej zajmuje się Krajowy System Ochrony Krytycznej Infrastruktury Teleinformatycznej (KSOKITI). Obecnie Agencja Bezpieczeństwa Wewnętrznego patronuje szkoleniom informacyjnym poświęconym upowszechnianiu wiedzy na temat zagrożeń cybernetycznych w wyniku, których, wydawane są certyfikaty inspektorów bezpieczeństwa teleinformatycznego.

Porównując amerykańskie i polskie doświadczenia oraz stan przygotowań naszego kraju do walki z zagrożeniami w dziedzinie teleinformatyki, dokonano oceny możliwości ataków na polską infrastrukturę informacyjną, w wyniku, czego uznano, że prawdopodobieństwo zmasowanych i celowych działań zagrażających bezpieczeństwu informacyjnemu jest niewielkie.

Zmienną, podnoszącą stopień zainteresowania Polską jako przedmiot ataku, staje się natomiast coraz większe zaangażowanie się w walkę ze światowym

---

[275]Por. Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa, Dz. U. nr 180, poz. 1855.
[276]Por. R. Kośla, *Ochrona infrastruktury krytycznej w Polsce - aktualny stan prac*; (URL http://www.cert.pl).
[277]Tamże, s. 113.

- Rządowy projekt ustaw o ochronie danych, przyjęty przez Radę Ministrów 29 sierpnia 1997 roku[265];
- Rozporządzenie Ministra Łączności z dnia 9 października 1999 roku w sprawie ogólnych warunków przyłączenia sieci telekomunikacyjnych oraz zasad rozliczeń[266];
- Ustawa „Prawo telekomunikacyjne" z dnia 21 lipca 2000 r.[267];
- Ustawa z dnia 18 września 2001 roku o podpisie elektronicznym[268];
- Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną [269];
- Ustawa *2* dnia 12 września 2002 roku o elektronicznych instrumentach płatniczych[270];
- Rozporządzenie Ministra Infrastruktury z dnia 24 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego[271];
- Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym[272];
- Rozporządzenie Ministra Infrastruktury z dnia 7 maja 2004 w sprawie sposobu uwzględniania w zagospodarowaniu przestrzennym potrzeb obronności i bezpieczeństwa państwa[273];
- Ustawa „Prawo Telekomunikacyjne" z dnia 16 lipca 2004 r.[274];

---

[265]Por. *Rządowy projekt ustaw o ochronie danych*, Dz. U. 1997 nr 133, poz. 883.

[266]Por. *Rozporządzenie Ministra Łączności z dnia 9 października 1999 roku w sprawie ogólnych warunków przyłączenia sieci telekomunikacyjnych oraz zasad rozliczeń*, Dz. U. 1999 nr 79, poz. 897.

[267]Por. *Ustawa „Prawo telekomunikacyjne" z dnia 21 lipca 2000 r.*, Dz. U. 2000 nr 73, poz. 852.

[268]Por. *Ustawa z dnia 18 września 2001 roku o podpisie elektronicznym* Dz. U. 2001 nr 130, poz. 1450.

[269]Por. *Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną* Dz. U. 2002 nr 144, poz. 1204.

[270]Por. *Ustawa 2 dnia 12 września 2002 roku o elektronicznych instrumentach płatniczych* Dz. U. 2002 nr 169, poz. 1385.

[271]Por. *Rozporządzenie Ministra Infrastruktury z dnia 24 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego*, Dz. U. 2003, nr 2 poz. 47.

[272]Por. *Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym*, Dz. U. nr 5 poz. 37.

[273]Por. *Rozporządzenie Ministra Infrastruktury z dnia 7 maja 2004 w sprawie sposobu uwzględniania w zagospodarowaniu przestrzennym potrzeb obronności i bezpieczeństwa państwa*, Dz. U. 2004 nr 6 poz.41.

[274]Por. Ustawa „Prawo telekomunikacyjne" z dnia 16 lipca 2004 r., Dz. U. 2004 nr 171, poz. 1800.

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

❑ szyfrowanie kanałowe:

- szyfrowanie baz danych;
- uwierzytelnianie użytkownika.

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

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

Mechanizmy zabezpieczające obejmują następujące działania:

□ szyfrowanie informacji;

□ uwierzytelnianie informacji (podpisy cyfrowe);

□ ochrona antywirusowa;

□ identyfikacja i uwierzytelnianie osób uprawnionych.

Kryptograficzne metody ochrony są ważnym elementem bezpieczeństwa informacji w sieciach teleinformatycznych i chociaż mają zasadnicze znaczenie, same nie gwarantują pełnego bezpieczeństwa informacji. Celem kryptograficznej

terroryzmem, które sytuuje nasz kraj wśród głównych sojuszników Stanów Zjednoczonych. Ryzyko realne jest, zatem dotąd niewielkie, lecz ryzyko potencjalne – sukcesywnie rośnie. Stopień bezpieczeństwa teleinformatycznego jest, zatem pochodną aktywności sojuszniczej Polski.

Prezes Rady Ministrów w dokumencie z 22 lipca 2002 roku, ustanowił odpowiedzialność Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego w zakresie: akredytacji bezpieczeństwa systemów i sieci teleinformatycznych, badań i certyfikacji środków ochrony kryptograficznej, elektromagnetycznej i fizycznej oraz organizacji szkoleń w dziedzinie bezpieczeństwa teleinformatycznego[278].

Znane dzisiaj metody ochrony informacji nie gwarantują absolutnego bezpieczeństwa i dalekie są od ideału, a zjawiska włamań do sieci nie dają się wyeliminować. Włamania do systemów teleinformatycznych przynoszą znaczne straty finansowe i często utratę zaufania do instytucji, której powierzono poufne informacje. Zgodnie z ustaloną i prowadzoną polityką ochronną w danej instytucji, istnieje szereg różnych metod i środków ochrony informacji. Do podstawowych z nich zaliczyć należy:

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

---

[278]Tamże, s. 124.

Wykorzystywanie tego samego klucza przez wielu użytkowników grozi jego dekonspiracją (np. wskutek utraty urządzenia utajniającego z kluczem), a w konsekwencji ujawnieniem wszystkich informacji zaszyfrowanych z jego użyciem. Stąd wymaga się, aby w każdej relacji i seansie łączności do szyfrowania informacji był wykorzystywany inny klucz. Do identyfikacji użytkownika wykorzystywane są tzw. inteligentne karty SIM, zawierające mikroprocesor z pamięcią. W pamięci są zapisane: numer użytkownika oraz jego prywatny tajny klucz szyfrowy. W SIM są zaimplementowane algorytmy szyfru jednokierunkowego, wykorzystywane w procesie identyfikacji i uwierzytelniania użytkownika oraz do wypracowania klucza wykorzystywanego w procesie szyfrowania przesyłanych informacji. Podstawowe pojęcia z zakresu ochrony danych to: atak na bezpieczeństwo danych, mechanizm zabezpieczający i usługa ochrony danych.

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

W specjalistycznej literaturze spotyka się często pojęcie, że urządzenia elektroniczne wytwarzają promieniowanie elektromagnetyczne, które może być związane z przetwarzaną informacją, jednak to stwierdzenie jest truizmem. Ta konstatacja spowodowała, że w Stanach Zjednoczonych pod koniec lat 50-tych zapoczątkowano specjalny program badawczy znany pod kryptonimem TEMPEST. TEMPEST jest oficjalnym akronimem (ang. „Telecommunications Electronics Material Protected From Emanating Spurious Transmissions") i zawiera techniczne środki bezpieczeństwa, standardy i oprzyrządowanie, które zapobiegają (ewentualnie minimalizują) wykorzystaniu słabych punktów bezpiecznych systemów. TEMPEST został „wynaleziony" w 1918 roku, gdy armia USA zatrudniła Herberta Yardleya wraz z jego zespołem, aby rozwinąć metody detekcji, podsłuchu i wykorzystania chronionych nadajników radiowych. Wstępne badania wykazały, że standardowy, niezmodyfikowany sprzęt, poprzez jego techniczne

ochrony informacji w systemie teleinformatycznym jest:

a) wyeliminowanie dostępu do zasobów podsystemu osobom nieuprawnionym;

b) zapewnienie dostępu do zasobów legalnym użytkownikom w ramach ich uprawnień;

c) zapewnienie poufności informacjom niejawnym przechowywanym na dyskach;

d) zapewnienie poufności, integralności i uwierzytelniania informacjom niejawnym przesyłanym w sieci teleinformatycznej.

Jeśli informacja jest szyfrowana, ale nie ma fizycznych ograniczeń w dostępie do systemu lub brak jest zabezpieczeń przed emisją ujawniającą, to szyfrowanie nie zapewni wysokiego poziomu bezpieczeństwa. Odpowiednio zaprojektowane i wdrożone szyfry zdecydowanie ograniczają możliwości działania nawet wyrafinowanego przeciwnika. Brak kryptograficznej ochrony informacji w sieci może powodować, że bezcelowe są inne działania (np. ochrona przed emisją ujawniającą). Metody kryptograficzne są wykorzystywane do:

- zapewnienia poufności informacjom przechowywanym i przesyłanym w sieci;
- zachowania integralności przesyłanych i przechowywanych danych;
- uwierzytelniania informacji;
- zapewnienia integralności połączenia (uniemożliwienie odbioru informacji przez innego niż adresat użytkownika);
- wiarygodnej identyfikacji i uwierzytelniania użytkowników i stacji;
- wiarygodnej weryfikacji uprawnień użytkowników do korzystania z zasobów sieci poprzez sterowanie dostępem (autoryzację) do danych;
- ochrony przed fałszywymi powtórzeniami;
- maskowania przepływu informacji między obiektami sieci.

Pełną poufność przesyłanych informacji zapewnić można tylko przez szyfrowanie u źródła i deszyfrowanie dopiero przy jej ujściu. Istotnym problemem jest wtedy dystrybucja kluczy szyfrowych. Zmiana kluczy odbywać się musi w taki sposób, aby nie powodowała utraty spójności sieci.

NATO. U podstaw zaproponowanej filozofii ochrony informacji przed elektromagnetycznym przenikaniem leżą zasady wielopłaszczyznowego wykorzystania różnych czynników.

Pierwszym etapem ochrony informacji jest projekt urządzenia przetwarzającego niejawną, nie utajnioną informację (np. mikrokomputer wykorzystywany do tworzenia niejawnych dokumentów). Można próbować tak zaprojektować i wykonać urządzenie, aby poziomy emisji ujawniających były jak najmniejsze. Takie działania prowadzą do uzyskania odpowiedniego poziomu zabezpieczenia urządzenia, czyli zakresu wykorzystania rozwiązań technologicznych jako integralnej części konstrukcji urządzenia w celu obniżenia poziomu emisji ujawniającej. Miarą poziomu zabezpieczenia urządzenia jest wartość współczynnika protekcji (czyli stosunku mocy zakłóceń do mocy sygnału emisji ujawniającej) w odległości ρ od przetwornika sygnału: $\Delta = \Delta(\rho)$.

Wyróżniono trzy poziomy zabezpieczeń:

I. poziom zabezpieczeń urządzeń - $\Delta(\rho) = \Delta_1$;

II. poziom zabezpieczeń urządzeń - $\Delta(\rho) = \Delta_2$;

III. poziom zabezpieczeń urządzeń - $\Delta(\rho) = \Delta_3$.

Jeżeli zapewnienie urządzeniu odpowiedniego poziomu zabezpieczenia okaże się zbyt trudne lub zbyt kosztowne, można je umieścić w odpowiednim środowisku, którego zadaniem byłoby zmniejszenie emisji ujawniającej. Prowadzi to do odpowiedniego poziomu zabezpieczenia miejsca - poprzez wykorzystanie technologii filtracji i ekranowania w celu obniżenia emisji ubocznej przetwornika w miejscu jego pracy (eksploatacji). Wykorzystanie tej technologii może polegać na filtracji obwodów sygnałowych i zasilania energetycznego oraz na stosowaniu specjalnych obudów, kabin ekranowych lub na ekranowaniu pomieszczeń.

Zgodnie z obowiązującą od 01.07.2000 r. normą obronną NO-06-A201, wprowadzającą wymagania na tłumienność obiektów ekranujących, istnieją trzy następujące poziomy:

I. poziom ekranowania - obniżenie poziomu emisji elektromagnetycznej o $A_e = A_1$;

II. poziom ekranowania - obniżenie poziomu emisji elektromagnetycznej o $A_e = A_2$;

słabości, umożliwia przeciwnikowi przechwytywanie niejawnych informacji. Następnie, jak wcześniej wspomniano, został wykreowany niejawny program badawczy, którego celem było rozwinięcie metod ograniczania tzw. „emisji ujawniających". Jednakże aktualny akronim znany jako TEMPEST został wymyślony na przełomie lat 60/70 i obecnie jest uważany jako termin przestarzały wypierany przez frazę ang. - „Emissions Security" lub EMSEC, co w języku polskim oznacza „Bezpieczeństwo emisji".

W celu uporządkowania terminologii stosowane są następujące definicje:

- emisja ujawniająca (Compromising Emanation);
- niepożądana emisja sygnału, którego pewne cechy związane są z informacją nadawaną, odbieraną, przechowywaną i przetwarzaną przez przetworniki sygnału.

Ze względu na kanał przenikania informacji, emisję ujawniającą dzielimy na emisję promieniowaną i emisję przewodzoną:

1. Bezpieczeństwo emisji (ang. Emission Security). Wszelkie przedsięwzięcia utrudniające dostęp osób niepowołanych do informacji, która może być uzyskana przez odbiór i analizę emisji ujawniającej. Część bezpieczeństwa łączności;
2. Bezpieczeństwo łączności (ang. Communication Security). Wszelkie przedsięwzięcia utrudniające dostęp osób niepowołanych do informacji, którą można uzyskać z penetracji systemów łączności. W USA bezpieczeństwo łączności oznaczane jest akronimem COMSEC i obejmuje fizyczne zabezpieczenie informacji, zabezpieczenie kryptograficzne, bezpieczeństwo transmisji i bezpieczeństwo emisji.

Uwzględniając powyższe można stwierdzić, że bezpieczeństwo emisji jest jedną z cegiełek, z których buduje się bezpieczeństwo sieci teleinformatycznej. Bezpieczeństwo emisji związane jest ściśle z normami dotyczącymi tej problematyki (zazwyczaj są to normy niejawne). Pomimo, że zagraniczne normy z tej dziedziny są niejawne, w tym najbardziej zaawansowane - amerykańskie normy TEMPEST, to na podstawie fragmentarycznych danych, dostępnych w literaturze technicznej oraz na podstawie doświadczeń z badań urządzeń ochrony informacji firm zachodnich, a także ostatnio coraz szerszego dostępu do wymagań

1999 r. o ochronie informacji niejawnych". W Polsce dość skutecznie chroni się bazy danych firm przed hakerami działającymi w sieciach komputerowych oraz zwykłymi włamaniami np. do linii transmisyjnych. Zupełnie inny wymiar ma ochrona przed włamaniami do systemów komputerowych dokonywanych przy użyciu nowoczesnych systemów skanujących dane „namierzonego" komputera. W naszym kraju normy te nie były dotychczas stosowane. Zabezpieczenie komputerów przed emisją ujawniającą w wielu instytucjach i urzędach centralnych z przedstawionych powyżej przyczyn nie jest najlepsze, a szczególnie w instytucjach placówkach naukowych. Można mieć nadzieję, że w najbliższych latach, konieczność tworzenia społeczeństwa informacyjnego, a przede wszystkim obecności państwa w strukturach NATO i UE pozwoli na nadrobienie zaistniałych zaległości i stworzenia skutecznych systemów zabezpieczeń i ochrony informacji w systemach komputerowych jak i samych komputerów.

Etapy realizacji podsystemu bezpieczeństwa i ochrony w systemach teleinformatycznych.

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

a) identyfikację słabych punktów systemu;
b) analizę prawdopodobieństwa występowania zagrożeń z uwzględnieniem słabych punktów systemu;
c) ocenę konsekwencji wykorzystania każdego zagrożenia indywidualnie oraz w powiązaniu z innymi zagrożeniami;
d) oszacowanie kosztów każdego ataku (w tym ocenę na ile udany atak ułatwia następne);
e) oszacowanie kosztów potencjalnych środków przeciwdziałania, w tym również ewentualnego pogorszenia parametrów funkcjonalnych systemu.

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

III. poziom ekranowania - obniżenie poziomu emisji elektromagnetycznej o $A_e = A_3$.

Naturalnym sposobem ograniczania poziomu emisji ujawniającej jest uniemożliwienie przeciwnikowi zbliżenia się do przetwornika informacji. W ten sposób pojawia się koncepcja stref bezpieczeństwa emisji warunkowanych wartościami tłumienności na ich granicy lub w terenie otwartym odległościami do ich granic. Wyróżniono następujące strefy:

- 0 (zerowa) strefa bezpieczeństwa emisji (0SBE): $d_0 \leq r_0$, lub minimalna tłumienność dla emisji ujawniającej A_{s0};
- 1 (pierwsza) strefa bezpieczeństwa emisji (1SBE): $r_0 < d_1 \leq r_1$, lub minimalna tłumienność dla emisji ujawniającej A_{s1};
- 2 (druga) strefa bezpieczeństwa emisji (2SBE): $r_1 < d_2 < r_2$, lub minimalna tłumienność dla emisji ujawniającej A_{s2};
- 3 (trzecia) strefa bezpieczeństwa emisji (3SBE): $d > r_2$, lub minimalna tłumienność dla emisji ujawniającej A_{s3}.

Wymienione metody ochrony, tzn. zabezpieczenie urządzenia, zabezpieczenie miejsca oraz strefa bezpieczeństwa emisji, w konkretnym przypadku muszą zapewnić odpowiedni poziom zabezpieczenia informacji, – czyli wymagany stopień obniżenia poziomu emisji ujawniającej w celu uniemożliwienia odtworzenia informacji z wymaganą wiernością i w zadanym czasie. Miarą poziomu zabezpieczenia informacji jest wartość współczynnika protekcji w odpowiedniej odległości od jej przetwornika. Przedstawiona powyżej wielowariantowa możliwość zapewnienia stanu bezpieczeństwa emisji pozwala elastycznie wybierać to rozwiązanie, które w danej sytuacji jest najlepsze z technicznego i ekonomicznego punktu widzenia.

Omówiona problematyka bezpieczeństwa emisji regulowana jest w NATO. Należy jednakże podkreślić, że poszczególne kraje członkowskie niezależnie od zobowiązań NATO-wskich stosują swoje narodowe normy, które stworzyły swoje wymagania narodowe nie udostępniane innym krajom, nawet sojusznikom. Postęp w komputeryzacji nie spowodował jednak doskonalenia systemów zabezpieczenia przed dostępem do informacji klasyfikowanych przez „Ustawę z dnia 22 stycznia

Szkolenie personelu w zakresie ochrony informacji jest sprawą poza wszelką dyskusją, choć często zaniedbywaną. Niezbędna jest ciągła współpraca personelu zajmującego się ochroną z komórkami organizacyjnymi przedsiębiorstwa, jak również wspomaganie, zrozumienie i elastyczność wobec użytkownika końcowego. Proces edukacyjny dla całego personelu powinien być dostosowany do oczekiwań i potrzeb każdej grupy pracowniczej, w przeciwnym razie ochrona będzie pomijana, wyłączana lub ignorowana. Ustalenie polityki ochrony i przeszkolenie personelu są wstępem do wprowadzenia w życie planu ochrony - realizacja tego zadania powinna być w miarę „bezbolesna" i płynna.

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

Jakość podsystemu bezpieczeństwa i ochrony zależy od prawidłowego opracowania założeń, wyboru odpowiednich urządzeń utajniających oraz zrealizowania przedsięwzięć organizacyjno-administracyjnych. Zaproponowana konstrukcja urządzeń utajniających powinna umożliwić wdrożenie modułu do wielu urządzeń podsystemu łączności. Przyjęta technologia powinna pozwolić na ciągły rozwój urządzeń już opracowanych, wdrożonych i eksploatowanych. Kolejne wersje urządzenia lub określone ich funkcje mogą być wprowadzane przez upoważnione osoby u użytkownika, po dołączeniu dowolnego urządzenia telekomunikacyjnego lub informatycznego.

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

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

Następnym etapem powinien być więc wybór odpowiednich urządzeń utajniających. W celu zrealizowania ww. założeń, w urządzeniach tych powinny być zainstalowane następujące niezbędne elementy:

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

Podstawowym etapem w organizowaniu systemu ochrony jest rozpoznanie obszaru ochrony. Przede wszystkim trzeba określić, z czego składa się sieć: jak wygląda schemat sieci, punkty dostępu do sieci i kto z nich korzysta. Ponadto należy dokonać oceny wartościowej informacji. Jakie zasoby informacyjne są na tyle ważne, aby je chronić, i gdzie są zlokalizowane?

w Goeteborgu 16.06.2001 r. plan działań sporządzony przez kraje kandydujące przy wsparciu Komisji Europejskiej;

- *ePolska* – „Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006" - rządowa strategia rozwoju społeczeństwa informacyjnego, która została przyjęta przez Radę Ministrów 11 września 2001r., przygotowana przez byłe Ministerstwo Łączności - od października 2001 r. przez Ministerstwo Infrastruktury;
- Ustawa z dnia 12 stycznia 1991 r. o Komitecie Badań Naukowych;
- uchwała Sejmu RP z 14 lipca 2000r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce;
- stanowisko Rady Ministrów z dnia 28 listopada 2000 r. w sprawie powyższej uchwały Sejmu RP, „Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce" - dokument przyjęty przez Radę Ministrów 28 listopada 2000 r., opracowany przez Komitet Badań Naukowych i Ministerstwo Łączności.

W związku z członkostwem w UE i koniecznością realizacji przyjętych programów należało podjąć niezbędne działania dotyczące wzmocnienia administracyjnego:

- stworzenie silnego i niezależnego regulatora rynku pocztowego i telekomunikacyjnego - Urzędu Regulacji Telekomunikacji i Poczty;
- świadczenie usług powszechnych odpowiedniej jakości, dostępnych wszystkim potencjalnym użytkownikom;
- kontynuowanie działań związanych z rozwojem społeczeństwa informacyjnego w Polsce.

Instytucjami realizującymi te programy w tym przypadku są:

- Ministerstwo Infrastruktury - program „*ePolska – Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*";
- Komitet Badań Naukowych - zespół ds. *e*Europe+, monitorowanie realizacji zadań w zakresie rozwoju społeczeństwa informacyjnego w Polsce, współpraca z programem eContent, zadania realizowane

Strategia bezpieczeństwa informacyjnego państwa nie została jeszcze w pełni określona, o tym decyduje poziom rozwoju sieci, komputeryzacja sektora publicznego i poziom zrozumienia nowych zagrożeń przez podmioty gospodarcze szczególnie prywatne. Powstaje ona na możliwościach dostosowań polskiej gospodarki do modelu społeczeństwa informacyjnego i zmian a przede wszystkim w sektorze telekomunikacyjnym. Program dostosowawczy *ePolska* jest inicjatywą pomostową, która odpowiada na unijne dyrektywy, sugerujące przygotowanie państw kandydackich do jednolitego modelu społecznego (program *eEuropa+).* Diagnozuje podstawowe zagrożenia w dziedzinie bezpieczeństwa informacyjnego i wskazuje prawne środki zapobiegania. Polski system legislacyjny powoli dostosowuje się do nowych rodzajów przestępstw teleinformatycznych.

Należy jednak opracować strategie szkoleniowe, prowadzić stały monitoring sieci i systemów, zapewnić szeroką kampanię informacyjną na temat zagrożeń bezpieczeństwa teleinformatycznego. Z tworzeniem systemu muszą być powiązane: harmonizacja systemu prawnego i zmiany legislacyjne, wprowadzające m.in. ściganie z urzędu przestępstw teleinformatycznych (szczególnie komputerowych).

3.3. Programy kształtowania infrastruktury telekomunikacyjnej na początku XXI wieku, a założenia postulowanego modelu rozwoju infrastruktury telekomunikacyjnej

3.3.1. Koncepcja kształtowania infrastruktury telekomunikacyjnej na początku XXI wieku

Jednym z programów kształtowania infrastruktury telekomunikacyjnej był „Raport w sprawie dostosowań instytucjonalnych w Polsce do wymogów członkostwa w Unii Europejskiej" dział „Telekomunikacja i technologie informacyjne" - przyjęty przez Komitet Integracji Europejskiej 10 kwietnia 2002 r. Instytucją wiodąca w zakresie telekomunikacji jest Ministerstwo Infrastruktury, a w zakresie technologii informacyjnych - Komitet Badań Naukowych. Rozwój społeczeństwa informacyjnego a tym samym infrastruktury telekomunikacyjnej został odzwierciedlony w następujących dokumentach programowych oraz podstawach prawnych;

- program „*eEurope+2003* - A Cooperative Effort to Implement the Information Society in Europe" - ogłoszony podczas szczytu UE

W związku z koniecznością rozwoju społeczeństwa informacyjnego w Polsce 17.05.1999 r. powołany został, zarządzeniem Prezesa Rady Ministrów, *Międzyresortowy Zespół ds. handlu metodami elektronicznym.* Zespół wykonał analizę obowiązującego stanu prawnego pod kątem możliwości wykorzystania istniejących regulacji prawnych w transakcjach zawieranych metodami elektronicznymi i wyznaczył kierunki niezbędnych prac legislacyjnych w tym obszarze w dokumencie z „*Program prac legislacyjnych Rządu w zakresie handlu metodami elektronicznymi na lata 2000-2002*", przyjętym przez Radę Ministrów 11.07.2000 r. - Zespól zakończył pracę 30.06.2000 r. natomiast 30.11.2000 r. Prezes RM powołał zarządzeniem nr 89, w celu kontynuacji prowadzonych działań, *Międzyresortowy Zespół do spraw gospodarki elektronicznej.*

Ministerstwo Gospodarki przygotowało program „*Zwiększanie innowacyjności gospodarki w Polsce do 2006 roku*" (zatwierdzony w lipcu 2000 r. przez Radę Ministrów), który ma na celu promowanie rozwoju technik informacyjnych, jako jednego z istotnych elementów wpływających na innowacyjność i konkurencyjność gospodarki,

Natomiast Rada Ministrów w dniu 28.11.2000 r. przyjęła dokument „*Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce*". Dokument ten zawiera priorytety dotyczące powszechnego dostępu do informacji, edukacji informatycznej, zmian struktury zatrudnienia, walki z przestępczością informatyczną, gospodarki elektronicznej, informatyzacji zamówień publicznych, administracji, rozwoju rynku teleinformatycznego, zastosowania informatyki w dziedzinie nauki i kultury oraz działania konieczne dla ich osiągnięcia.

Zgodnie z ustaleniami z posiedzenia Rady Ministrów z 28.11.2000 r. oraz z zapisami dokumentu *ePolska – plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*, Minister Nauki i Informatyzacji – przewodniczący Komitetu Badań Naukowych monitoruje realizację zadań związanych z rozwojem społeczeństwa informacyjnego w Polsce i przedkłada Radzie Ministrów co kwartał raporty w tym zakresie. Wszystkie raporty publikowane są również w Internecie,

Minister Nauki – Przewodniczący Komitetu Badań Naukowych 23.01.2001 r. powołał *Forum ds. Społeczeństwa Informacyjnego* - zespół

w ramach 5 Programu Ramowego oraz prace nad 6 Programem Ramowym;

- Ministerstwo Gospodarki - handel elektroniczny oraz realizacja „Program prac legislacyjnych Rządu w zakresie handlu metodami elektronicznymi na lata 2000-2002";
- Ministerstwo Spraw Wewnętrznych i Administracji - informatyzacja administracji;
- Ministerstwo Kultury,
- Ministerstwo Edukacji Narodowej i Sportu,
- Ministerstwo Finansów, Główny Urząd Statystyczny,
- Urząd Regulacji Telekomunikacji i Poczty,
- Ministerstwo Sprawiedliwości,
- Urząd Komitetu Integracji Europejskiej.

Polska jest stale reprezentowana we Wspólnym Komitecie Wysokiego Szczebla do spraw społeczeństwa informacyjnego przez Przewodniczącego KBN - obecnie Ministra Nauki i Informatyzacji oraz Ministra Infrastruktury. Ponadto na mocy postanowień KIE z 28 marca 2001r. stworzony został Zespołu ds. eEuropy+, którego zadaniem jest m.in. opracowywanie stanowisk Polski na spotkania Wspólnego Komitetu Wysokiego Szczebla (pod przewodnictwem Ministra Nauki i Informatyzacji, w skład, którego weszli przedstawiciele Ministerstwa Łączności – obecnie Ministerstwa Infrastruktury, Ministerstwa Gospodarki, Głównego Urzędu Statystycznego, Ministerstwa Spraw Wewnętrznych i Administracji, Ministerstwa Finansów, Urzędu Komitetu Integracji Europejskiej, Ministerstwa Zdrowia oraz Ministerstwa Rolnictwa i Rozwoju Wsi).

Od 2000 r. Polska jest pełnoprawnym uczestnikiem Piątego Programu Ramowego Badań, Rozwoju Technicznego i Prezentacji WE. Polscy eksperci biorą udział w pracach Wspólnoty Europejskiej nad Szóstym Programem Ramowym, który ma wejść w życie w 2002 r. Polskie instytucje aktywnie uczestniczą m.in. w Information Society Technologies – podprogramie poświęconym rozwojowi technik informacyjnych i ich zastosowaniom, zaś przedstawiciele Polski biorą również udział w pracach IST Committee oraz jego grupach roboczych ds. edukacji, zdrowia, transportu oraz bezpieczeństwa i zaufania.

- opracowanie zbiorczego planu rozwoju teleinformatyki i jej zastosowań w administracji rządowej;
- rozwój infrastruktury niezbędnej do wdrażania założeń programów wspierania społeczeństwa informacyjnego;
- działania na rzecz edukacji informatycznej i walki z tzw. informacyjnym wykluczeniem;
- promowanie innowacyjnych zastosowań technik informacyjnych;
- zwiększenie powszechnego dostępu do Internetu;
- liberalizacja rynku telekomunikacyjnego, w tym uwolnienie pętli abonenckich.

Zgodnie z dokumentem „*ePolska - Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*" ma nastąpić przygotowanie społeczeństwa polskiego do szybkich przemian technologicznych, społecznych i gospodarczych związanych z tworzeniem się społeczeństwa informacyjnego, poprzez:

- dostosowanie regulacji prawnych do wymagań szybkiego postępu technologicznego i ery społeczeństwa informacyjnego;
- przygotowanie społeczeństwa polskiego do wyzwań nowego rynku pracy i nowych metod pracy;
- dostosowanie gospodarki narodowej do wymagań globalnej gospodarki,
- stworzenie przejrzystych i przyjaznych obywatelowi struktur administracji publicznej na miarę otwartego społeczeństwa informacyjnego za pomocą narzędzi wykorzystujących technologie informacyjne i komunikacyjne;
- stworzenie warunków dla trwałego i zrównoważonego rozwoju regionalnego z uwzględnieniem nowoczesnych technik społeczeństwa informacyjnego;
- wzrost innowacyjności gospodarki w celu poprawy jej konkurencyjności,
- zapewnienie wsparcia dla gospodarki elektronicznej przez zaplecze naukowe w celu lepszego wykorzystania szans, jakie oferuje model społeczeństwa informacyjnego;
- szeroką promocję kultury polskiej;

przedstawicieli ministerstw, urzędów centralnych, organizacji pozarządowych oraz samorządowych działających w dziedzinie społeczeństwa informacyjnego, którego zadaniem tego zespołu jest inicjowanie nowych zadań w zakresie społeczeństwa informacyjnego.

Rada Ministrów w dniu 11.09.2001r. przyjęła strategię rozwoju społeczeństwa informacyjnego „*ePolska - Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*". Dokument ten, przygotowany przez byłe Ministerstwo Łączności (obecnie Ministerstwo Infrastruktury) na wzór podjętej przez UE inicjatywy *e*Europe – przedstawia analizę potrzeb w sferze dostępu do informacji, jej zakresu, środków jej przekazywania i udostępniania. Corocznie weryfikowany i aktualizowany plan działań *ePolska,* jest dokumentem o znaczeniu strategicznym.

Ministerstwo Spraw Wewnętrznych i Administracji prowadzi prace nad zbiorczym planem informatyzacji administracji w Polsce *„Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce – informatyzacja administracji".*

Sejm RP w dniu 21.12.2001 przyjął ustawę o zmianie ustawy o organizacji i trybie pracy Rady Ministrów oraz o zakresie działania poszczególnych ministrów, ustawy o działach administracji rządowej oraz o zmianie niektórych ustaw, na mocy, której utworzony został dział administracji rządowej pod nawą 'informatyzacja', obejmujący m.in. sprawy społeczeństwa informacyjnego w Polsce. Odnośne przepisy wejdą w życie z dniem 01.07.2002 r.

W związku z członkostwem w Unii Europejskiej realizacja określonych celów, zależeć będzie od wykonania w jak najkrótszym czasie następujących zadań:

- przygotowanie oraz wdrożenie zgodnych z prawem wspólnotowym WE regulacji dotyczących dokumentu i handlu elektronicznego (m.in. Ustawa o świadczeniu usług drogą elektroniczną – przewidywany termin rozpatrzenia przez Radę Ministrów – 16 kwietnia 2002 r., Ustawa o elektronicznych instrumentach płatniczych);
- wdrożenie ustawy z dnia 28 kwietnia 2000 r. o systemie oceny zgodności i akredytacji oraz zmianie niektórych innych ustaw, związane z działaniem jednostki akredytującej w związku z wymogami ustawy o podpisie elektronicznym, w Ministerstwie Gospodarki;

do tych dziedzin, gdzie są niezbędne: ustanawianie prawa, dbanie o bezpieczeństwo, tworzenie struktur administracyjnych oraz podejmowania niezbędnych decyzji administracyjnych. Dopiero wówczas możemy mówić o usunięciu przeszkód stających na drodze rozwoju państwa" – teza ta została wygłoszona, podczas konferencji pt. *„Standardy bezpieczeństwa systemów informatycznych w Unii Europejskie"*[279]. Została ona zorganizowana w Krakowie w maju 2002 roku i stała się okazją do wzmocnienia rządowego stanowiska w sprawie bezpieczeństwa informatycznego. Minister Danuta Huebner, w wystosowanym na tę okazję liście do uczestników konferencji, stwierdziła m.in.: „Droga do rozwoju wiedzie przez wiedzę, dlatego naturalne wydaje się realizowanie wizji społeczeństwa informacyjnego i elektronicznego obrotu gospodarczego"[280]. Nawiązywano w ten sposób do aktywnej postawy Polski w organizowaniu wielostronnych konsultacji związanych z dostosowaniem do standardów Sl. W maju 2000 roku w Warszawie zorganizowana została konferencja pt. *„Information Society — Accelerating European* Integra*tion",* poświęcona zagadnieniom społeczeństwa informacyjnego. W dokumencie końcowym konferencji Polska i inne kraje kandydujące zobowiązały się do współpracy z Komisją Europejską przy opracowaniu wspólnego dokumentu programowego *eEurope+* oraz przygotowania krajowego planu działania inicjatywy - *ePolska.* Deklaracja konferencji warszawskiej zakłada, że celami politycznymi, które mają osiągnąć kraje kandydackie poprzez wspólny plan działania *eEurope+* są:

- zademonstrowanie opinii publicznej wspólnych wysiłków krajów „Piętnastki" oraz krajów nowo przyjętych na rzecz realizacji wyzwań nowej ekonomii;
- wskazanie, że proces akcesji to coś znacznie większego niż negocjowanie *acquis communautaire;*
- polityczne wsparcie dla wysiłków czynionych przez kandydujące kraje w kierunku integracji europejskiej;
- zaprezentowanie komplementarności inicjatywy *eEurope* oraz planu

---

[279]Por. M. Wardaszko, *Bezpieczeństwo a problemy informatyzacji w Polsce,* [URL - http://www.m-signet.com.pl/archiwum/ 51.html].
[280]Tamże, s. 98.

- podjęcie działań tworzących warunki do angażowania się samorządów w zwiększaniu liczby punktów dostępu do sieci, oraz Wspieranie inicjatyw rozwoju i budowy sieci amatorskich i prywatnych oraz stworzenie, przyjęcie i skuteczne egzekwowanie przepisów uniemożliwiających blokowanie budowy sieci;
- realizuje program *„PIONIER: Polski Internet Optyczny – Zaawansowane Aplikacje, Usługi i Technologie dla Społeczeństwa Informacyjnego”.*

Program ePolska 2001-2006 obejmuje działania związane z:

- rozwojem infrastruktury teleinformatycznej;
- stworzeniem powszechnego dostępu do tańszego, szybszego i bezpiecznego Internetu (szybki Internet dla naukowców, bezpieczeństwo sieci, wolne oprogramowanie);
- inwestowaniem w ludzi i umiejętności (edukacja w erze cyfrowej, praca zawodowa w społeczeństwie informacyjnym, powszechny udział w gospodarce opartej na wiedzy, polskie zasoby kultury w sieciach globalnych);
- stymulowaniem lepszego wykorzystania technologii informacyjnych (gospodarka elektroniczna, sądownictwo i prokuratura w sieci, administracja publiczna on-line, teleinformatyka w policji, ochrona zdrowia on-line, integracja społeczna on-line, inteligentne systemy wspomagania transportu);
- wprowadzaniem teleinformatyki na obszary wiejskie;
- rozwojem radiofonii i telewizji cyfrowej.

Polska podziela stanowisko grupy państw nowo przyjętych do Unii, że należy dostosowywać systemy administracyjne do założeń wspólnej polityki rozwojowej. Strona polska deklarowała w 2001 roku posiadanie 49% osieciowanych jednostek samorządowych, przyznając równocześnie niewystandaryzowanie jakości ich połączeń. Integracja Polski ze strukturami Unii Europejskiej wymaga realizacji idei społeczeństwa informacyjnego, w którym ogromną rolę w gospodarce odgrywają systemy informacyjne. „Społeczeństwo informacyjne jest narzędziem dla rozwoju państwa. [...] Dążąc do celu, jakim jest rozwój społeczeństwa informacyjnego, państwo musi ograniczyć swe kompetencje

efekty współpracy z zagranicą w zakresie bezpieczeństwa sieciowego[282]. Celom tym podporządkowano sektorowe działania przewidziane do realizacji w okresie pięciu lat. Deklaruje się, zatem opracowanie szczegółowej strategii bezpieczeństwa sieciowego, nowelizację i tworzenie aktów prawnych odnoszących się do cyberprzestępstw, pogłębienie kooperacji międzynarodowej. Koordynacja strategii leży w gestii Ministerstw: Sprawiedliwości, Spraw Wewnętrznych i Administracji, Spraw Zagranicznych; Komitetu Badań Naukowych, CERT Polska i Komendy Głównej Policji (KGP).

Dążenie do poprawy bezpieczeństwa wewnętrznego państwa zostało opisane jako nadrzędny cel rozwoju łączności i technologii informacyjnej w policji[283]. Komunikacja intranetowa służyć ma przepływowi danych z systemów PESEL, REGON, Centralnej Ewidencji Kierowców i Pojazdów, oraz Centralnego Rejestru Skazanych. Przewidywane są działania na rzecz budowy systemów analizy kryminalnej (ALERT i *Analysfs Notebook)* oraz zacieśnienie współpracy w zakresie zdalnego obiegu danych z Interpolem i Europolem.

Stopień przygotowania Polski do wdrożenia strategii rozwojowej *ePolska* został przedstawiony w raporcie o implementacji programu *eEuropa+,* podczas konferencji, zorganizowanej w Ljubljanie w czerwcu 2002 roku[284]. Przedstawiono tam zarówno raport z listopada 2000 roku, jak również założenia strategii na lata 2001-2006, a zaprezentowany poziom zaawansowania spotkał się z aprobatą władz Unii Europejskiej.

3.3.2. Bariery i zagrożenia realizacji postulowanego modelu rozwoju infrastruktury telekomunikacyjnej ze strony zasad regulacji rynku telekomunikacyjnego

Utworzenie nowymi dyrektywami wspólnych ram regulacyjnych dla całego sektora komunikacji elektronicznej, w tym sektora audiowizualnego może mieć znaczenie, także dla kształtu lub podziału kompetencji pomiędzy tradycyjnie ukształtowane organy regulacyjne sektora telekomunikacyjnego i medialnego.

Przygotowując, zatem nowe regulacje, należy - podobnie jak w nowych

---

[282]Tamże, s. 17.
[283]Tamże, s. 46-47.
[284]*Pierwszy raport o postępach we wdrażaniu eEurope+ w krajach kandydujących,* Ljubljana 2002; [URL-http://www.kbn.gov.pl/cete/ljubtjana/progress_pl.rtf].

eEurope+.

Jednocześnie podkreślano, że plan działania *eEurope+* jest ofertą fakultatywną i nie będzie krajom tym narzucany, powinien natomiast korelować z narodowymi inicjatywami, do których należy *ePolska.* W programie *ePolska,* autoryzowanym przez Ministerstwo Łączności, przedstawiono w czerwcu 2001 roku plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce[281]. Program obejmuje pięcioletni okres zmian, które nastąpią w wielu sektorach gospodarki pod patronatem rządu. Rozdziały dokumentu odpowiadają realizacji proponowanych przez Sejm i KBN obszarów implementacji społeczeństwa informacyjnego: rozwojowi infrastruktury telekomunikacyjnej, szybkiej, powszechnej internetyzacji, programom edukacyjnym adresowanym do pracowników, wykorzystaniu Internetu w administracji, sądownictwie i policji, ochronie zdrowia, opiece społecznej, w transporcie. Informacje o ogólnej koncepcji bezpieczeństwa informacyjnego zawarto w rozdziale pt. *„Bezpieczeństwo sieci".* Wymieniono tu nowe rodzaje przestępstw: przestępstwa przeciwko poufności, integralności i dostępności danych oraz systemów. Zwraca się uwagę na wysokie koszty zaproponowanych zabezpieczeń oraz spowolnienie pracy systemów informacyjnych, dlatego też sugerowane jest zróżnicowanie technik bezpieczeństwa, pozostawiające sektorowi prywatnemu swobodę w ich doborze.

Wymienia się także instytucje działające na rzecz bezpieczeństwa informacyjnego, systematyzując ich obszary kompetencyjne. Zespół powstały w Wydziale ds. Przestępczości Gospodarczej Biura Koordynacji Służby Kryminalnej Komendy Głównej Policji zajmuje się od 1998 roku zwalczaniem cyberprzestępczości oraz koordynacją operacyjną w tym zakresie. CERT Polska, działający od 1996 roku, monitoruje i rejestruje zdarzenia naruszające bezpieczeństwo sieci. Powyższe struktury realizować mają następujące cele: podnosić stopień bezpieczeństwa sieci i dostępu do usług elektronicznych, nie ograniczać wolności wyboru zabezpieczeń przez podmioty prywatne, pogłębiać konwergencję zabezpieczeń w różnych rodzajach mediów, inspirować i wdrażać

---

[281] *Por. ePolska. Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*, Ministerstwo Łączności, Warszawa 2001.

Ponadto rozstrzygnięcia wymaga wprowadzenie i stosowanie pojęcia wspólnej pozycji rynkowej (dopuszczalnego na gruncie obowiązującej ustawy o ochronie konkurencji i konsumentów, ale nie stosowanego obecnie przez regulatora), przeniesienia pozycji na inny rynek oraz dostosowanie pojęcia pozycji znaczącej do znaczenia nadawanego mu w nowych dyrektywach UE.

Jedną z najważniejszych kwestii jest sposób stosowania takich regulacji wobec operatorów nowo wchodzących, którym przedwczesne zastosowanie regulacji może wyrządzić znaczne szkody, uniemożliwiając ich dalszy rozwój. Analiza rynku, stosowana w nowej rzeczywistości regulacyjnej, musi odbywać się na zasadach analizy antymonopolowej, co wymaga bardzo zaawansowanych umiejętności od pracowników regulatora.

Mechanizmy zapewnienia *usług powszechnych,* które nie będą antykonkurencyjne, to takie mechanizmy, które umożliwiają racjonalizację obowiązku zapewniania usługi powszechnej w trzech kierunkach:

- nakładanie tego obowiązku na operatora zdolnego do jego poniesienia;
- kontrola kosztów jego wykonania i w przypadku ich nadmierności - rekompensata tych kosztów;
- budowa mechanizmów rekompensaty w taki sposób, aby jak najszerzej rozłożyć i zminimalizować indywidualne obciążenia (np. przez podatek VAT).

Wdrożenie tych mechanizmów wymaga szczegółowej analizy polskiego rynku telekomunikacyjnego (z jego specyfiką związaną z niską gęstością telefoniczną), a w szczególności wzmocnienia kompetencji regulatora w zakresie kontroli kosztów operatora. Najpilniejszym jednak jest określenie polityki rządu w usłudze powszechnej, tj. jej zakresu podmiotowego (uprawnieni i zobowiązani), przedmiotowego (usługi) oraz możliwości finansowania z budżetu państwa lub dopuszczalnego poziomu obciążeń nakładanych na przedsiębiorców.

Struktura oraz podział *zadań i kompetencji organów regulacyjnych* (URTiP, KRRiTV oraz UOKiK) są ściśle związane z nowymi wymaganiami regulacyjnymi. W krajach UE stosowane są różne rozwiązania, a dyrektywa nie formułuje pod tym względem wymagań innych niż efektywność działania. Kwestia ta - przekładająca

dyrektywach - rozdzielić regulacje dotyczące przekazywania informacji od regulacji dotyczących przekazywanych treści, z rozpoznaniem takich powiązań między nimi, które mogą być potencjalnym zagrożeniem dla konkurencji. Ponadto, w zakresie radiofonii i telewizji trzeba w sposób wyważony rozwiązać kwestię, w jaki sposób najlepiej wpisać rozpowszechnianie publiczne w nowe otoczenie, a przede wszystkim wymagać od takich nadawców wyraźnego rozgraniczenia między określoną działalnością związaną z nadawaniem publicznym a działalnością w sferze poddanej konkurencji.

Ważną kwestią pakietu nowego porządku regulacyjnego na rynku telekomunikacyjnym musi się stać zmiana zasad jego regulacji.

Oznacza to potrzebę uwzględnienia w pracach nad nowymi regulacjami roli prawa antymonopolowego oraz organu Urzędu Ochrony Konkurencji i Konsumentów (UOKiK). Podobnie jak w nowych dyrektywach, jego znaczenie winno rosnąć w miarę stopniowego odchodzenia od regulacji sektorowych wraz ze wzrostem konkurencji na rynku. Wymaga to określenia zasad współpracy z organem antymonopolowym. Rozwiązania wymaga problem implementowania do prawa krajowego tzw. klauzul wygaszających.

Organ regulacyjny, który uprawniony jest w nowych dyrektywach do określenia w miarę potrzeby znacznie węższych rynków, musi zostać wyposażony w daleko idące kompetencje stanowiące, pozwalające na decydowanie o stosowaniu poszczególnych przepisów prawa i zmianie zakresu podmiotowego poszczególnych regulacji. Polskie ustawodawstwo z zamkniętym systemem źródeł prawa, ściśle określonymi kompetencjami organów administracji i ustawowymi podstawami tych kompetencji bardzo słabo reaguje na potrzeby regulacji stale zmieniającego się rynku. Tymczasem elastyczności wymagają także regulacje prokonsumenckie, które na gruncie nowych dyrektyw upoważniają regulatora do decydowania, czy interes konsumentów wymaga w danym momencie objęcia regulacją podmiotów pozostawionych zwykle poza jej granicami (nie mających znaczącej pozycji rynkowej). Z drugiej strony, obowiązki operatorów będą teraz ściślej związane z wąskimi rynkami, na których operatorzy mają taką pozycję, a sam zakres obowiązków może zostać dopasowany do potrzeb danej sytuacji regulacyjnej.

w kontekście nowych celów UE ujawniają się bariery: *finansowanie inwestycji, uwolnienie pętli lokalne, udostępnianie elementów infrastruktury innym operatorom.*

Pakiet regulacyjny łączności elektronicznej nie odpowiada na pytanie o *finansowanie* i środki zmierzające do zwiększenia gęstości telekomunikacyjnej oraz budowy infrastruktury w krajach takich, jak Polska. Potrzeby dużych inwestycji na obszarach wiejskich wraz z finansowaniem dostarczania usług przy niskiej rentowności takiej działalności nie zaspokoi fundusz usługi powszechnej, gdyż jego oddziaływanie na rynek przy potrzebnej skali inwestycji mogłoby znacznie zniekształcać konkurencję.

Zalecenie UE, żeby stosując podobne źródła finansowania, związane z usługą powszechną, w maksymalnym stopniu zminimalizować dolegliwość dla operatorów i negatywne oddziaływanie na rynek, mogą zostać częściowo spełnione przez rozwiązania specjalne, rozkładające obciążenia na jak największą liczbę uczestników lub przeciwnie, obciążające wyłącznie budżety publiczne, (co w sytuacji Polski nie jest możliwe). Przykładowo, podczas przygotowywania nowych dyrektyw rozpatrywano możliwość finansowania usługi powszechnej z takich źródeł, jak VAT. Drugim, istotnym źródłem zwiększania gęstości mogłyby być środki pochodzące z funduszy strukturalnych UE.

Wątpliwości budzą obowiązujące zasady i spodziewane efekty *uwolnienia pętli lokalnej*. W warunkach uwolnienia pętli lokalnej operator zasiedziały poddany temu wymaganiu ma mniej bodźców do dalszej rozbudowy sieci dostępowej (o ile nie jest zmuszony do tego działaniami regulacyjnymi), ponieważ zwrot z inwestycji w specyficzny sposób także podlega temu uwolnieniu - operator infrastruktury dostępowej musi się nim dzielić z korzystającymi z jego uwolnionej linii. Podobne zahamowania występują w obszarze innowacji technicznych. Zwrot z nowej technologii może być zmniejszony przez zdolność do przechwytywania przejściowej renty monopolu, z której można skorzystać, wprowadzając różnego rodzaju innowacje na własnych liniach, bez wpuszczania na nie konkurencji.

Warto też zdać sobie sprawę, że w przypadku realizacji specjalnych programów skierowanych na zwiększenie gęstości linii stacjonarnych, a szczególnie przy nakładaniu obowiązków w zakresie usługi powszechnej na operatora

się na zagadnienie liczby organów i ich kompetencji, a także liczby ustaw, które będą wykonywane, wymaga jednak decyzji politycznej.

Nowe dyrektywy przynoszą zupełnie nowe i znacznie szersze niż dotąd formy nadzoru Komisji Europejskiej nad krajowymi organami regulacyjnymi. Będzie to wymagało ustanowienia zupełnie nowych procedur wewnątrz administracyjnych. Przedsięwzięcie to będzie trafiało na *bariery wdrażania pakietu regulacyjnego.* Do podstawowych barier we wdrażaniu nowego porządku należy zaliczyć:

- brak odpowiednich kadr w administracji; dotychczasowa administracja sektorowa od strony kompetencji, struktury i umiejętności nie jest przygotowana ani do implementacji nowego porządku prawnego do systemu prawa ani do jego wdrożenia. Przygotowanie administracji nie pozwala nawet na efektywne wdrożenie obecnej ustawy. Wynika to z niedofinansowania administracji, braku szkoleń, braku doświadczonych specjalistów. Problemem jest też głęboka zależność polityczna, powodująca okresowe załamania struktur i procedur;
- zamknięty system źródeł prawa, uniemożliwiający elastyczne reagowanie właściwe regulatorowi i powoływanie się na generalne klauzule ustawowe-, temat ten poruszono wyżej. Problematyka ta związana jest z konstytucyjnym systemem źródeł prawa oraz usytuowaniem organów regulacyjnych;
- niedostateczny rozwój infrastruktury telekomunikacyjnej, powodujący wiele skutków ubocznych, a wśród nich: konieczność ustalenia mechanizmów zapewnienia usługi powszechnej, zastępcze utrzymywanie antykonkurencyjnych mechanizmów finansowania deficytu dostępu, blokowanie regulacji związanych z uwolnieniem pętli lokalnej;
- techniczny stan sieci, uniemożliwiający pełne wdrożenie pakietu z lat 1990-2000 (liberalizacja rynku usług międzynarodowych, zapewnienie wymagań dotyczących dostępu do sieci i współpracy międzyoperatorskiej w zakresie budowy punktów styku, wyboru operatora, przenoszalności numerów).

Natomiast w zakresie polskiej polityki w sektorze telekomunikacji

okresów przejściowych. Dla określenia ram czasowych procesu harmonizacji i implementacji prawa wspólnotowego, jako datę gotowości do członkostwa w Unii Europejskiej przyjęto datę 31 grudnia 2002 r., co dotyczyło dyrektyw wydanych do 2000 r. Implementacja prawa UE w *Prawie telekomunikacyjnym* z 21 lipca 2000 r. okazała się jednak nie w pełni prawidłowa i efektywna. Dlatego przygotowano i skierowano do Sejmu RP projekt nowelizacji ustawy, sformułowany w duchu obowiązujących obecnie dyrektyw UE z lat 1990-2000. Znowelizowane *Prawo telekomunikacyjne* obowiązuje już od 16 lipca 2004 r. i po tym terminie zostało uzupełnione systemem rozporządzeń wykonawczych, które również powinny odpowiadać obowiązującym regulacjom unijnym.

Pomimo wielkich nadziei, jakie środowisko wiąże ze znowelizowaną ustawą, budzi ona jednak wciąż wiele wątpliwości. Przykładowo, nie jest jasne, dlaczego w przypadku sprzeciwu ABW lub AW do zgłoszenia działalności telekomunikacyjnej uzasadnienia do tego sprzeciwu nie sporządza się, a do zezwolenia - tak. Znaczna część działalności operatorów niezależnych odbywa się na podstawie zgłoszenia. Może to spowodować także nieuzasadnioną nierówność traktowania operatorów działających na podstawie zgłoszenia, w porównaniu z operatorami działającymi na podstawie zezwolenia.

Pomimo tego, prezes Urzędu Regulacji Telekomunikacji i Poczty w porozumieniu z prezesem Urzędu Ochrony Konkurencji i Konsumentów ustalił w drodze decyzji operatorów o pozycji dominującej i o znaczącej pozycji rynkowej zakresy świadczenia usług telekomunikacyjnych określonych w art. 57 ustawy *Prawo telekomunikacyjne*. Zgodnie z tymi decyzjami, Telekomunikacja Polska SA zajmuje pozycję dominującą na krajowym rynku świadczenia usług powszechnych oraz na krajowym rynku świadczenia usług dzierżawy łączy telekomunikacyjnych. Jest ona natomiast operatorem o znaczącej pozycji w zakresie usług świadczonych na krajowym rynku połączeń międzyoperatorskich. Polkomtel, Polska Telefonia Cyfrowa oraz Polska Telefonia Komórkowa Centertel są operatorami o znaczącej pozycji w zakresie świadczenia usług telefonicznych, świadczonych w ruchomych publicznych sieciach telefonicznych na obszarze Rzeczpospolitej Polskiej.

Stałe i niezmienne od dłuższego czasu uwagi dotyczące nieadekwatnego nakładania obowiązków w stosunku do rynku, na którym operator zajmuje pozycję,

zasiedziałego, nałożenie na niego nadmiernych obowiązków dotyczących uwolnienia pętli lokalnej stanowić może zbyt dużą uciążliwość i asymetrię obowiązków operatora znaczącego, stawiając pod znakiem zapytania ekonomiczną opłacalność jego inwestycji. W taki właśnie sposób zaowocowało wprowadzenie prawnego uwolnienia pętli lokalnej w większości krajów europejskich.

Uwolnienie pętli lokalnej nie zwiększy konkurencji w zakresie podstawowych usług głosowych ani też nie będzie sprzyjać rozwojowi infrastruktury dostępowej, na której Polsce szczególnie zależy. Korzyścią związaną z otwarciem pętli lokalnej jest natomiast możliwość świadczenia usług szerokopasmowych. Na te jednak usługi nie ma na razie zbyt wielkiego zapotrzebowania,

W kwestii *udostępniania innym operatorom pozostałych elementów infrastruktury telekomunikacyjnej,* takich jak kanalizacja techniczna, maszty, dachy i wieże, widać poważną potrzebę specjalnych rozwiązań, zobowiązujących operatora do budowy takiej infrastruktury z nadwyżką - a więc rozwiązań idących dalej niż regulacje Unii Europejskiej.

Zasady budowy tych elementów infrastruktury oraz ich udostępniania powinny być zgodne z interesem publicznym związanym z ochroną krajobrazu, środowiska, zasobów zabytkowych. Powinny też być zgodne z zasadą niedublowania zbędnych inwestycji. Operator powinien natomiast mieć prawo do należytego zwrotu poczynionych inwestycji. Wspierać należy również wszelkie inicjatywy budowy infrastruktury otwartej, np. przez jednostki samorządu lokalnego, co przyspieszyłoby znacznie proces inwestycyjny w telekomunikacji.

3.3.3. Bariery i zagrożenia realizacji postulowanego modelu rozwoju infrastruktury telekomunikacyjnej ze względu na kryteria kształtowania bezpieczeństwa ekonomicznego Polski

Stanowisko negocjacyjne Polski w obszarze „Telekomunikacja i technologie informacyjne" sformułowane na potrzeby naszych negocjacji z Unią Europejską zostało przyjęte przez Radę Ministrów w dniu 27 sierpnia 1998 r. i zmodyfikowane 13 kwietnia 1999 r. Polska zobowiązała się w nim do przyjęcia i wdrożenia całości prawa wspólnotowego w obszarze telekomunikacji i technologii informacyjnych do końca 2002 r. i w trakcie negocjacji nie występowała z wnioskiem o ustanowienie

- rozporządzenie w sprawie współpracy i rozliczeń międzyoperatorskich *(interconnection.* art. 80); rozporządzenie to dotyczy także ramowych ofert interconnectowych oraz ofert unbundlingu operatora dominującego, a także innych ofert ramowych wskazanych w ustawie. Rozporządzenie jest kluczowe dla sporów w zakresie współpracy międzyoperatorskiej i rozliczeń;
- rozporządzenie w sprawie systemów kalkulacji kosztów, bez którego nie można wprowadzić kontroli rachunkowości i systemów kosztowych (art. 59);
- rozporządzenie w sprawie uwolnienia pętli lokalnej (art. 87a);
- rozporządzenie w sprawie uprawnień abonentów (w tym wyboru operatora i przenoszalności numerów, art. 43).

W uzgodnieniach i konsultacjach środowiskowych były już wstępne projekty rozporządzeń:

- w sprawie współpracy międzyoperatorskiej (art. 81);
- w sprawie szczegółowych wymagań związanych z zapewnieniem dostępu do lokalnej pętli abonenckiej i związanych z nim udogodnień - art. 87a;
- w sprawie szczegółowych kryteriów ustalania udziału operatora w rynku usługi telekomunikacyjnej oraz sposobu określania, tego udziału, dzięki któremu możliwe było ustalenie pozycji rynkowej TP SA na rynku usług powszechnych i dzierżawy łączy - art. 57.

Jest także przygotowany wstępny projekt w sprawie kosztów i rachunkowości regulacyjnej - art. 59. Kilka niezbędnych aktów to akty wydane także do obecnie obowiązującej ustawy. Mogą one obowiązywać dzięki przepisom przejściowym utrzymującym je w mocy na 12 miesięcy. Są to na przykład:

- z dnia 22 grudnia 2000 r. w sprawie określenia wzoru wniosku o wydanie zezwolenia telekomunikacyjnego, trybu jego składania oraz rodzajów dokumentów wymaganych przy rozstrzyganiu wniosku;
- z dnia 22 grudnia 2000 r., w sprawie wysokości i terminów uiszczania opłat za wydanie zezwolenia telekomunikacyjnego;
- z dnia 7 czerwca 2001 r. w sprawie szczegółowego trybu sporządzania przez operatorów publicznych planu działań w sytuacjach szczególnych

dotyczą ciągle wszystkich przypadków, gdzie używa się enigmatycznego określenia „operator o znaczącej pozycji rynkowej" nie wskazując, na jakim rynku ta pozycja jest zajmowana, lub nakłada się obowiązki związane na przykład z rynkiem interconnection na operatora zajmującego pozycję na rynku dzierżawy łączy albo odwrotnie, nie nakłada się obowiązków na operatora, który na danym rynku zajmuje pozycję uzasadniającą nałożenie określonych zobowiązań.

Krokiem wstecz jest rezygnacja z jakiejkolwiek regulacji dostępu do sieci. W parlamencie skreślono art. 62, który nakładał na operatora znaczące obowiązki w zakresie udostępniania sieci operatorom działającym na podstawie zgłoszenia. Do ustawy nowelizującej wprowadzono także niezwykle obciążające dla operatorów niezależnych i na szczęście niewykonalne w praktyce przepisy dotyczące deficytu dostępu. Istnieje wiele poważnych argumentów oraz orzecznictwo UE potwierdzające sprzeczność tej instytucji z prawem UE. Przepisom o deficycie dostępu towarzyszy przepis dotyczący ustalania cen usług powszechnych w oparciu o benchmarki - niestety, jest on niekonstytucyjny, gdyż nie wymienia uprawnionego do ich ustalania. Ponadto nadal brak regulacji porządkujących współkorzystanie z nieruchomości oraz współkorzystanie z infrastruktury.

Wreszcie, szereg zastrzeżeń budzą przepisy dotyczące usługi powszechnej, której na podstawie tak brzmiących zapisów nadal nie uda się zapewnić ani wyegzekwować. Niektóre z nich, np. art. 54, wydają się przepisami martwymi.

Pozytywnymi elementami ustawy są: znowelizowany rozdział o współpracy międzyoperatorskiej, nowe przepisy o rachunkowości regulacyjnej i kalkulacji kosztów oraz nowe przepisy dotyczące wyboru operatora. Trudno ocenić natomiast przepisy dotyczące *unbundlingu* pętli lokalnej - prawdopodobnie nie będą one potrzebne, gdyż dostępowi operatora usług telefonicznych do abonenta znacznie lepiej służy NDS, a szerokopasmowy dostęp do Internetu wciąż nie należy do usług lawinowo rozwijających się.

W związku z uchwaleniem nowelizacji ustawy *Prawo telekomunikacyjne,* podjęto prace nad rozporządzeniami do tej ustawy, szczególnie, że większość materiałów pokrywa się z pracami toczącymi się nad rozporządzeniami do ustawy obecnie obowiązującej.

Najważniejsze, z brakujących do tej pory aktów wykonawczych to:

- dyrektywy o wspólnych ramach regulacyjnych dla sieci i usług komunikacji elektronicznej;
- dyrektywy o dostępie i połączeniach sieci;
- dyrektywy o autoryzowaniu sieci i usług komunikacji elektronicznej;
- dyrektywy o usłudze powszechnej i prawach użytkowników;
- dyrektywy o ochronie danych.

Celami nowego pakietu regulacyjnego są w szczególności:

- ostateczne ujednolicenie, harmonizacja i uproszczenie prawa komunikacji elektronicznej, integrującego w większym niż dotychczas stopniu sektory telekomunikacji, teleinformatyki i mediów;
- usunięcie pozostałych barier rozwoju sektora;
- zapewnienie, by użytkownicy osiągali maksimum korzyści co do wyboru, ceny, jakości i stosunku wartości do ceny;
- zapewnienie, by nie występowały zniekształcenia bądź ograniczenia konkurencji w sektorze komunikacji elektronicznej;
- tworzenie zachęt do efektywnego inwestowania w infrastrukturę;
- zapewnienie efektywnej alokacji częstotliwości radiowych;
- stworzenie podstaw dla rozwoju komunikacji elektronicznej jako bazy rozwoju społeczeństwa informacyjnego.

Jest pięć ważnych cech charakterystycznych systemu prawa wprowadzonego w nowych dyrektywach:

- konsument jako wartość i cel nadrzędny;
- zreformowanie ostatnich instytucji prawnych mogących negatywnie oddziaływać na rozwój konkurencji, jak np. mechanizmy finansowania usługi powszechnej;
- uznanie stanu konkurencyjności niektórych segmentów rynku za znajdujący się na poziomie usprawiedliwiającym stopniowe wycofywanie się z poszczególnych regulacji *ex ante* na rzecz prawa konkurencji i wiążąca się z tym zmiana treści pojęcia pozycji znaczącej;
- wprowadzenie pojęcia dostępu do sieci jako pojęcia nadrzędnego nad interconnection i doprowadzenie w ten sposób do objęcia prawem wykorzystywania sieci operatora znaczącego przez wszystkich

zagrożeń oraz jego aktualizacji;

- z dnia 18 czerwca 2001 r. w sprawie wysokości, terminów i sposobu uiszczania opłat za prawo do wykorzystywania zasobów numeracji oraz opłat za posiadanie zezwolenia telekomunikacyjnego;
- z dnia 5 września 2002 r. w sprawie planu numeracji krajowej dla publicznych sieci telefonicznych, bardzo istotne dla nowych sieci i usług, w szczególności dla liberalizacji usług dostępu do operatorów komórkowych;
- z 19 grudnia 2002 r. w sprawie warunków świadczenia usług powszechnych;
- z 31 grudnia 2002 r. w sprawie usług dzierżawy łączy telekomunikacyjnych.

Z dniem 1 stycznia 1998 roku nastąpiło formalne otwarcie europejskiego rynku telekomunikacyjnego, do którego kraje członkowskie UE przygotowywały się od 1990 r. Na przestrzeni lat 1990-1998 wydanych zostało kilkanaście istotnych dyrektyw, które otwierały poszczególne segmenty rynku, najpierw ostrożnie, a potem bardzo zdecydowanie. Prawdziwym przełomem stały się dyrektywy wydane po 1996 r., które określiły datę i zasady pełnego otwarcia. Cechą systemu regulacyjnego w latach 1996-2001 była silna regulacja *ex ante* (czyli uprzednia), poddających kontroli regulatora wszelkie zachowania zasiedziałych operatorów poprzez nałożenie na nich ściśle określonych i konsekwentnie egzekwowanych obowiązków oraz związanie tych obowiązków ze znaczącą pozycją rynkową operatorów.

Już jednak w 1999 r. (a więc po roku od otwarcia) Komisja podjęła w tzw. *1999 EU Review* problem, czy stopień rozwoju konkurencji na poszczególnych rynkach telekomunikacyjnych uzasadnia zmianę podejścia regulacyjnego. Stwierdzenie konkurencyjności rynku pozwoliłoby na stopniowe wycofywanie się z regulacji *ex ante* i specyficznej sektorowej regulacji zagadnienia siły rynkowej oraz zastąpienie ich narzędziami regulacji antymonopolowej.

W 2002 roku Unia Europejska zaprezentowała pakiet dyrektyw nowego podejścia, składający się z pięciu projektów:

- sprzęt i standaryzacja jako warunki zapewnienia otwartego dostępu użytkowników do usług konkurencyjnych operatorów (zadania regulatora telekomunikacyjnego i KRRiTV) oraz wolnego przepływu informacji, pluralizmu medialnego i różnorodności kulturowej (zadania KRRiTV);
- stworzenie systemu zezwoleń obejmującego wszystkie sieci i usługi w podobny sposób;
- powszechnie obowiązujące zasady otwartych, jawnych i niedyskryminacyjnych procedur (w szczególnych przypadkach - przetargów) przyznawania częstotliwości dotyczące także nadawców;
- ograniczenie do kwestii związanych z interesem publicznym i interesem użytkowników wymagań związanych z licencjonowaniem działalności w zakresie sieci i usług komunikacji elektronicznej, zmniejszenie zakresu swobody uznaniowej organu regulacyjnego, stosowanie zasad jawności, przejrzystości i niedyskryminacji, uproszczenie systemów przyznawania uprawnień ograniczające rolę organów regulacyjnych i likwidujące ostatecznie pozostałe bariery dostępu, z pozostawieniem ograniczeń dotyczących pewnych aspektów interesu publicznego, związanych z przekazywanymi treściami lub bezpieczeństwa państwa;
- kompatybilność urządzeń telewizji cyfrowej;
- obowiązek transmisji programów publicznych wraz z zasadami rekompensowania tego obowiązku;
- telewizja szerokoformatowa (Polska do tej pory nie implementowała przepisów dyrektywy 95/47/WE, z których wynikał obowiązek zapewnienia, by sieci cyfrowej łączności elektronicznej używane w rozpowszechnianiu usług telewizyjnych i publicznie dostępne mogły prowadzać dystrybucję usług i programów telewizji szerokiego ekranu, tak by użytkownicy mieli możliwość odbierania takich programów w formacie, w jakim zostały one przetransmitowane. Zgodnie z art. 4 nowej dyrektywy o dostępie: „Publiczne sieci łączności elektronicznej ustanowione dla dystrybucji usług telewizji cyfrowej powinny być w stanie dystrybuować programy i usługi w formacie dużego ekranu.

operatorów i usługodawców działających w obszarze „komunikacji elektronicznej", przez co wybór dla użytkownika końcowego znacznie się poszerza;

- postawienie przez Komisję kropki nad „i" poprzez powtórzenie w sposób bardziej niż dotąd dobitny obowiązku państw członkowskich rezygnacji z ostatnich barier dostępu do rynku - w tym systemu licencji indywidualnych.

Minister Infrastruktury powołał zespół ekspertów, którzy mają pracować nad nowym prawem telekomunikacyjnym. Prace mają rozpocząć się na jesieni i otrzymać wsparcie ze środków Phare. Tymczasem Krajowa Rada Radiofonii i Telewizji realizuje program Phare przeznaczony na implementację pakietu nowych dyrektyw w kontekście sektora mediów. Jest on w istocie ***pakietem regulacyjnym problemów mediów w Polsce.***

Elementy nowego porządku regulacyjnego, które z punktu widzenia interesów Polski są najważniejsze, to:

- konwergencja[285] technologii i wynikające z niej wspólne rozwiązania regulacyjne dla telekomunikacji, mediów i teleinformatyki oraz włączenie do nowych dyrektyw rozwiązań specyficznych dla mediów;
- rozwiązania w zakresie regulacji *ex ante* i *ex post,* ściśle związane z określonym etapem rozwoju rynku (pozycja rynkowa i związane z nią obowiązki); przechodzenie na grunt prawa antymonopolowego;
- wspólna pozycja znacząca, przeniesienie pozycji na inne rynki;
- mechanizmy zapewnienia usług powszechnych, które nie będą antykonkurencyjne;
- struktura i podział zadań oraz kompetencji organów regulacyjnych (URTiP, KRRiTV);
- nadzór Komisji Europejskiej nad krajowymi organami regulacyjnymi.

Zupełnie nowym wyzwaniem dla Polski są zagadnienia konwergencji mediów elektronicznych, które są równoprawnym elementem pakietu nowych dyrektyw:

---

[285]Konwergencja – określenie procesów obejmujących kojarzenie zjawisk znajdujących się na pograniczu działów telekomunikacji, informatyki i multimediów.

ZAKOŃCZENIE

Zmiany, jakie dokonały się w dekadach przełomu XX i XXI wieku w Polsce oraz w międzynarodowym otoczeniu naszego kraju wywarły znaczący wpływ na problematykę bezpieczeństwa państwa, a szczególnie na kształt bezpieczeństwa ekonomicznego. Przeprowadzone w rozprawie analizy wskazują, że dylematem naszego kraju pozostanie nie tylko zmiana wewnętrznych wzorów funkcjonowania, ale również rozpoznawanie i odpowiednie wykorzystanie doświadczeń innych krajów. Realizacja tych zamierzeń wyznaczana będzie przez procesy globalizacji i regionalizacji rozwojowej, powodującej konieczność poszukiwania przez nasz kraj dalszych możliwości włączenia się do głównego nurtu zmian jakie zachodzą w wysoko rozwiniętych krajach Unii Europejskiej i Sojuszu Północnoatlantyckim przy ich udziale.

W kształtowaniu bezpieczeństwa ekonomicznego znacząca rola przypada telekomunikacji, a za jej sprawą infrastruktury telekomunikacyjnej. Pełnienie takiej roli ma liczne związki z jej rozwojem społeczeństwa informacyjnego, które to poprzez dostępność do gromadzenia, przetwarzania, przesyłania i wykorzystania informacji, które to osiągnęło już taki stopień, iż telekomunikacja, a wraz z nią infrastruktura telekomunikacyjna staje się jednym z immanentnych wskaźników rozwoju bądź zacofania cywilizacyjnego. Dowiodły tego podjęte i przeprowadzone w rozprawie dociekania w kwestii infrastruktury telekomunikacyjnej jako elementu kształtowania bezpieczeństwa ekonomicznego Polski na przełomie XX-XXI wieku. Upoważniają one jednocześnie do sformułowania szeregu wniosków.

Pierwszy. Podstawowym celem polityki Polski jest zapewnienie szeroko rozumianego bezpieczeństwa. Stanowi to bowiem warunek jego rozwoju w wymiarze społecznym i gospodarczym. W praktyce wyrażana jest ona w dążeniu do utrzymania suwerenności i nienaruszalności granic RP oraz w rozwijaniu jej potencjału gospodarczego, a w konsekwencji kształtowania bezpieczeństwa ekonomicznego. Postrzegać trzeba je jako taki stan rozwoju krajowego systemu gospodarczego, który zapewnia wysoką sprawność jego funkcjonowania oraz zdolność do skutecznego przeciwstawienia się zewnętrznym naciskom mogącym doprowadzić do zaburzeń rozwojowych. Jest on istotną częścią, jednym z filarów

Operatorzy sieci, którzy odbierają i redystrybuują programy i usługi w formacie dużego ekranu, zachowają ten format.";

- obowiązek zapewnienia dostępu do sieci i usług medialnych na warunkach sprawiedliwych, rozsądnych i niedyskryminujących.

Konwergencja technologii i wynikające z niej wspólne rozwiązania regulacyjne dla telekomunikacji, mediów i teleinformatyki oraz włączenie do nowych dyrektyw rozwiązań specyficznych dla mediów, stanowią dla Polski szansę na rozwój nowoczesnych zintegrowanych usług komunikacyjnych. Zarazem jednak te zupełnie nowe wątki wymagają współpracy w procesie tworzenia prawa z Krajową Radą Radiofonii i Telewizji, jako właściwą i kompetentną w sprawach mediów.

bezpieczeństwa ekonomicznego przez perspektywę elementów tworzących i decydujących o jego poziomie oraz negatywną - sprowadzającą się do postrzegania bezpieczeństwa ekonomicznego z perspektywy istniejących, jak i zakładanych zagrożeń.

Realizacja obu opcji wymaga uwzględnienia uwarunkowań (wewnętrznych i zewnętrznych) jego kształtowania. W zbiorze uwarunkowań wewnętrznych polityki bezpieczeństwa państwa, dostrzec i wyróżnić trzeba przede wszystkim czynniki polityczne, ekonomiczne, społeczne itp., które mogą mieć zarówno charakter kreatywny, jak i destrukcyjny.

W tej grupie istotne znaczenie mają *uwarunkowania infrastrukturalne,* które znajdują odbicie we wszystkich grupach uwarunkowań. Ich wpływ na kształtowanie bezpieczeństwa ekonomicznego wyraża się współdecydowaniem: w wymiarze ekonomicznym o podzielności nakładów i ich zaangażowaniu; pracochłonności i kapitałochłonności przedsięwzięć, a także wpływie na kwestie zmian jakościowych; w wymiarze społecznym wyraża się to wspomaganiem działań administracji państwowej i samorządowej na rzecz zapewnienia odpowiedniej sytuacji prawno-ekonomicznej społeczeństwa; natomiast w wymiarze techniczno-organizacyjnym są one odpowiedzialne za zarządzanie i koordynowanie procesów kształtowania bezpieczeństwa ekonomicznego, a także kształtowanie cech niezbędnych do realizacji tych przedsięwzięć, tj. dużej mobilności, żywotności przestrzennej, jedności funkcjonalnej itd.

Czwarty. Do obszarów kształtowania i wzmacniania bezpieczeństwa ekonomicznego państwa coraz częściej zalicza się infrastrukturę telekomunikacyjną, określaną także jako infrastruktura teleinformatyczna, a obecnie coraz częściej (w dobie budowy społeczeństwa informacyjnego) jako informacyjna. Oczekuje się od niej operatywnego i niezawodnego zapewnienia łączności jako środka komunikacji i organizacji bytu społeczeństwa i zarządzania państwem – w tym gospodarką narodową. Spełnienie tych oczekiwań zależy od stanu infrastruktury telekomunikacyjnej (teleinformatycznej) na obszarze kraju, a także sprawności organizacyjno-technicznej funkcjonujących systemów łączności, ich jakości, przepustowości i niezawodności. Z tych też względów pozostaje ona w obszarze szerokiego zainteresowania publicznego i jest obszarem dynamicznego

bezpieczeństwa państwa, bowiem wartości w sferze ekonomicznej bardzo silnie wpływają na określenie racji stanu. Tworzy go taki poziom rozwoju gospodarczego (jednostki, państwa, organizacji itd.), który zapewnia mu harmonijny rozwój i efektywne wykorzystywanie szans i ograniczanie zagrożeń wypływających z otaczającego środowiska, które pozwoliłyby na trwanie i rozwój państwa (narodu). Jest ono także wypadkową wielu czynników, w tym: przyszłości – która to charakteryzuje się dużym stopniem niepewności i wysokim stopniem nieprzewidywalności; położenia i obszaru państwa oraz posiadanych zasobów naturalnych; rozwoju gospodarczego, naukowo-technicznego, kulturowego itp.; międzynarodowych powiązań gospodarczych; oraz płaszczyzn oddziałujących na kształt struktur państwa, tzn. społeczno-gospodarczej i wojenno-obronnej. Jako takie ujawnia się ono na dwóch płaszczyznach: społeczno - ekonomicznej (nazywanej także ogólnogospodarczą), i obronno-wojskowej.

Drugi. Osiągnięcie pożądanego poziomu bezpieczeństwa ekonomicznego państwa, wymaga skorelowana ze sobą szeregu elementów, przede wszystkim zaś: poziomu kierowania (zarządzania) państwem, który będąc jednym z motorów napędowych rozwoju gospodarki narodowej, przyczyniłby się do osiągania pożądanego poziomu dobrobytu jednostki; rozwoju gospodarczego zapewniającego trwanie i rozwój państwa (narodu); wielokierunkowy system przepływu informacji między wszelkimi sferami życia podmiotu i otaczającym go środowiskiem; systemu wykrywania i likwidowania lub zmniejszania niekorzystnych skutków zagrożeń, zarówno zewnętrznych, jak i wewnętrznych. Jego osiągnięcie może przebiegać dwiema drogami: pierwszą, która polega na tym, że bezpieczeństwo ekonomiczne byłoby kształtowane przez wzrost własnej siły ekonomicznej w stosunku do innych państw, co może powodować narastanie szeregu sytuacji kryzysowych w stosunkach międzynarodowych; drugą - która w swych założeniach sprowadza się do tworzenia między państwami (ugrupowaniami państw) szeregu powiązań, wytworzenia szerokiej współpracy, co w konsekwencji może okazać się korzystne do stymulowania relacji dwu- i wielostronnych przez budowę głębokich powiązań gospodarczych.

Trzeci. Kreacja bezpieczeństwa ekonomicznego państwa może być dokonywana opierając się na opcji pozytywnej - wyrażającej się postrzeganiem

telekomunikacyjnej. Problemem aktualnym jest, także ciągle wspomniana różnica pomiędzy telefonizacją obszarów miejskich i wiejskich. Jest on znaczący przede wszystkim ze względu na małą aktywność gospodarczą polskiej wsi co powoduje, że podłączanie abonentów wiejskich jest mało opłacalne ekonomicznie i mało który z operatorów decyduje się na rozwój swojej sieci na obszarach wiejskich. Tymczasem większość przyznawanych koncesji obliguje operatorów do inwestowania zarówno na obszarach miejskich jak i wiejskich. Mimo wyraźnie widocznego postępu technologicznego i ilościowego, nadal są regiony, w których jest utrudniony dostęp do telefonów stacjonarnych. Wydaje się, iż przyszłość telefonii jest w znacznym stopniu zdeterminowana rozwojem telefonii komórkowej. Nowym zjawiskiem z tego obszaru jest pojawienie na rynku telefonii stacjonarnej firm prywatnych. Należy się spodziewać, iż presja konkurencji pomiędzy dotychczasowym monopolistą a firmami prywatnymi z jednej strony, a z drugiej pomiędzy siecią stacjonarną i komórkową, przyczyni się do powstania rozwiązań jakościowo nowych w obszarze technologicznym, a przede wszystkim szerokiej gamy tanich usług.

Siódmy. Infrastruktura telekomunikacyjna państwa będąc elementem systemu informacyjnego państwa postrzeganego jako zorganizowany kompleks technicznych środków łączności, spełniający określone funkcje i realizujące postawione cele oraz obsługująca go kadra, ściśle wiąże się ze skutecznością systemu kierowania i zarządzania państwem, sterowania gospodarką narodowa, dowodzenia siłami zbrojnymi oraz funkcjonowania organów bezpieczeństwa publicznego jest uzależniona od niezawodnie i efektywnie funkcjonującego systemu informacyjnego - łączności państwa. Zdolność wykonania tych zadań zależy w dużym stopniu od stanu rozbudowy infrastruktury systemu telekomunikacyjnego na obszarze całego kraju i jego sprawności organizacyjno-technicznej funkcjonujących systemów, ich jakości, przepustowości i niezawodności. Tworzą go: obiekty i linie telekomunikacyjne (kablowe, światłowodowe, radiowe, a nawet jeszcze napowietrzne) obiekty teletransmisyjne (stacje wzmacniakowe, przełączalnie) i radiokomunikacyjne (łączności radiowej i radiofonicznej, radiofonii oraz telewizji), a także naziemne stacje łączności satelitarnej. Linie łączności przebiegają ze wschodu na zachód, a rokady

rozwoju. Stała się ona jednym z ważniejszych czynników rozwoju życia społecznego, gospodarczego i kulturalnego. Ułatwia ona generowane przez społeczeństwo procesów informacyjnych oraz stymuluje rozwój i ewolucję systemów telekomunikacyjnych. Sytuacja ta jest funkcją wzrostu znaczenia informacji we wszystkich obszarach i płaszczyznach ludzkiej działalności.

Piąty. W rzeczywistości społecznej, politycznej, gospodarczej, a także militarnej, zmianom ulega samo pojęcie telekomunikacji. Kojarzy się ono dzisiaj nie tylko z zarządzaniem siecią, a przede wszystkim z dynamicznym rozwojem różnorodnych usług telekomunikacyjnych i informatycznych. Stopień jej doskonałości organizacyjnej uzewnętrznia infrastruktura telekomunikacyjna. Jej rozwój staje się jednym z podstawowych przedsięwzięć stanowiących wkład w przyszłe społeczeństwo informacyjne. Jego fundamentem jest zaś coraz powszechniejszy dostęp do technik informacyjnych, telekomunikacyjnych, informatycznych i mediów elektronicznych, które to stają się głównymi stymulatorami współczesnych przemian gospodarczych, społecznych i kulturowych.

Szósty. Funkcjonujący w naszym kraju system infrastruktury telekomunikacyjnej nie jest spójny Jest on podzielony na szereg podsystemów, np. sieci użytku publicznego, sieci resortowe, sieci zakładowe i inne, co stwarza znaczne utrudnienia w obiegu informacji, szczególnie w sytuacjach wykorzystania systemu łączności na potrzeby kierowania i zarządzania państwem, zarówno w czasie pokoju, jak i w warunkach zaistnienia potencjalnych zagrożeń. Sieci telekomunikacyjne poszczególnych resortów lub instytucji centralnych budowane są własnymi środkami, co powoduje, iż często się one dublują i opierają na różnych rozwiązaniach technicznych. Nie sprzyja to osiąganiu zakładanych celów, lecz powoduje niewspółmierny wzrost nakładów finansowych z budżetu państwa. Taki stan infrastruktury telekomunikacyjnej kraju negatywnie rzutuje nie tylko na kształtowanie bezpieczeństwa ekonomicznego kraju, ale również na realizację zadań obronnych stawianych przez naczelne organy władzy i administracji państwa, jak również na funkcjonalność całego systemu telekomunikacyjnego kraju. Mimo gwałtownego rozwoju telekomunikacji w ciągu ostatnich kilkunastu lat, Polska nadal pozostaje krajem o niezbyt dobrze rozwiniętej infrastrukturze

przekonfigurowanie systemu itp., nieumyślne spowodowanie dekonspiracji podsystemu zabezpieczenia poufności informacji);

- celowych oddziaływań (dywersji prowadzonej przez grupy zainteresowane zniszczeniem elementów systemu obronnego; próby programowego przekonfigurowania elementów sieci telekomunikacyjnych i komputerowych; próby ataku na system zabezpieczenia poufności informacji).

Oznacza to, że elementy systemu telekomunikacyjnego państwa poddawane są różnym destrukcyjnym oddziaływaniom o charakterze losowym, klęsk żywiołowych i ekologicznych. Natomiast oddziaływanie środków rażenia przeciwnika a tym samym zagrożenia, będą uzależnione od wagi celu i przestrzennego rozmieszczenia elementów systemu telekomunikacyjnego. Wynika z powyższego, że rozkład infrastruktury telekomunikacyjnej, a przede wszystkim węzłów i linii sieci powinien być bardzo nierównomierny, co spowoduje wzrost uodpornienia.

W trakcie zmian stanów gotowości obronnej państwa zacznie narastać stopień oddziaływań zewnętrznych dezorganizujących system łączności (np. niszczenie, rozpoznanie i obezwładnianie radioelektroniczne), który będzie maleć w czasie konfliktu wskutek wyczerpywania się potencjałów walczących stron. Prawdopodobieństwo największych zagrożeń w konfliktach lokalnych występuje przede wszystkim w rejonach przygranicznych szczególnie na wschodnich obszarach kraju.

Funkcjonowanie systemu telekomunikacyjnego może również zostać zakłócone przez szereg barier i czynników takich jak: terroryzm, sabotaż, broń konwencjonalna, jądrowa, chemiczna i biologiczna, walka elektroniczna, katastrofy naturalne i ekologiczne.

Dziewiąty. W ostatnich latach nastąpił w Polsce gwałtowny rozwój infrastruktury telekomunikacyjnej. Sytuacja ta umożliwiła szerokie wykorzystywanie w procesach zarządzania i kierowania nowoczesnych technik przekazu i przetwarzania informacji.

Znaczenie obiegu informacji w instytucji państwowej, przedsiębiorstwie, organizacji militarnej, czy też koncernie działającym w sieci teleinformatycznej,

biegną z północy na południe. W punktach przecięcia tych linii znajdują się stacje wzmacniakowe bądź teletransmisyjne. Obecny stan telekomunikacji jest niezadowalający zarówno pod względem ilościowym, jak i jakościowym. Dowodzi tego niewłaściwa struktura organizacyjna przez zagęszczenia i rozrzedzenia linii telekomunikacyjnych w różnych regionach kraju, mała skuteczność ochrony i obrony przed zagrożeniami, szczególnie przed rozpoznaniem i obezwładnianiem, a zwłaszcza radioelektronicznym, duża różnorodność stosowanych technik i technologii. Obieg informacji oparty jest na sprzęcie, pochodzącym przede wszystkim z importu. Sieci łączności niektórych resortów i instytucji funkcjonują na podstawie różnych rozwiązań technicznych. Eksploatowany system łączności jest mało spójny i podzielony na zbyt wiele podsystemów resortowych, co nie zapewnia wymaganej koordynacji i kompatybilności systemowej. Stwarza to znaczne utrudnienia w przekazywaniu informacji, a zarazem naraża na niebezpieczeństwo utraty informacji, jak również powoduje duże niedogodności w organizowaniu łączności na potrzeby obronności i zapewnieniu bezpieczeństwa państwa. W zakresie zaś polskiej polityki w sektorze telekomunikacji w kontekście nowych celów UE ujawniają się bariery: finansowanie inwestycji, uwolnienie pętli lokalne, udostępnianie elementów infrastruktury innym operatorom.

Ósmy. W czasie pokoju elementy infrastruktury telekomunikacyjnej państwa mogą być niszczone (poza naturalnymi uszkodzeniami wynikającymi z niedoskonałości sprzętu) w wyniku:

- środowiskowych oddziaływań losowych (powodzi; katastroficznych zatopień; pożarów; trzęsień ziemi; tąpnięć; rozprzestrzenienia się przemysłowych środków trujących; eksplozji gazów lub pyłów; wyładowań atmosferycznych; uszkodzeń linii wysokiego napięcia, innych awarii zasilania itp.; fali uderzeniowej, impulsu elektromagnetycznego i promieniowania radioaktywnego będącego skutkiem katastrofy urządzeń jądrowych);
- niecelowych oddziaływań działań ludzkich (błędów użytkowników i personelu powodujących awarie, uszkodzenia, skasowania zbiorów,

W ślad za przedstawioną formułą wniosków celowym i pożądanym staje się wysnucie także szeregu postulatów.

W świetle zagrożeń występujących aktualnie i mogących mieć miejsce w bliższej i dalszej przyszłości, ogromnego znaczenia nabiera sprawa budowy i utrzymania *bezpieczeństwa ekonomicznego państwa.* To przedsięwzięcie zaś ściśle wiąże się z racjonalnym wykorzystaniem obok potencjału ludzkiego i gospodarczego również infrastruktury gospodarczej. W jej zaś obszarze dostrzec trzeba również *infrastrukturę telekomunikacyjną*, która to powinna zapewnić sprawne funkcjonowanie najwyższych organów władzy i administracji państwa w wykonywaniu zadań wiążących się z budową potencjału gospodarczego państwa, a w konsekwencji także kształtowania pożądanego stanu bezpieczeństwa ekonomicznego kraju. Sieć łączności państwa na potrzeby bezpieczeństwa państwa powinna być rozwinięta na bazie infrastruktury teleinformatycznej wykorzystującej węzły komutacyjne stacjonarne jak i polowe oraz powinna być powiązana z innymi systemami. Z kolei członkostwo Polski w Unii Europejskiej i w Sojuszu Północnoatlantyckim wymusza konieczność posiadania systemu telekomunikacyjnego, kompatybilnego z ich systemami.

Wobec sytuacji braku ścisłych ustaw i przepisów prawnych, które stanowiłyby podstawę efektywnej działalności sektora telekomunikacji we wszystkich resortach w zakresie wymiany informacji konieczne wydaje się podjęcie działań na rzecz zmiany istniejącego stanu rzeczy. Zachodzi, więc pilna konieczność poprawienia tego stanu rzeczy, ponieważ szybki rozwój usług telekomunikacyjnych i przekształcenie ich w system wielousługowy, nadaje telekomunikacji nową rolę w gospodarce i społeczeństwie. Wymaga tego także unowocześnienie sieci oraz instalacji do coraz to nowocześniejszych urządzeń teleinformatycznych, co z kolei rodzi konieczność poniesienia ogromnych kosztów. Inwestycje te z czasem zaczną generować niskie koszty eksploatacyjne. W ślad za tym, przy zwiększającym się zakresie i obszarze świadczonych usług; przez sieć teleinformatyczną, oczekiwać należy wzrostu efektywności organizacji i zarządzania, poszerzenie zakresu działania i obecności instytucji oraz

porównać można do znaczenia krwioobiegu w organizmie ludzkim. Każda organizacja dysponująca informacjami, wykorzystuje do ich przechowywania, przetwarzania i przesyłania systemy teleinformatyczne.

Pojawiło się szereg niebezpieczeństw, spowodowanych przejęciem kontroli nad informacją nie tylko przez nieuprawnione działanie w sieci teleinformatycznej jej użytkowników lub pojedyncze osoby, ale również przez zorganizowane grupy o nastawieniu antyspołecznym i antypaństwowym. Potencjalne możliwości nieuprawnionego działania w sieci teleinformatycznej jej użytkowników lub osób nie będących jej użytkownikami nazywane są zagrożeniami. Zagrożenia mogą występować przypadkowo lub być skutkiem działania celowego. Działania celowe, nazywane atakiem na system , mogą być realizowane bez aktywnego oddziaływania - atak pasywny lub z oddziaływaniem na system atak aktywny.

Dziesiąty. Określenie zasad funkcjonowania oraz obszaru oddziaływania postulowanego modelu kształtowania bezpieczeństwa ekonomicznego stwarza konieczność odwołania się do szeregu procedur. W procesie konstruowania modelu procedury postępowania będą rzutować na jego zakres, relacje zachodzące wewnątrz niego oraz produkt finalny, którym będzie zbiór postulatów. Wskazanym będzie określenie i ocena ogólnych uwarunkowań tworzenia postulatywnego modelu kształtowania bezpieczeństwa ekonomicznego.

Konstrukcja postulowanego modelu kształtowania bezpieczeństwa ekonomicznego jest czynnością wieloetapową, *w pierwszym etapie* sprowadza się do sformułowania najważniejszych uwarunkowań wynikających z funkcjonowania istniejących systemów wewnętrznych państwa, a także ich kształtu, jakiego nabierają pod wpływem układu zewnętrznego.

Drugim etapem będzie określenie realnych wymagań bezpieczeństwa ekonomicznego, jakie będą wynikały z powiązań o charakterze gospodarczym, politycznym i społecznym ze strategią obronną.

Natomiast *trzeci etap* budowy modelu będzie ukazywał, jakie wymagania generowane przez strategię obronną są podstawą dla prawidłowego funkcjonowania modelu.

Etapem końcowym będzie próba sformułowanie głównych założeń postulowanego modelu.

w wypadku uszkodzenia odcinka traktu powoduje skuteczne zabezpieczenie systemu przed brakiem łączności w wyniku uszkodzeń pojedynczych traktów czy podwęzłów.

Infrastruktura sieci teleinformatycznej kr*aju* powinna stanowić podstawę do budowy zintegrowanego systemu wymiany informacji pomiędzy różnymi grupami użytkowników jak i różnymi instytucjami czy urzędami. Pełna funkcjonalność systemu łączności wymaga zapewnienia użytkownikom możliwości korzystania z zasobów baz danych oraz ich uzupełniania, aktualizowania i przesyłania między sobą niezbędnych informacji. Oznacza to jednocześnie, że przyszłość ekonomiczną narodu, a rolę systemu informacyjnego i nowych technologii w inicjowaniu wzrostu gospodarczego należy widzieć jako zasadnicze filary w rozważaniach tradycyjnego bezpieczeństwa państwa. Gospodarkę państwa należy traktować jako pole bitwy, co jednocześnie oznacza, że narodowe bezpieczeństwo zależy od bezpieczeństwa ekonomicznego. Zadanie przygotowania bezpiecznej przyszłości państwa wymaga więc silnej gospodarki i zapewnienia wymaganej zdolności nie tylko sile militarnej ale i efektywności systemu informacyjnego. Oznacza to także, że szeroko rozumiana obronność państwa powinna być rozumiana w kategoriach prowadzenia biznesu. W kierowaniu państwem najwyższe organa władzy i administracji powinny postrzegać techniki i technologie informacyjne jako swoje nowe zbrojne ramię, i jako nowe założenie polityki bezpieczeństwa państwa które okraczyło już w XXI wiek.

Rozbudowa infrastruktury telekomunikacyjnej patrząc z punktu widzenia kształtowania i utrzymania bezpieczeństwa ekonomicznego państwa musi wiązać się także z:

- dostosowaniem regulacji prawnych do wymagań szybkiego postępu technologicznego i ery społeczeństwa informacyjnego;
- przygotowaniem społeczeństwa polskiego do wyzwań nowego rynku pracy i nowych metod pracy;
- dostosowanie gospodarki narodowej do wymagań globalnej gospodarki; stworzeniem przejrzystych i przyjaznych obywatelowi struktur administracji publicznej na miarę otwartego społeczeństwa

przedsiębiorstw na obszarze całego kraju jak i innych dotychczas niedostępnych regionach świata.

Ogromny postęp cywilizacyjny (nowe techniki i technologie telekomunikacyjne) generujący w ciągu ostatnich latach zmiany jakościowe spowodował, że w telekomunikacji istnieje pilna potrzeba nowego spojrzenia na system łączności w państwie i oparcie go na nowoczesnej infrastrukturze telekomunikacyjnej kraju. Dokonane analizy i oceny, zebrane opinie ekspertów, wnioski z dotychczasowej eksploatacji sieci teleinformatycznej jednoznacznie potwierdzają potrzebę modernizacji i rozbudowy istniejącej infrastruktury, celem zwiększenia zdolności i obszaru świadczonych usług. Potrzebę podjęcia tego rodzaju działań wymuszają także światowe trendy rozwoju sieci teleinformatycznych, generujące nowe koncepcje ich wykorzystania oraz inspirujące prowadzone prace normalizujące w tym obszarze. Chodzi bowiem o to, by usługi sieci teleinformatycznej bazujące na szeroko rozwiniętej infrastrukturze zwiększały efektywność i skuteczność, a szczególnie zapewniały bezpieczeństwo realizowanych połączeń i ochronę przesyłanych informacji przez organa administracji państwa, instytucje i urzędy, a także odbiorców biznesowych jak i indywidualnych.

System łączności państwa powinien opierać się na istniejącej infrastrukturze telekomunikacyjnej kraju i posiadać powiązania informacyjne między różnymi instytucjami, służbami itd. Ich sprawne funkcjonowanie jest w dużym stopniu zależne od jej odporności oraz właściwej wymiany informacji między instytucjami i służbami obsługującymi całą infrastrukturę. Dotyczy to przede wszystkim: straży pożarnej, policji, wojska, pogotowia (energetycznego, gazowego, ratunkowego), jak i służb sanitarnych, urzędów miejskich czy przedsiębiorstw komunikacyjnych. Zwiększenie odporności infrastruktury telekomunikacyjnej na zagrożenia można uzyskać przez: zmiany rozmieszczenia elementów sieci, rozproszenie sprzętu w miejscach największych zagrożeń; zastosowanie przedsięwzięć organizacyjno - technicznych w zależności od stopnia poszczególnych zagrożeń; zrealizowanie struktury telekomunikacyjnej powiązanych liniami łączności ze sobą węzłów, podwęzłów i automatyczne wybieranie drogi obejściowej dla połączenia

struktury stacjonarnej jak i do zabezpieczenia pracy doraźnie organizowanych stanowisk kierowania obroną państwa oraz mobilnych (polowych) stanowisk i punktów dowodzenia sił zbrojnych. Struktura systemu łączności powinna zagwarantować trwałość i niezawodność procesów informacyjnych. Powinna ona także spełniać szereg kryteriów, do których zalicza się wskaźniki jej oceny tj. terminowość, wierność i skrytość łączności, natomiast do kryteriów oceny systemu łączności zalicza się: gotowość obronną, przepustowość, mobilność, trwałość (tj. żywotność, odporność na zakłócenia i niezawodność) oraz bezpieczeństwo łączności. System łączności kierowania obronnością państwa obecnie realizowany jest głównie przy wykorzystaniu niehierarchicznego i hierarchicznego systemu łączności. Specyfiką systemu jest konieczność tworzenia bezpośrednich relacji łączności (kanałów) pomiędzy współpracującymi stanowiskami kierowania, a nawet i poszczególnymi miejscami pracy osób funkcyjnych.

Zapobieganie niedoskonałości infrastruktury telekomunikacyjnych kraju i jej poprawa powinna obejmować przedsięwzięcia o charakterze: organizacyjnym, inwestycyjnym i technicznym w sieci telekomunikacyjnej nie tylko użytku publicznego, ale również w sieciach operatorów niezależnych. Powinna być ona rozbudowywana stosownie do potrzeb wynikających z potrzeb bezpieczeństwa ekonomicznego kraju i maksymalnie odporna na oddziaływania zewnętrzne, zapewniać alternatywny wybór tras, różnorodną dystrybucję kanałów oraz zapewniać sprawowanie kontroli nad połączeniami przychodzącymi z zewnątrz do jego sieci, poprzez połączenia automatyczne i półautomatyczne. Konieczne w tej sytuacji staje się zobowiązanie poszczególnych ogniw gospodarczo-obronnych państwa już w czasie pokoju do realizacji związanych z tym zadań. Aby mogły one być realizowane wskazane jest:

- zweryfikowanie zbioru użytkowników i ruchu przez nich generowanego;
- zweryfikowanie i uzupełnienie wymagań technicznych na obiekty;
- ustalenie zasobów, które mogą być wykorzystywane z sieci TP S.A. i innych operatorów;
- opracowanie zasad rozpływu ruchu z uwzględnieniem właściwości elementów komutacyjnych i posiadanych zasobów sieci;

informacyjnego za pomocą narzędzi wykorzystujących technologie informacyjne i komunikacyjne;

- stworzenie warunków dla trwałego i zrównoważonego rozwoju regionalnego z uwzględnieniem nowoczesnych technik społeczeństwa informacyjnego;
- wzrostem innowacyjności gospodarki w celu poprawy jej konkurencyjności;
- zapewnieniem wsparcia dla gospodarki elektronicznej przez zaplecze naukowe w celu lepszego wykorzystania szans, jakie oferuje model społeczeństwa informacyjnego;
- podjęciem działań tworzących warunki do angażowania się samorządów w zwiększaniu liczby punktów dostępu do sieci; wspieranie inicjatyw rozwoju i budowy sieci amatorskich i prywatnych oraz stworzenie, przyjęcie i skuteczne egzekwowanie przepisów uniemożliwiających blokowanie budowy sieci.

W systemie łączności kierowania obronnością państwa w stanach nadzwyczajnych należy uwzględnić tendencje rozwojowe technik i systemów łączności, który będzie stanowić zintegrowany pod względem organizacyjnym i technicznym zespół węzłów, traktów i linii łączności, urządzeń kanałotwórczych i komutacyjnych stacjonarnych i polowych, jak również urządzeń końcowych zapewniających korzystanie z niezbędnych usług telekomunikacyjnych wszystkim organom i osobom funkcyjnym znajdującym się w strukturach kierowania i dowodzenia. Szczególne zagrożenia państwa a przede wszystkim stany nadzwyczajnych zagrożeń wymagają odpowiednio systemu łączności bazującego na organizowanie określonych węzłów, sieci łączności i linii łączności dla stacjonarnych i mobilnych (polowych) stanowisk kierowania i dowodzenia (prezydenta, premiera, ministrów urzędów centralnych i instytucji, wojewodów i innych. Oznacza to, że wcześniej powinny być przygotowane siły i środki umożliwiające zorganizowanie stanowisk kierowania i dowodzenia. W związku z tym należy przygotować infrastrukturę telekomunikacyjną określonych rejonów kraju i posiadać osobne, mobilne węzły łączności przeznaczone do uzupełnienia

- ustalenie i uzupełnienie wymagań technicznych na zastosowane w sieci obiekty i linie telekomunikacyjne;
- zastosowanie zasad rozpływu ruchu z uwzględnieniem właściwości elementów komutacyjnych i transportowych posiadanych zasobów sieci;
- przyjęcie zaprojektowanej dopuszczalnej struktury sieci z uwzględnieniem: wymagań użytkowników, natężenia i rozpływu ruchu oraz wskaźnika jakości obsługi;
- dokonanie badań symulacyjnych (lub analitycznych) niezawodności, trwałości i przepustowości newralgicznych fragmentów sieci telekomunikacyjnej.

Należy również prowadzić badania i działania w celu optymalizacji rozmieszczenia węzłów i podwęzłów w systemie łączności oraz zastosowanej przepływności traktów, uwzględniając przewidywane natężenie ruchu, rozmieszczenie abonentów i ich przemieszczanie - wymagane w sytuacjach stanów nadzwyczajnych. Realizacja organizowanego i docelowego systemu łączności powinna być poprzedzona badaniem modelu struktury powiązań jej węzłów.

System teleinformatyczny na potrzeby bezpieczeństwa państwa powinien spełniać także istotną funkcję w integracji z Organizacją Traktatu Północnoatlantyckiego. Zgodnie z wytycznymi NATO zawartymi w Kompendium Łączności Cywilnej, wszystkie kraje członkowskie traktują swoje urządzenia telekomunikacyjne, pracujące w sieciach krajowych i międzynarodowych, jako część ogólnego potencjału obronnego Sojuszu. Tym kierunkom postępowania sprzyjać powinny tendencje rozwojowe systemu teleinformatycznego, ukierunkowane na zapewnienie trzech podstawowych grup wymagań: trwałości - a więc zapewnienia odporności na zakłócenia, dużej niezawodności i żywotności, co wiąże się z budową sieci o strukturze siatkowej; skrytości - zapewnienia utajniania z wymaganą mocą kryptograficzną; mobilności – tzn. zachowania ciągłości łączności w czasie przemieszczania się stanowisk kierowania i dowodzenia. W ślad za tym pożądana infrastruktura telekomunikacyjna powinna umożliwiać przesyłanie informacji do korespondentów w sposób bezpieczny. Powinna ona spełniać wymagania najwyższych organów władzy, administracji

- zaprojektowanie dopuszczalnej struktury sieci z uwzględnieniem zweryfikowanych wymagań, rozpływu ruchu i wskaźnika jakości obsługi;
- w zbiorze dopuszczalnych struktur przeprowadzenie badań analitycznej niezawodności, trwałości i przepustowości, a na tej podstawie określić suboptymalną strukturę obiektu docelowego.

Budowa i eksploatacja sieci publicznych w czasie pokoju ma na celu nie tylko zapewnienie potrzeb komercyjno - usługowych, ale także wymagań okresu kryzysu i wojny, na przykład w zakresie jej żywotności i elastyczności. Biorąc pod uwagę wymagania obronne, możliwość technicznej realizacji oraz ograniczenia finansowe, należy w planowaniu budowy uwzględnić:

- wymagania w zakresie wielospójności węzłów i obiektów telekomunikacyjnych;
- zróżnicowany przebieg tras kablowych i mikrofalowych pomiędzy regionami państwa i państwami, dokonywaniu obejść strategicznych obiektów narażonych na zniszczenie w pierwszej kolejności;
- przygotowanie możliwości dynamicznej zmiany przepustowości określonych relacji łączności poprzez planowanie odpowiedniej nadmiarowości przepływności oraz określenie priorytetu w ruchu i czasu dostępu do sieci;
- zorganizowaniu ciągłego nadzoru nad poszczególnymi częściami sieci; oraz odpowiedniego systemu sprawozdawczości i bezpiecznej sieci łączności dyspozytorskiej.

Patrząc z punktu widzenia kształtowania i utrzymania bezpieczeństwa państwa, budowa infrastruktury telekomunikacyjnej, powinna uwzględniać algorytm postępowania zakładający:

- określenie zbioru użytkowników i ruchu przez nich generowanego w infrastrukturze telekomunikacyjnej;
- uwzględnienie sieciowych zasobów krajowych, regionalnych i lokalnych operatorów, które mogą być wykorzystane w sieci telekomunikacyjnej państwa;

BIBLIOGRAFIA

A. Pozycje zwarte

1. Adamczewski P., *Zintegrowane systemy informatyczne*, ZNI MIKOM, Warszawa 1998.
2. Alberts D. S., Garstka J. J., Stein F. P., *Network Centric Warfare. Developing and Leveraging Information Superiority*, National Defense University Press, Washington 2000.
3. Alberts D. S., Garstka J. J., Hayes R. E., Signori D A., *Understanding Information Age Warfare*, National Defense University Press, Washington 2001.
4. *Analogowe systemy teletransmisyjne*, Praca zbiorowa pod kierunkiem Włodzimierza Barjasza, WKiŁ, Warszawa 1979.
5. Balcerowicz B., *Obronność państwa średniego*, Bellona, Warszawa 1997.
6. Balcerowicz B., *Pokój i „nie-pokój" na progu XXI wieku,* Bellona, Warszawa 2002.
7. Balcerowicz B., *Wybrane problemy obronności państwa. Materiał studyjny*, AON, Warszawa 1997.
8. Balcerowicz B., *Sojusz a obrona narodowa*, Bellona, Warszawa 1999.
9. *Bariery i zagrożenia gospodarcze dla systemu obronnego Polski, „Materiały i Studia"*, IEO WS-0 nr 8(26), AON, Warszawa 1994.
10. Beaufre A., *Wstęp do strategii. Odstraszanie i strategia*, MON, Warszawa 1968.
11. Bem D. J., Kazimierczak W., Szymanowski M., *Systemy telekomunikacyjne cz. I i cz. II,* Politechnika Wrocławska, Wrocław 1983.
12. Beg D, Fischer S., Dombusch R., *Ekonomia*, PWE, Warszawa 1992.
13. *Bezpieczne niebo,* Materiały z konferencji naukowej, AON, Warszawa 2002.
14. Bolesta - Kukułka K., *Gra o władzę a gospodarka 1944-1991*, PWN, Warszawa 1990.
15. Bolkowska Z., Skowronek C., *Rezerwy państwowe. Funkcje, organizacja, ekonomika,* PWE, Warszawa 1997.

państwowej i sił zbrojnych wobec telekomunikacji są szczególne, do których zaliczyć należy:

- utrzymanie wyprzedzającej gotowości systemu w każdej sytuacji, a przede wszystkim w stanach nadzwyczajnych;
- zapewnienie bezpieczeństwa przekazywanych informacji i ochrony systemu; zapewnienie adaptacyjności i mobilności systemu;
- zintegrowanie rozwiązań technicznych w celu zapewnienia współdziałania wszystkich elementów systemu teleinformatycznego;
- uzyskanie efektywności ekonomicznej rozwiązań systemowych.

Realizacji przedstawionych wymagań i zadań powinny sprzyjać: jednoznacznie sformułowane i skoordynowane potrzeby organów władzy i administracji w zakresie usług teleinformatycznych; wyraźnie określone założenia techniczne i organizacyjne dotyczące wszystkich elementów systemu; możliwość wyboru najkorzystniejszych rozwiązań spełniających powyższe wymagania ogólne integrujące potrzeby użytkowników z uwzględnieniem ich specyfiki, np. sił zbrojnych, policji, straży pożarnej, urzędu celnego, itp. Należy jednak opracować strategie szkoleniowe, prowadzić stały monitoring sieci i systemów, zapewnić szeroką kampanię informacyjną na temat zagrożeń bezpieczeństwa teleinformatycznego. Z tworzeniem systemu muszą być powiązane: harmonizacja systemu prawnego i zmiany legislacyjne, wprowadzające m.in. ściganie z urzędu przestępstw teleinformatycznych (szczególnie komputerowych).

Warszawa 2002.

34. *Encyklopedia PWN t. 1,2,3,* Wydawnictwo Naukowe PWN, Warszawa 1999.
35. *Europejska ekonomika bezpieczeństwa. Kryptonim „Euro", część 1 - Identyfikacja problemu*, pod red. nauk. Z. Stachowiaka, AON, Warszawa 1999.
36. Gągor F., Paszkowski K., *Międzynarodowe operacje pokojowe w doktrynie obronnej RP*, Adam Marszałek, Warszawa 1998.
37. Gąsiorek K., Skobel W., R*ola i zadania województwa w systemie obronnym państwa w czasie pokoju, zagrożenia (kryzysu) i wojny*, AON, Warszawa 1998.
38. Gąsiorek K., Skobel W., Berliński T., *Współdziałanie terenowych organów administracji wojskowej z organami administracji rządowej i samorządowej w realizacji zadań operacyjno-obronnych*, AON, Warszawa 1998.
39. Giermakowski L., *Infrastruktura techniczno-ekonomiczna gospodarki narodowej w potencjale gospodarczo-obronnym kraju*, AON, Warszawa 1994.
40. Glikman P., Kabaj M., Muszkiet T., *Ciągłość i transformacja gospodarki. Zasoby kapitału, pracy, energii i ich wykorzystania do 2000-2010*, Key Tex, Warszawa 1997.
41. Goban-Klas T., Sieńkiewicz P., Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania., Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999.
42. Gontarski Z.,: *Polityka zatrudnienia w procesie przemian systemowych,* Ośrodek Badań Społecznych, Warszawa 1991.
43. *Gospodarcze podstawy bezpieczeństwa państwa wobec wyzwań rozwojowych świata na początku XXI wieku*, Praca pod kier. nauk. B. Balcerowicza, AON, Warszawa 2002.
44. *Gospodarka wybranymi zasobami naturalnymi w Polsce, a bezpieczeństwo ekonomiczne*, Praca pod kier. nauk. J. Płaczka, AON, Warszawa 1999.
45. Góralski W., *Japonia, działalność na rzecz osiągnięcia pozycji*

16. Bógdał-Brzezińska A. Gawrycki M. F., Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie, Fundacja Studiów Międzynarodowych, Warszawa 2003.
17. Bromirski M., *Sieci inteligentne w telekomunikacji*, Instytut Łączności, Warszawa 1999.
18. Bubnicki Z., *Wstęp do systemów ekspertowych*, PWN, Warszawa 1990.
19. Chojnacki M., Fornal M., *Infrastruktura NATO Charakterystyka programu inwestycji NATO na rzecz bezpieczeństwa (NSI.)*, AON, Warszawa 2000.
20. Ciborowski L., *Walka Informacyjna*, ECE, Toruń 1999.
21. Cieślak M. *Prognozowanie gospodarcze. Metody i zastosowania. Organizacja procesu prognostycznego,* PWN, Warszawa 1999.
22. Ciupiński A., Legucka A., *Podstawowe elementy polityki bezpieczeństwa i obrony Rzeczypospolitej Polskiej*, AON, Warszawa 2003.
23. Ciupiński A., Malak K., *Bezpieczeństwo polityczne i wojskowe*, AON, Warszawa 2004.
24. Clausewitz C., *O wojnie*, MON, Warszawa 1958.
25. Danecki J., A. Jajszczyk, *Nowoczesne techniki i usługi telekomunikacyjne*, TP S.A., Poznań 1996.
26. Dawidczyk A., *Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI wieku*, AON, Warszawa 2001.
27. Dolny E., Meller J., Wiśniewski Z., *Zarys polityki zatrudnienia*, PWE, Warszawa 1990.
28. Dworecki S., *Zagrożenia bezpieczeństwa państwa*, Warszawa 1994.
29. Dworecki S., *Od konfliktu do wojny*, BUWIK, Warszawa 1996.
30. Dworecki S.E., Kulisz M., Berny J., *Wpływ współczesnych konfliktów zbrojnych na politykę bezpieczeństwa państwa*, AON -Wyższa Szkoła Humanistyczna, Warszawa 1999.
31. Dworecki S. E., Kęsoń T.J., Kulisz M.Z., *Wskaźniki ekonomiczne obronności państwa*, AON, Warszawa 1999.
32. Dworecki S. E., Kęsoń T.J., Kulisz M.Z., *Współczesne konflikty zbrojne (Aspekt prognostyczny)*, AON, Warszawa 1998.
33. *Działania (operacje) połączone*, Materiały z konferencji naukowej, AON,

Państwowe Wydawnictwo Naukowe, Warszawa 1981.

62. Karpiński A., *Zakres interwencji państwa we współczesnych gospodarkach rynkowych*, Ossolineum 1991, Wrocław 1991.
63. *Kierowanie obronnością państwa w stanach nadzwyczajnych*, *Praca studyjna*, pod kier. nauk. M. Krauze, AON, Warszawa 2000.
64. *Kierowanie obronnością państwa w aspekcie wykorzystania technicznych środków najnowszej generacji*, *Materiały z seminarium naukowego przeprowadzonego w Centrum Konferencyjnym WP*, AON, Warszawa 2001.
65. *Kierowanie obronnością państwa w aspekcie wykorzystania technicznych środków najnowszej generacji*, *Materiały z konferencji naukowej przeprowadzonej w Centrum Konferencyjnym MON*, Sz. Gen.-AON, Warszawa 2002.
66. Klimaszewska A., Urbański L., *Kompetencje i zadania organów władzy i administracji publicznej w zakresie bezpieczeństwa i obronności państwa*, AON - Kancelaria Prezesa RM, Warszawa 1999.
67. *Kompatybilność elektromagnetyczna w radiotechnice*, Praca pod kier. nauk. W. Rotkiewicza, WKiŁ, Warszawa 1978.
68. *Koncepcja organizacji krajowej struktury planowania łączności cywilnej na potrzeby sytuacji kryzysowych*, *Praca naukowo – badawcza* pod kier. nauk. M. Krauze, AON, Warszawa 2000.
69. *Koncepcja wykorzystania technicznych środków łączności najnowszej generacji (mobilnych i sieciowych) w systemie łączności na potrzeby sytuacji kryzysowych,* Praca naukowo badawcza pod kier. nauk. M. Krauze, AON, Warszawa 2000.
70. Kościelak D. *ISDN cyfrowe sieci zintegrowane usługowo,* WKiŁ, Warszawa 1996.
71. Kownacki S., Rummel-Szyska Z., *Sprawne kierowanie*, IWZZ, Warszawa 1982.
72. Koziej S., Wołkowicz F., *Podstawowe założenia polityki bezpieczeństwa i strategii obronnej*, AON DSO MON. Warszawa 1998.
73. Koziej S., *Podstawowe problemy strategii i systemy obronności na*

supermocarstwa, Warszawa 1992.

46. Griffin P., *Podstawy zarządzania organizacjami,* PWN, Warszawa 1997.
47. Gregg W. D., *Podstawy telekomunikacji analogowej i cyfrowej*, WNT, Warszawa 1983.
48. Gwiazda A., *Globalizacja i regionalizacja gospodarki światowej*, Adam Marszałek, Toruń 1998.
49. Haliżak E., *Bezpieczeństwo narodowe Polski, geopolityczne, geoekonomiczne uwarunkowania*, Adam Marszałek, Toruń 1995.
50. Haliżak E., Zięba R., *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku,* Fundacja Stosunków Międzynarodowych, Warszawa 1997.
51. Hołyński M., *E-mailem z Doliny Krzemowej,* Prószyński i S-ka, Warszawa 2000.
52. *Infrastruktura – klucz do rozwoju*, Praca zbiorowa. Realizacji programu w zakresie rozwoju telekomunikacji, Departament Telekomunikacji Ministerstwa Infrastruktury, Warszawa 2003.
53. Jabłonowski M., *Wobec zagrożeń wojną. Wojsko a gospodarka II RP w latach 1935-1939*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2001.
54. Jajszczyk A., *Wstęp do telekomutacji*, Wydawnictwa Naukowo-Techniczne, Warszawa 2000.
55. Jałoszyński K., *Zagrożenie terroryzmem w wybranych krajach Europy Zachodniej oraz w Stanach Zjednoczonych*, AON, Warszawa 2001.
56. Jemioło T., *Globalizacja szanse i zagrożenia*, AON, Warszawa 2000.
57. Juszczyk M., *Wsparcie działań przez Panstwo-Gospodarza. Podstawowe problemy teorii*, AON, Warszawa 2003.
58. Kaczmarek J., Słowiński A., *Bezpieczeństwo, Świat - Europa - Polska*, Warszawa 1998.
59. Kaczmarek W., Ściborek Z., *Przyszła wojna jaka?*, BUWiK, Warszawa 1995.
60. Karlöf B., *Strategia biznesu,* Biblioteka Menedżera i Bankowca, Warszawa 1992.
61. Kapiński J., Firkowicz Sz.: *Zasady profilaktyki obiektów technicznych*,

kierunkiem Czesława Syca, WKiŁ, Warszawa 1997.

90. Misztal J., *Surowce strategiczne*, MON, Warszawa 1974.
91. *Możliwości wdrożenia systemu zapewniającego preferencyjną obsługę wybranych abonentów szczebla państwowego w systemie zarządzania telekomunikacją w warunkach sytuacji kryzysowych,* Praca naukowo badawcza pod kier. nauk. M. Krauze, AON, Warszawa 2000.
92. *NATO, Vademecum*, Warszawa, Bellona 1999.
93. *Operacja „Iracka Wolność" Materiały z konferencji naukowej zorganizowanej z inicjatywy i pod patronatem Ministra Obrony Narodowej*, AON, Warszawa 2003.
94. *Operacyjne przygotowanie obszaru kraju pod względem łączności.* E. Piedziuk, w: Wiedza Obronna, Towarzystwo Wiedzy Obronnej Nr 2/181, Warszawa 1997.
95. Ostrowski P., Dąbrowski M., *Systemy i sieci teleinformatyczne*, WKiŁ, Warszawa 1979.
96. *Patriotyzm Obronność Bezpieczeństwo*, Praca zbiorowa pod red. nauk. E. A. Wesołowskiej i A. Szerauca, AON, Warszawa 2002.
97. Penc J., *Strategia zarządzania, cz. 1.* Agencja Wydawnicza Placet, Warszawa 1994.
98. Penc - Pietrzak J., *Strategie biznesu i marketingu.* Wydawnictwo Profesjonalnej Szkoły Biznesu, Kraków 1998.
99. Peppard J., Rowlanda P., *Re-engineering,* Gebetner & S-ka, Warszawa 1997.
100. Piasecki B., Rogut A., Stawosz E., Johnson S., Smallbone D., *Warunki prowadzenia działalności gospodarczej przez MSP w Polsce i krajach Unii Europejskiej*, Polska Fundacja Promocji i Rozwoju MSP, Warszawa 1998.
101. Piątek S., *Prawo telekomunikacyjne Wspólnoty Europejskiej*, C.H.Beck, Warszawa 2003.
102. Piedziuk E. *System łączności w stanach nadzwyczajnych z punktu widzenia potrzeb obronnych państwa,* AON, Warszawa 1998.
103. Pieter J., *Z zagadnień pracy naukowej*, Zakład Narodowy im. Ossolińskich – Wydawnictwo, Wrocław 1974.

przełomie XX i XXI wieku, AON. Warszawa 2001.

74. Koziej S., *Rozważania o przyszłej strategii NATO oraz strategii bezpieczeństwa i obronności RP*, AON DSO, Warszawa 1999.
75. Krystek J., *Rola i zadania wojewódzkich komitetów obrony. Kompetencje wojewodów oraz ogólne zasady wykonywania zadań obronnych w województwach*, AON, Warszawa 1998.
76. Kucowski J., Laudyna D., Przekwasa M., *Energetyka a ochrona środowiska*, Warszawa 1997.
77. Kukułka J., *Problemy standardów międzynarodowych*, PAN, Warszawa 1978.
78. Kukułka J., *Problemy teorii stosunków międzynarodowych*, PAN, Warszawa 1979.
79. Kukułka J., Zięba R., *Polityka państwa*, Uniwersytet Warszawski, Warszawa 1992.
80. Kuźma T., *Aspekty organizacyjne i prawne realizacji zadań gospodarczo-obronnych przez terenowe organy administracji rządowej, samorządowej i podmioty gospodarcze*, AON, Warszawa 1998.
81. Kuźma T., *Kierowanie systemem gospodarczo - obronnym państwa*, CUP, Warszawa 1994, materiał nie publikowany.
82. Liderman K., *Bezpieczeństwo teleinformatyczne,* Instytut Informatyki i Robotyki WAT, Warszawa 2001.
83. Luard E., *The Globalization of Politics: The Changed focus of political action in the modem world*, New York 1990.
84. *Łączność w stanach nadzwyczajnych zagrożeń*, Materiały z seminarium specjalistycznego, Instytut Łączności – Ośrodek Szkolenia, Warszawa 2000.
85. Majewski W., *Systemy sieci zintegrowanej*, WKiŁ, Warszawa 1978.
86. Marczak J., Jakubczak R., Gąsiorek K., *Obrona terytorialna w obronie powszechnej RP,* AON, Warszawa 2002.
87. McGrew T.G, i Lewis E.G., *Global politics*, Cambridge 1992.
88. Merike Kaeo, *Tworzenie bezpiecznych sieci,* MIKOM, Warszawa 2000.
89. *Metodyka projektowania sieci telekomunikacyjnych*, praca zbiorowa pod

Polskiej, AON, Warszawa 2000.

118. Schatt S., *Zrozumieć sieci lokalne,* Intersoftland, Warszawa 1994
119. Sienkiewicz P., *Inżynieria systemów,* MON Warszawa 1983.
120. Sienkiewicz P., *Analiza systemowa – podstawy i zastosowania*, Bellona, Warszawa 1994.
121. Sienkiewicz P., *Wystarczalność obronna*, Bellona, Warszawa 1996.
122. Sikorski W., *Komputerowe planowanie przedsięwzięć – Microsoft Project*, ZNI MIKOM, Warszawa 1992.
123. *Słownik terminów z zakresu bezpieczeństwa narodowego*, pod kier. nauk. J. Pawłowskiego, AON, Warszawa 2002.
124. *Słownik terminów z zakresu bezpieczeństwa narodowego*, pod kier. nauk. B. Balcerowicza, AON, Warszawa 1996.
125. *Słownik pojęć z zakresu telekomunikacji w zastosowaniach cywilnych i wojskowych,* pod kier. nauk. E. Piedziuka, AON Warszawa 1996.
126. *Słownik wyrazów obcych*, PWN, Warszawa 1988.
127. Sportack Mark, *Sieci komputerowe. Księga eksperta.,* Helion, Glwice 2000.
128. Stachowiak Z., *Bezpieczeństwo żywnościowe Rzeczypospolitej Polskiej na przełomie XX i XXI wieku. Aspekt obronno - ekonomiczny i społeczny*, AON, Warszawa, 1995.
129. Stachowiak Z., *Ekonomia. Zarys podstawowych problemów*, WSISiZ, Warszawa 1998.
130. Stachowiak Z., *Ekonomia międzynarodowa wobec wyzwań cywilizacyjnych*, AON, Warszawa 2004.
131. *Stan telekomunikacji w 2002 r. i I półroczu 2003 r.,* Praca zbiorowa – analiza, Departament Telekomunikacji Ministerstwa Infrastruktury, Warszawa 2003.
132. Stankiewicz W., *Historia myśli ekonomicznej*, Polskie Wydawnictwo Ekonomiczne, Warszawa 1998.
133. Stańczuk J., *Współczesne pojmowanie bezpieczeństwa,* Warszawa 1996.
134. Stefanowicz J., *Ład międzynarodowy*, Warszawa 1996.
135. Stoner J.A.F., Wankel Ch., *Kierowanie*, PWE, Warszawa 1992.
136. Stopford J.M., Strange S., *Rival States, Rival Firms Competition for World*

104. Płaczek J., *Ewolucja polskiej myśli obronno-ekonomicznej w latach 1976-2000*, AON, Warszawa 2001.

105. *Podstawowe zadania, organizacja oraz perspektywy rozwiązań organizacyjnych w obronie cywilnej*, Urząd Szefa Obrony Cywilnej Kraju, AON, Warszawa 1998.

106. *Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego Polski z punktu widzenia narodowej i sojuszniczej strategii obronnej. Część I i II,* Opracowanie nauk. pod kier. nauk. Z. Stachowiaka, AON, Warszawa 2001.

107. Polarczyk K., *Gospodarka i bilans militarny. Polska na tle krajów NATO i Europy,* BSE, Warszawa 1997.

108. Polarczyk K., *NATO w świecie. Polska w NATO. Porównanie międzynarodowej sytuacji społeczno - gospodarczej i militarnej*, KS-BSiE, Raport nr 159, Warszawa czerwiec 1999.

109. Polarczyk K., *Gospodarka i bilans militarny. Polska na tle krajów NATO i Europy*, BSE, Warszawa listopad 1997.

110. *Polska polityka bezpieczeństwa 1989-2000*, pod redakcją R. Kuxniara, Wydawnictwo Naukowe Scholar, Warszawa 2001.

111. Popiuk - Rysińska I., *Uczestnicy stosunków międzynarodowych, ich interesy i oddziaływania wzajemne*, Warszawa 1996.

112. Prażewska M.: *Niezawodność urządzeń elektronicznych*, WKiŁ, Warszawa 1987.

113. Przewodzki E., Górski P., *Wybrane problemy planowania strategiczno - obronnego w warunkach członkostwa RP w Sojuszu Północnoatlantyckim*, AON-DSO MON, Warszawa 1999.

114. *Rezerwy, konflikty, obrona,* Pod. red. Z. Kołodziejaka, AE w Poznaniu, WAP, WSOSK, Poznań 1989.

115. Roden Martin S. *Systemy telekomunikacyjne analogowe i cyfrowe,* Wydawnictwo Naukowo Techniczne, Warszawa 1983.

116. Rotfeld A.D., *Europejski system bezpieczeństwa in statu nascendi*, Warszawa 1990.

117. Sabak Z., Królikowski J., *Ocena zagrożeń bezpieczeństwa Rzeczypospolitej*

152. *Vademecum teleinformatyka, Część I, II, III*, Praca zbiorowa, International Data Group Poland S.A., Warszawa 2000, 2002, 2004.
153. Varian H.R., *Mikroekonomia*, PWN, Warszawa 1997.
154. Wesołowski W.J., I*nżynieria zarządzania. Metodyka inżynieryjna tworzenia struktur systemów gospodarczych*, WSHiP, Warszawa 1999.
155. Wojnarowski J., *Utrzymywanie i podnoszenie gotowości obronnej państwa w sytuacjach kryzysowych,* AON, Warszawa 2002.
156. *World Investment Report 1999 Foreign Divert Investment and the Challenge of Development*, Untied Nations, New York and Geneva 1999.
157. Wróblewski R., *Podstawowe pojęcia z dziedziny polityki bezpieczeństwa strategii i sztuki wojennej*, AON, Warszawa 1993.
158. Wróblewski R., *Przygotowanie i prowadzenie wojny obronnej przez Polskę po 2000 roku „KAPPA", Część 1*, AON, Warszawa 1998.
159. Wróblewski R., *Wprowadzenie do strategii wojskowej*, BUWIK, Warszawa 1998.
160. *Wybrane problemy ekonomiki bezpieczeństwa*, pod red. nauk. Z. Stachowiaka i J. Płaczka, AON, Warszawa 2002.
161. Wyszczelski L., *Historia myśli wojskowej*, Bellona, Warszawa 2000.
162. Zacher L., *Społeczne wymiary efektywności informacyjnej,* Sigma NOT, Warszawa 1990.
163. Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego, koncepcje – struktury – funkcjonowanie*, Wydawnictwo naukowe Scholar, Warszawa 2001
164. Zięba R., *Kategorie bezpieczeństwa w nauce o stosunkach międzynarodowych*, pod red. D. Bobrowa, UW, Warszawa 1997.

B. Artykuły

1. Ciborowski L., *Analiza zagrożeń Rzeczpospolitej Polskiej,* Zeszyty Naukowe AON nr 3 (12), AON, Warszawa 1993.
2. Cieślarczyk M., *Niektóre psychospołeczne aspekty bezpieczeństwa, wyzwań, szans i zagrożeń,* Zeszyty naukowe AON nr 2 (35), AON, Warszawa 1999.

Market Shares, Cambridge 1991.

137. *Strategia obronności Rzeczypospolitej Polskiej. Studia i materiały nr 53,* Biuro Prasy i Informacji MON, Warszawa 2000.
138. Sułek M., Łuczak M., *Gospodarcze podstawy polityki i strategii bezpieczeństwa / „QUASIMODO" /*, AON, Warszawa 1996.
139. *Systemy kierowania obronnością państwa w stanach nadzwyczajnych w kontekście wykorzystania w nim środków i systemów łączności najnowszej generacji*, *Praca studyjna*, pod kier. nauk. M. Krauze, AON, Warszawa 2003.
140. *Systemy sieci zintegrowanej*, praca zbiorowa pod kierunkiem W. Majewskiego, WKiŁ, Warszawa 1978.
141. Szymański J. M., *Życie systemów*, PW „Wiedza Powszechna", Warszawa 1991.
142. Średniawa M., *Sieci inteligentne – architektura, usługi, zastosowania*, Politechnika Warszawska, Warszawa, 1998
143. *Środki dowodzenia*, pod kier. J. Janczaka i P. Daniluka, AON, Warszawa 2003.
144. Świniarski Z., *O naturze bezpieczeństwa*, Ulmak, Warszawa - Pruszków 1992.
145. Tarasiuk B., Czarniecki A., Suwiński W., *Kierowanie obronnością państwa w czasie pokoju, kryzysu i wojny. Materiał studyjny*, AON, Warszawa 1998.
146. *Telekomunikacja 2004,* Praca zbiorowa, MSG-Media, Bydgoszcz 2003.
147. *Teletransmisyjne systemy cyfrowe*, praca zbiorowa pod kierunkiem Władysława Majewskiego, WKiŁ, Warszawa 1976.
148. Toffler A i M., *Wojna i antywojna*, Warszawa 1997.
149. Tyrała P., *Zarządzanie kryzysowe. Ryzyko – Bezpieczenstwo - Obronność,* Wydawnictwo Adam Marszałek, Toruń 2001.
150. Ungerer H., *Telekomunikacja w Europie*, Ministerstwo Łączności, Warszawa 1992.
151. Urbanek A., Ilustrowany leksykon teleinformatyka, International Data Group Poland S.A., Warszawa 2001.

15. *Świat przyszłości a Polska*, Komitet Prognoz „Polska w XXI wieku" przy prezydium PAN, Elipsa, Warszawa 1995.
16. Świniarski J., *Czym jest bezpieczeństwo?,* Zeszyty Naukowe AON nr 3, AON, Warszawa 1993.
17. Świniarski J., *Ekonomia wojenna i ekonomika pokojowa w systemie ogólnej teorii bezpieczeństwa*, w: „Ekonomika wojskowa i logistyka wojskowa – podobieństwa i różnice", Materiały z sympozjum, AON, Warszawa 1998.
18. Stachowiak Z., *Bezpieczeństwo ekonomiczne,* w: „Ekonomika obrony", pod red. W. Stankiewicza, AON, Warszawa 1994.
19. Stachowiak Z., *Polityka gospodarczo-obronna,* w: „Gospodarka obronna Polski. Stan obecny i perspektywy", pod red. M. Sułka, AON, Warszawa 1995.
20. Sułek M., *System gospodarki obronnej RP,* w: „Ekonomika obrony, pod red. W. Stankiewicza, AON, Warszawa 1994.
21. Sułek M., *Metodologiczne podstawy wyodrębnienia ekonomiki bezpieczeństwa państwa,* w: „ Ekonomika bezpieczeństwa państwa średniej wielkości . Teoria i praktyka.", AON, Warszawa-Brno 2000.
22. Urbański L., *Kierowanie gospodarką obronną państwa. Stan aktualny i kierunki rozwoju,* w: „Gospodarka obronna Polski w końcu lat dziewięćdziesiątych. Szanse i zagrożenia.", pod red. J. Płaczka, AON, Warszawa 2001.
23. Wróblewski R., *Wybrane problemy diagnozy bezpieczeństwa narodowego,* Zeszyty Naukowe AON nr 3/4, AON, Warszawa 1991.
24. Zubek J., *System pojęć i podstawowe problemy bezpieczeństwa RP,* Zeszyty Naukowe AON nr 3, AON, Warszawa 1992.

C. Dokumenty

1. Ustawa o łączności z dnia 23 listopada 1990 r., (Dz. U. 1990 Nr 117, poz. 564.).
2. Ustawa z dnia 29 grudnia 1992 roku o radiofonii i telewizji., (Dz. U. 1993 Nr 7, poz. 34.).

3. Dąbrowski M., Średniawa M., *Ewolucja usług telekomunikacyjnych*, Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne nr 5, Warszawa 2000.
4. Dąbrowski M., *Z telekomunikacją w nowym milenium*, Przegląd Telekomunikacyjny nr 1, Warszawa 2001.
5. Haliżak E., *Ekonomiczny wymiar bezpieczeństwa narodowego i międzynarodowego,* w: „Bezpieczeństwo narodowe i międzynarodowe u schyłku XX wieku", pod red. D. Bobrowa i inni, Fundacja Studiów Międzynarodowych, UW, Warszawa 1997.
6. Kołodziejak Z., *Bezpieczeństwo ekonomiczne, geneza, uwarunkowania obronne,* w: „Bezpieczeństwo ekonomiczne teoria i praktyka. pod red. Z. Kołodziejaka, Instytut Ekonomii Politycznej, Łódź 1986.
7. Kurek St., *Identyfikacja gospodarczych podstaw bezpieczeństwa państwa,* w: „Podstawy, mechanizmy i procedury kształtowania bezpieczeństwa ekonomicznego Polski z punktu widzenia narodowej i sojuszniczej strategii obronnej. Część I – Metodologia i model badań bezpieczeństwa ekonomicznego kraju", pod red. Z. Stachowiaka, AON, Warszawa 2001.
8. Lubbe A., *Bezpieczeństwo ekonomiczne państwa*, w: „Sprawy międzynarodowe" nr 4, Warszawa 1997.
9. Łukaszuk L., *Prawno międzynarodowe uwarunkowania bezpieczeństwa i obronności Polski,* w: „Myśl wojskowa" nr 1, Warszawa 1995.
10. Mikielewicz G., *Kierowanie gospodarką obronną RP,* w: Materiały z konferencji naukowej „ Kierowanie obronnością państwa", AON, Warszawa 1993.
11. *Polska 2025. Długookresowa strategia trwałego i zrównoważonego rozwoju*, RzCSS-RM, Warszawa 2000.
12. *Przyszłość państwa a gospodarka*, Komitet Prognoz „Polska w XXI wieku" przy prezydium PAN, Elipsa, Warszawa 1997.
13. Rotfeld A.D., *Bezpieczeństwo Polski a bezpieczeństwo Europy,* w: „Sprawy międzynarodowe" nr 7-8, Warszawa 1984.
14. Rutkowski C.,. *Bezpieczeństwo, obronność: strategie – doktryny – koncepcje*, Zeszyty Naukowe AON nr 1, AON, Warszawa 1995.

18. Ustawa o stanie klęski żywiołowej z dnia 18 kwietnia 2002 r., (Dz. U. Nr 62 poz. 558.).
19. Ustawa o stanie wyjątkowym z dnia 21 czerwca 2002 r., (Dz. U. Nr 113, poz. 985, Nr 153, poz. 1271.).
20. Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną., (Dz. U. 2002 Nr 144, poz. 1204.).
21. Ustawa o stanie wojennym oraz o kompetencjach naczelnego dowódcy sił zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej z dnia 29 sierpnia 2002 r., (Dz. U. z dnia 25 września 2002 r.).
22. Rozporządzenie Prezesa Rady Ministrów z dnia 9 września 2002 r. w sprawie wymiany informacji istotnych dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczypospolitej Polskiej., (Dz. U. Nr 150, poz. 1234.).
23. Ustawa *2* dnia 12 września 2002 roku o elektronicznych instrumentach płatniczych., (Dz. U. Nr 169, poz. 1385.).
24. Rozporządzenie Rady Ministrów w sprawie sposobu tworzenia gminnego zespołu reagowania, powiatowego i wojewódzkiego zespołu reagowania kryzysowego oraz Rządowego Zespołu Koordynacji i ich funkcjonowania z dnia 3 grudnia 2002 roku., (Dz. U. Nr 215 poz. 1818.).
25. Rozporządzenie Ministra Infrastruktury z dnia 24 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa i porządku publicznego., (Dz. U. z dnia 7 lutego 2003 r.).
26. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Przyjęta na posiedzeniu RM w dniu 8 września 2003 r., Urząd Rady Ministrów, Warszawa 2003.
27. Raport 3. Kongresu Informatyki Polskiej z dnia 1listopada 2003 r.
25. Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym., (Dz. U. Nr 98 poz. 978.).

3. Rozporządzenie Ministra Łączności z dnia 31 maja 1993 roku w sprawie określania systemów telekomunikacyjnych, zakładanych i użytkowanych na terytorium Rzeczpospolitej Polskiej., (Dz. U. 1993 Nr 63, poz. 302.).
4. Ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych., (Dz. U. 1994 Nr 24, poz. 83.).
5. Planowanie działań NATO na wypadek zagrożeń cywilnych. Bruksela 1995 r.
6. Kompendium Łączności Cywilnej Rady Północnoatlantyckiej. Bruksela 1996 r.
7. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.
8. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r., (Dz. U. 1997 Nr 133, poz. 883.).
9. Strategia finansów publicznych i rozwoju gospodarczego. Polska 2000 ÷ 2010, Ministerstwo Finansów, Rada Ministrów, Warszawa 1999.
10. Rozporządzenie Ministra Łączności z dnia 9 października 1999 roku w sprawie ogólnych warunków przyłączenia sieci telekomunikacyjnych oraz zasad rozliczeń., (Dz. U. 1999 Nr 79, poz. 897.).
11. Raport 2. Kongresu Informatyki Polskiej z dnia 3 grudnia 1999 r.
12. Strategia Bezpieczeństwa Rzeczypospolitej Polskiej. Przyjęta na posiedzeniu Rady Ministrów w dniu 4 stycznia 2000 r.
13. Strategia Obronności Rzeczypospolitej Polskiej. Przyjęta na posiedzeniu Rady Ministrów w dniu 23 maja 2000 r.
14. Ustawa „Prawo telekomunikacyjne" z dnia 21 lipca 2000 r., (Dz. U. 2000 Nr 73, poz. 852.).
15. Decyzja nr 182/MON z dnia 6 października 2000 r. w sprawie sprawowania nadzoru nad ochroną informacji niejawnych w resorcie obrony narodowej (dokument wewnętrzny).
16. Ustawa z dnia 18 września 2001 roku o podpisie elektronicznym., (Dz. U. 2001 Nr 130, poz. 1450.).
17. Raport w sprawie dostosowań instytucjonalnych w Polsce do wymogów członkostwa w Unii Europejskiej. Przyjęty przez Komitet Integracji Europejskiej w dniu 10 kwietnia 2002 r.

WYKAZ MAP, SCHEMATÓW, TABEL, WYKRESÓW I ZAŁĄCZNIKÓW

A. Mapy

2.1. Połączenia teleinformatyczne sieci TELBANK S.A. w sieci satelitarnej VSAT (Wariant) 142

2.2. Struktura sieci inteligentnej IN (Uproszczony) 202

2.3. Liczba abonentów na 100 mieszkańców – stan na 31.12.2002 r. 251

2.4. Sieć telekomunikacyjna transmisji danych na potrzeby Straży Granicznej 274

2.5. Tereny o największym prawdopodobnym zagrożeniu w konfliktach lokalnych 330

2.6. Prawdopodobne miejsca wystąpienia powodzi i zatopień 332

2.7. Obszary kraju zagrożone trującymi środkami przemysłowymi 333

2.8. Obszary występowania z największym prawdopodobieństwem różnych typów zagrożeń 334

B. Schematy

1.1. Idea bezpieczeństwa państwa 31

1.2. System obronności państwa 34

1.3. Podstawy polskiej polityki bezpieczeństwa 43

1.4. Architektura bezpieczeństwa państwa 44

1.5. Podział telekomunikacji 67

1.6. System łączności państwa (Wariant) 73

1.7. Ogólny podział analogowych sieci telekomunikacyjnych 76

1.8. Ogólny podział cyfrowych sieci telekomunikacyjnych 77

1.9. Uproszczona struktura sieci telekomunikacyjnej użytku publicznego 78

1.10. Typowe przepływności i zasięgi łączy telekomunikacyjnych. 79

26. Rozporządzenie Ministra Infrastruktury z dnia 7 maja 2004 w sprawie sposobu uwzględniania w zagospodarowaniu przestrzennym potrzeb obronności i bezpieczeństwa państwa., (Dz. U. Nr 6 poz.41.).
27. Ustawa „Prawo telekomunikacyjne" z dnia 16 lipca 2004 r., (Dz. U. 2004 Nr 171, poz. 1800.).
28. Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa., (Dz. U. Nr 180. poz. 1855.).

D. Materiały statystyczne

1. *Mały rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 1999.
2. *Mały rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2000.
3. *Mały rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2001.
4. *Mały rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2002.
5. *Mały rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2003.
6. *Rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 1999.
7. *Rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2000.
8. *Rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2001.
9. *Rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2002.
10. *Rocznik statystyczny Polski*, Główny Urząd Statystyczny, Warszawa 2003.

C. Tabele

1.1. Rodzaje i cechy użytkowe łączy telekomunikacyjnych 80

2.1. Zasadnicze różnice systemów N-ISDN i B-ISDN 123

2.2. Przepływności oraz nazwy sygnałów (modułów) SDH 152

2.3. Podstawowe cechy generacji systemów komórkowych 171

2.4. Przepływność dla poszczególnych usług (kb/s) 175

2.5. Wady i zalety komutacji kanałów 190

2.6. Zalety i wady komutacji pakietów 191

2.7. Zalety i wady komutacji wiadomości 192

2.8. Zalety i wady technologii ATM 235

2.9. Standardowe telefoniczne łącza główne (abonenci telefonii przewodowej) w latach 1990 – 2002 249

2.10. Telefoniczne łącza główne (abonenci telefonii przewodowej + łącza ISDN) w latach 1999 - 2002 250

2.11. Ilość abonentów obsługiwanych przez największych niezależnych operatorów telekomunikacyjnych 254

2.12. Liczba łączy głównych TP S.A. na dzień 31 grudnia 2001 i 2002 r. 256

2.13. Struktura ruchu wychodzącego z sieci TP S.A. w 2001 i 2002 r. 257

2.14. Abonenci i użytkownicy telefonii komórkowej w latach 1995 – 2002 261

2.15. Abonenci i użytkownicy telefonii komórkowej (w tys.) w 2002 r. 263

2.16. Liczba operatorów, sieci TVK i gniazd abonenckich w latach 1993-2003 266

2.17. Ważniejsze dane zbiorcze o łączności stan w dniu 31.12.2002 267

2.18. Przychody ze sprzedaży wyrobów i usług łączności 268

1.11. Usługi i technologie multimedialne 82
1.12. Uproszczony warstwowy schemat infrastruktury telekomunikacyjnej kraju 84
1.13. Współużytkownicy systemu teleinformatycznego 104
2.1. Rozwój usług telekomunikacyjnych 110
2.2. Infrastruktura telekomunikacyjna kraju 113
2.3. Zalety zintegrowanej sieci cyfrowej ISDN 118
2.4. Podział usług sieci ISDN 119
2.5. Współpraca systemu trankingowego TETRA z systemem łączności radiowej 137
2.6. Realizacja sieci VPN dla potrzeb sieci POLPAK – T (Wariant) 148
2.7. Rozwój sieci Internet w ogólnej ewolucji sieci telekomunikacyjnej 160
2.8. Architektura ruchomej sieci multimedialnej 181
2.9. Schemat sieci satelitarnej (Wariant) 184
2.10. Podstawowe elementy sieci komputerowych 205
2.11. Funkcje realizowane przez warstwy modelu OSI/ISO 207
2.12. Sieć ATM integrująca sieć lokalną oraz sieć rozległą (Wariant) 233
2.13. Obszary powstawania zagrożeń bezpieczeństwa państwa 339
2.14. Ekonomiczne przyczyny powstawania zagrożeń 340
3.1. Atrybuty systemu informacyjnego państwa 422
3.2. Elementy składowe systemu teleinformatycznego na potrzeby kierowania bezpieczeństwem państwa 429
3.3. Kierowanie obronnością państwa (Wariant) 448
3.4. Struktura niemilitarnych ogniw kierowania 455
3.5. Uproszczony schemat ochrony danych w sieci teleinformatycznej 458
3.6. Ataki na bezpieczeństwo w sieciach teleinformatycznych 459

E. Załączniki

1. Wyciąg z Konstytucji Rzeczypospolitej Polskiej zawierający artykuły dotyczące obronności państwa. 539
2. Kompendium Łączności Cywilnej Rady Północnoatlantyckiej, SCEPC NATO, Bruksela 1995. 542
3. Planowanie działań NATO na wypadek zagrożeń cywilnych, CEP NATO, Bruksela 1996. 559
4. Ustawa o stanie wojennym oraz o kompetencjach naczelnego dowódcy sił zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej z dnia 29 sierpnia 2002 r. (Dz. U. Nr 87 poz. 87.). 564
5. Ustawa o stanie wyjątkowym z dnia 21 czerwca 2002 r. (Dz. U. Nr 113, poz. 985, Nr 153, poz. 1271.). 575
6. Ustawa o stanie klęski żywiołowej z dnia 18 kwietnia 2002 r. (Dz. U. Nr 62 poz. 558.). 582
7. Rozporządzenie Rady Ministrów w sprawie sposobu tworzenia gminnego zespołu reagowania, powiatowego i wojewódzkiego zespołu reagowania kryzysowego oraz Rządowego Zespołu Koordynacji Kryzysowej i ich funkcjonowania z dnia 3 grudnia 2002 r. (Dz. U. Nr 215, poz.1818.). 590
8. Działania niezbędne związane z rozwojem społeczeństwa informacyjnego w Polsce. Wyciąg z raportu w sprawie dostosowań instytucjonalnych w Polsce do wymogów członkostwa w Unii Europejskiej. Przyjęty przez Komitet Integracji Europejskiej w dniu 10 kwietnia 2002 r. 596
9. Rozporządzenie Ministra Infrastruktury z dnia 24 stycznia 2003 r. w sprawie wykonywania przez operatorów zadań na rzecz obronności, bezpieczeństwa państwa i porządku publicznego. (Dz. U. Nr 2 poz. 24.). 601
10. Rozporządzenie Rady Ministrów z dnia 27 kwietnia 2004 r. w sprawie przygotowania systemu kierowania bezpieczeństwem narodowym

D. Wykresy

2.1. Etapy rozwoju usług sieci inteligentnej 203

2.2. Standardowe telefoniczne łącza główne (abonenci telefonii przewodowej – w tys.) w miastach i na wsi w latach 1990 – 2002 250

2.3. Polska na tle Europy - liczba abonentów telefonii przewodowej na 100 mieszkańców 252

2.4. Ilość linii stacjonarnych w Polsce na tle niektórych krajów 253

2.5. Liczba abonentów telefonicznych na 100 mieszkańców w Polsce na tle świata, Europy i Unii Europejskiej 253

2.6. Podział rynku telekomunikacyjnego pomiędzy TP S.A. i pozostałymi największymi operatorami telekomunikacyjnymi w latach 1997÷2001 255

2.7. Udział w rynku telefonii przewodowej lokalnej (linie) w 2002 r. 255

2.8. Udział w rynku międzystrefowym (ruch telefoniczny) w 2002 r. 256

2.9. Liczba łączy głównych TP S.A. w latach 2000 - 2002 r. 257

2.10. Abonenci i użytkownicy telefonii komórkowej w latach 1995 – 2002 (w tys.) 261

2.11. Udział w rynku telefonii komórkowej 2002 r. 262

2.12. Udział w rynku telefonii ogółem w 2002 r. 262

2.13. Abonenci i użytkownicy poszczególnych operatorów telefonii komórkowej w latach 2001-2002 264

2.14. Prognozy rozwoju telefonii komórkowej i stacjonarnej do 2005 r. 265

2.15. Zagrożenia sieci telekomunikacyjnej w okresie konfliktu zbrojnego 328

ZAŁĄCZNIKI

Załącznik nr 1

WYCIĄG
z KONSTYTUCJI RZECZYPOSPOLITEJ POLSKIEJ
zawierający artykuły dotyczące obronności państwa

Rozdział I
RZECZPOSPOLITA
Art.5.

Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju.

Art.8.

1. Konstytucja jest najwyższym prawem Rzeczpospolitej Polskiej.
2. Przepisy Konstytucji stosuje się bezpośrednio, chyba że Konstytucja stanowi inaczej.

Art.26.

1. Siły Zbrojne Rzeczpospolitej Polskiej służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic.
2. Siły Zbrojne zachowują neutralność w sprawach politycznych oraz podlegają cywilnej i demokratycznej kontroli.

Rozdział II
WOLNOŚĆ, PRAWA I OBOWIĄZKI
CZŁOWIEKA I OBYWATELA
ŚRODKI OCHRONY WOLNOŚCI I PRAW
Art.85.

1. Obowiązkiem obywatela polskiego jest obrona Ojczyzny.
2. Zakres obowiązku służby wojskowej określa ustawa.
3. Obywatel, któremu przekonania religijne lub wyznawane zasady moralne nie pozwalają na odbywanie służby wojskowej, może być obowiązany do służby zastępczej na zasadach określonych w ustawie.

Rozdział III
ŹRÓDŁA PRAWA
Art. 87.

1. Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia.
2. Źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są na obszarze działania organów, które je ustanowiły, akty prawa miejscowego.

Art. 89.

1. Ratyfikacja przez Rzeczpospolitą Polską umowy międzynarodowej i jej wypowiedzenie wymaga uprzedniej zgody wyrażonej w ustawie, jeżeli umowa dotyczy: pokoju, sojuszy, układów politycznych lub układów wojskowych.

Art.91.

1. Ratyfikowana umowa międzynarodowa, po jej ogłoszeniu w Dzienniku Ustaw Rzeczypospolitej Polskiej, stanowi część krajowego porządku prawnego i jest bezpośrednio stosowana, chyba że jej stosowanie jest uzależnione od wydania ustawy.

Rozdział IV
ORGANIZACJA I DZIAŁANIE
Art. 116.

1. Sejm decyduje w imieniu Rzeczypospolitej Polskiej o stanie wojny i o zawarciu pokoju.
2. Sejm może podjąć uchwałę o stanie wojny jedynie w razie zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umów międzynarodowych wynika zobowiązanie do wspólnej obrony przeciwko agresji. Jeżeli Sejm nie może zebrać się na posiedzenie, o stanie wojny postanawia Prezydent Rzeczypospolitej.

(Dz. U. Nr 5 poz. 17.). 604

11. Rozporządzenie Rady Ministrów z dnia 3 sierpnia 2004 r. w sprawie przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa (Dz. U. Nr 180. poz. 1855 z 2004 r.). 609

Rozdział VII
SAMORZĄD TERYTORIALNY

Art. 164.

1. Podstawową jednostką samorządu terytorialnego jest gmina.

Rozdział IX
STANY NADZWYCZAJNE

Art. 228.

1. W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej.
2. Stan nadzwyczajny może być wprowadzony tylko na podstawie ustawy, w drodze rozporządzenia, które podlega dodatkowemu podaniu do publicznej wiadomości.
3. Zasady działania organów władzy publicznej oraz zakres, w jakim mogą zostać ograniczone wolności i prawa człowieka i obywatela w czasie poszczególnych stanów nadzwyczajnych określa ustawa.
4. Ustawa może określić podstawy, zakres i tryb wyrównywania strat majątkowych wynikających z ograniczenia w czasie trwania stanu wyjątkowego wolności i praw człowieka i obywatela.
5. Działania podjęte w wyniku wprowadzenia stanu nadzwyczajnego muszą odpowiadać stopniowi zagrożenia i powinny zmierzać do jak najszybszego przywrócenia normalnego funkcjonowania państwa.

Art. 229.

W razie zewnętrznego zagrożenia państwa, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić stan wojenny na części lub na całym terytorium państwa.

Art. 230.

W razie zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, Prezydent Rzeczypospolitej na wniosek Rady Ministrów może wprowadzić, na czas oznaczony, nie dłuższy niż 90 dni, stan wyjątkowy na części lub na cały terytorium państwa.

Art. 231.

Rozporządzenie o wprowadzeniu stanu wojennego lub wyjątkowego Prezydent Rzeczypospolitej przedstawia Sejmowi w ciągu 48 godzin od podpisania rozporządzenia. Sejm niezwłocznie rozpatruje rozporządzenia Prezydenta Rzeczypospolitej. Sejm może je uchylić bezwzględną większością głosów w obecności co najmniej połowy ustawowej liczby posłów.

Art. 232.

W celu zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia Rada Ministrów może wprowadzić na czas oznaczony, nie dłuższy niż 30 dni, stan klęski żywiołowej na części lub na całym terytorium państwa. Przedłużenie tego stanu może nastąpić za zgodą Sejmu.

Art. 234.

1. Jeżeli w czasie stanu wojennego Sejm nie może zebrać się na posiedzenie, Prezydent Rzeczypospolitej na wniosek Rady Ministrów wydaje rozporządzenia z mocą ustawy w zakresie i granicach określonych w art. 228 ust. 3-5. Rozporządzenia te podlegają zatwierdzeniu przez Sejm na najbliższym posiedzeniu.
2. Rozporządzenia, o których mowa w ust. 1, mają charakter powszechnie obowiązującego prawa.

Art.117.

Zasady użycia Sił Zbrojnych poza granicami Rzeczypospolitej Polskiej określa ratyfikowana umowa międzynarodowa lub ustawa. Zasady pobytu obcych wojsk na terytorium Rzeczypospolitej Polskiej i zasady przemieszczania się ich przez to terytorium określają ratyfikowane umowy międzynarodowe lub ustawy.

Rozdział V
PREZYDENT RZECZYPOSPOLITEJ POLSKIEJ

Art.126.

2. Prezydent Rzeczypospolitej czuwa nad przestrzeganiem Konstytucji, stoi na straży suwerenności i bezpieczeństwa państwa oraz nienaruszalności i niepodzielności jego terytorium.

Art.134.

1. Prezydent Rzeczypospolitej Polskiej jest najwyższym zwierzchnikiem Sił Zbrojnych Rzeczypospolitej Polskiej.
2. W czasie pokoju Prezydent Rzeczypospolitej sprawuje zwierzchnictwo nad Siłami Zbrojnymi za pośrednictwem Ministra Obrony Narodowej.
3. Prezydent Rzeczypospolitej mianuje Szefa Sztabu Generalnego i dowódców rodzajów sił zbrojnych na czas określony. Czas trwania kadencji, tryb i warunki odwołania przed jej upływem określa ustawa.
4. Na czas wojny Prezydent Rzeczypospolitej, na wniosek Prezesa Rady Ministrów, mianuje Naczelnego Dowódcę Sił Zbrojnych. W tym samym trybie może on Naczelnego Dowódcę Sił Zbrojnych odwołać. Kompetencje Naczelnego Dowódcy Sił Zbrojnych i zasady jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej określa ustawa.
5. Prezydent Rzeczypospolitej Polskiej, na wniosek Ministra Obrony Narodowej, nadaje określone w ustawach stopnie wojskowe.
6. Kompetencje Prezydenta Rzeczypospolitej, związane ze zwierzchnictwem nad Siłami Zbrojnymi, szczegółowo określa ustawa.

Art. 135.

Organem doradczym Prezydenta Rzeczypospolitej w zakresie wewnętrznego i zewnętrznego bezpieczeństwa państwa jest Rada Bezpieczeństwa Narodowego.

Art. 136.

W razie bezpośredniego, zewnętrznego zagrożenia państwa Prezydent Rzeczypospolitej, na wniosek Prezesa Rady Ministrów, zarządza powszechną lub częściową mobilizację i użycie Sił Zbrojnych do obrony Rzeczypospolitej.

Art. 141.

1. W sprawach szczególnej wagi Prezydent Rzeczypospolitej może zwołać Radę Gabinetową. Radę Gabinetową tworzy Rada Ministrów obradująca pod przewodnictwem Prezydenta Rzeczypospolitej.
2. Radzie Gabinetowej nie przysługują kompetencje Rady Ministrów.

Art. 144.

1. Prezydent Rzeczypospolitej, korzystają ze swoich konstytucyjnych i ustawowych kompetencji, wydaje akty urzędowe.
2. Akty urzędowe Prezydenta Rzeczypospolitej wymagają dla swojej ważności podpisu Prezesa Rady Ministrów, który przez podpisanie aktu ponosi odpowiedzialność przed Sejmem.

Przepis ust. 2 nie dotyczy:

- zwoływania Rady Gabinetowej,
- powoływania i odwoływania członków Rady Bezpieczeństwa Narodowego.

Rozdział VI
RADA MINISTRÓW I ADMINISTRACJA RZĄDOWA

Art. 146.

1. Rada Ministrów prowadzi politykę wewnętrzną i zagraniczną Rzeczypospolitej Polskiej.
2. Do Rady Ministrów należą sprawy polityki państwa nie zastrzeżone dla innych organów państwowych i samorządu terytorialnego.
3. Rada Ministrów kieruje administracją rządową.
4. W zakresie i na zasadach określonych w Konstytucji i ustawach Rada Ministrów w szczególności:

7) Zapewnia bezpieczeństwo wewnętrzne państwa.
8) Zapewnia bezpieczeństwo zewnętrzne państwa.
11) Sprawuje ogólne kierownictwo w dziedzinie obronności kraju oraz określa corocznie liczbę obywateli powoływanych do czynnej służby wojskowej.

Art. 152.

1. Przedstawicielem Rady Ministrów w województwie jest wojewoda.

medycyna i łączność cywilna. Każdą, dziedziną zajmują się poszczególne komórki lub komisje planowania. CCPC to wyspecjalizowany komitet zgłaszający plany łączności cywilnej do SCEPC.

5. Postępy prac w zakresie CEP stanowią przedmiot regularnej analizy i oceny zgodnie z „Cyklem Planowania i Badania". Podstawowymi elementami tego cyklu są: Resortowe Wytyczne Planowania, Programy Robocze i Raporty z Postępu Prac opracowywane przez Komórki i Komisje Planowania PB&Cs) oraz Ankiety CEP. Część techniczna Kwestionariusza jest opracowywana i aktualizowana przez PB&Cs; także te jednostki zajmują się analiza odpowiedzi udzielonych w Ankiecie przez poszczególne kraje. W ten sposób możliwe jest gromadzenie danych oraz mierzenie i ocena stanu przygotowania i postępów poczynionych przez poszczególne kraje na różnych obszarach CEP. W wyniku tej oceny staje się jasne, czy wysiłki w zakresie planowania należy zintensyfikować w skali kraju czy istnieje potrzeba wzmożonej koordynacji po stronie międzynarodowej.

Zadania CCPC

6. Zadaniem CCPC jest wspomaganie krajowych władz i organizacji w procesie legislacyjnym, regulacyjnym, świadczeniu usług i eksploatacji cywilnych sieci telekomunikacyjnych i usług pocztowych. Zadania te są realizowane w formie wytycznych i zaleceń w zakresie zapewnienia nieprzerwanej łączności tego typu w celu wspomagania funkcjonowania społeczeństwa w sytuacji wyjątkowej CCPC pomaga też cywilnym komórkom i komitetom ds. planowania w planowaniu łączności i systemów informacyjnych. CCPC składa się z przedstawicieli władz poszczególnych krajów członkowskich NATO odpowiedzialnych za sprawy związane z łącznością cywilną.

Przeznaczenie Kompendium

7. Sprawą zasadniczej wagi jest, by wszyscy użytkownicy systemów łączności, którzy mają do spełnienia rolę w sytuacjach wyjątkowych, w czasie kryzysu i wojny, byli w stanie nadal spełniać swoje zadania i wspierać Pakt. Do takich użytkowników zaliczają się: władze rządowe i regionalne, siły zbrojne, obrona cywilna, najważniejsze urządzenia użyteczności publicznej i przemysł strategiczny, itp.
8. Udogodnieniem dla poszczególnych krajów może być połączenie planowania w wypadku kryzysu i wojny z planowaniem w sytuacjach wyjątkowych oraz klęskach żywiołowych lub wywołanych działaniem człowieka. Mimo iż ten ostatni rodzaj planowania nie mieści się w zakresie niniejszego dokumentu, jego charakter będzie często podobny do planowania w sytuacji kryzysowo-wojennych: tego rodzaju połączenie może okazać się korzystne, szczególnie pod względem finansowym.
9. CEP z poszczególnych krajów wypełniają stałe zadania polegające na przeglądzie istniejących i planowanych systemów łączności w celu określenia ich przydatności w sytuacjach kryzysowo-wojennych oraz wdrożenia środków niezbędnych do poprawienia ich skuteczności. Także na płaszczyźnie międzynarodowej maja za zadanie koordynację wszystkich działań podejmowanych na rzecz zapewnienia nieprzerwanej łączności na płaszczyźnie międzynarodowej.
10. Celem niniejszego Kompendium jest koordynacja i zharmonizowanie nieprzerwanej łączności w czasie kryzysu i wojny dzięki działaniom CEP na szczeblu krajowym, rządowym lub międzyrządowym, dysponujących odpowiednią dokumentacją i wytycznymi w zakresie planowania i realizacji środków i działań. Łączność międzynarodowa nie będzie funkcjonować właściwie w sytuacjach kryzysowo-wojennych, o ile każdy kraj nie zaplanuje i wdroży tych środków. Z tego powodu CCPC usilnie nakładania poszczególne kraje do zapewnienia, by środki zaproponowane w niniejszym dokumencie zostały wzięte pod uwagę w procesie planowania w wypadku sytuacji wyjątkowych, kryzysowych i wojennych, wykonywanych w czasie pokoju.
11. Kompendium składa się z:
    Część 1 Telekomunikacji, nadzorowanej przez Grupę Robocza CCPC
    Część 2 Usług Pocztowych, nadzorowanych przez Grupę Robocza CCPC

II. WYTYCZNE NIEPRZERWANEJ DOSTĘPNOŚCI ŁĄCZNOŚCI CYWILNEJ

Zasady Ogólne

12. Sprawą najwyższej wagi jest, by Kraje Członkowskie NATO traktowały swoje krajowe i międzynarodowe urządzenia telekomunikacyjne za część ogólnego potencjału obronnego Paktu, w czym zawiera się Gotowość Cywilna.
13. W niniejszym rozdziale znajdują się wytyczne spełniania wymogów Paktu w zakresie łączności cywilnej. Niektóre aspekty wytycznych mogą też zaspokajać wymogi wojskowe.

Potrzeba Informacji, Konsultacji i Koordynacji

14. Ważne jest, by każdy kraj uruchomił skuteczny mechanizm umożliwiający wprowadzanie, monitorowanie i wdrażanie odpowiednich środków w zakresie krajowych usług telekomunikacyjnych mających na celu zagwarantowanie nieprzerwanej łączności krajowej i międzynarodowej w sytuacjach wyjątkowych, kryzysowych i wojennych. W tym celu wybrane mechanizmy krajowe winny zapewnić możliwość regularnych konsultacji, koordynacji oraz wymiany informacji w ramach i pomiędzy Członkami NATO.

Załącznik 2

KOMPENDIUM ŁĄCZNOŚCI CYWILNEJ
RADA PÓŁNOCNOATLANTYCKA

NADZWYCZAJNA CYWILNA KOMISJA PLANOWANIA
(Ang. SCEPC – Senior Civil Emergency Planning Committe)
Notatka Dyrektora Ds. CEP (Ang. Civil Emergency Committe)
NACC/PFP(SCEPC)(95)4 1995 r.
Bruksela 1995 r.

1. Komisja ds. Planowania Łączności Cywilnej NATO (ang. CCPC -Civil Communications Planning Committe) sporządziła niedawno „Kompendium Komunikacji Cywilnej". Głównym zadaniem CCPC jest wspomaganie krajowych władz i organizacji zajmujących się legislacją, regulacją, świadczeniem usług i eksploatacją cywilnych sieci telekomunikacyjnych i usług pocztowych. Zadania te realizuje w formie dostarczania wytycznych i zaleceń w zakresie zapewnienia nieprzerwanej dostępności tego rodzaju łączności w celu wspomagania funkcjonowania społeczeństwa w sytuacji wyjątkowej.
2. Celem niniejszego Kompendium jest koordynacja i zharmonizowanie nieprzerwanej łączności w czasie kryzysu i wojny dzięki działaniom Cywilnych Planistów ds. Sytuacji Wyjątkowych na szczeblu krajowym, rządowym lub międzyrządowym, dysponujących odpowiednią dokumentacją i wskazówkami w zakresie planowania i realizacji środków i działań. Łączność międzynarodowa nie będzie funkcjonować właściwie w sytuacjach wyjątkowych, o ile każdy kraj nie zaplanuje i nie wdroży tych środków.
3. Ponieważ wymiana informacji stanowi istotną część aktualnie realizowanego „Programu Współpracy", pragnę zachęcić organy CEP (ang. Civil Emergency Committe) NATO i krajów partnerskich do udostępnienia niniejszego kompendium organizacjom z ich krajów zajmującym się Planowaniem Łączności w sytuacjach wyjątkowych
4. Dodatkowe egzemplarze kompendium można otrzymać na żądanie z Dyrekcji CEP NATO (fax. +32-2-728.7900).

Podpisał (dr F.P. Palmeri)

I. WSTĘP

Technologia

1. Na przestrzeni kilku ostatnich lat technologie w dziedzinie Telekomunikacji i Systemów Informacyjnych rozwijały się dynamicznie i przenikały wzajemnie. Wywarło to, i nadal wywiera w dużym stopniu, wpływ na współczesne społeczeństwo. Dotyka to wszystkich aspektów współczesnego życia. Krajowe i międzynarodowe instytucje życia kulturalnego, politycznego, gospodarczego, wojskowego, naukowego, a nawet osoby fizyczne coraz bardziej uzależniają się od stałej dostępności usług opartych na tych technologiach. W efekcie łączy się to z zapotrzebowaniem na skuteczne, solidne i tanie systemy łączności oraz systemy informacyjne, wyrażanym przez rząd i źródła prywatne.

Organizacja Telekomunikacji

2. Organizacja telekomunikacji także uległa zmianie w większości krajów członkowskich Paktu. W przeszłości za całość uregulowań dotyczących łączności, infrastrukturę i świadczenie usług odpowiedzialny był jeden resort rządowy, zwykle określany jako PTT. Na przestrzeni ostatnich kilku lat w paru krajach doszło do rozdziału funkcji regulacyjnych od świadczenia usług i budowy sieci. Sprawy regulacyjne zazwyczaj nadal leżą w kompetencji jednostki rządowej zwanej w niniejszym dokumencie „Władzą Krajową".
3. Budowę infrastruktury telekomunikacyjnej oraz świadczenie usług w ramach infrastruktury można rozdzielić pomiędzy kilka jednostek. Każda z. tych jednostek może stanowić własność rządu danego kraju lub będzie w rękach prywatnych, zależnie od stopnia liberalizacji i prywatyzacji. W niniejszym dokumencie osoby zbiorowo odpowiedzialne za świadczenie usług telekomunikacyjnych określa się mianem „Operatorów" (TOs). W razie konieczności rozróżnienia, osoby odpowiedzialne za infrastrukturę określa się jako „Operatorów Sieci", natomiast odpowiedzialnych za świadczenie usług świadczonych w ramach infrastruktury określa się jako „Usługodawców".

Struktura CEP

4. CEP w zasadzie nadal pozostaje w kompetencjach danego kraju tym niemniej, aby polityka Paktu była skuteczna i spójna, samostanowienie i zakres odpowiedzialności danego kraju musi umożliwiać maksymalna współpracę bezpośrednią między, stolicami oraz na szczeblu NATO. SCEPC to główna płaszczyzna koordynacji na szczeblu poniżej Rady NATO (której podlega), odpowiedzialna za całość CEP NATO, obejmuje takie dziedziny jak transport, zasoby strategiczne, produkcja przemysłowa,

Personel i Zarządzanie

24. Należy wziąć pod uwagę możliwość braków kadrowych w wypadku powszechnej mobilizacji w kraju oraz potrzebę zapewnienia, za pomocą odpowiedniej akcji krajowej, wykwalifikowanego personelu telekomunikacyjnego. Wyznaczony personel musi otrzymać odpowiednie instrukcje i zostać przeszkolony, np. w formie udziału w ćwiczeniach.
25. Należy przygotować:
    - ośrodki zarządzania w sytuacji kryzysowej i/lub kwaterę a czas wojny, w tym zapewnić odpowiednie, bezpieczne środki łączności i procedury do stopniowego przestawienia się, w razie konieczności, na funkcje kryzysowe i wojenne;
    - wzmocnienie organizacji i usług na obszarach, gdzie spodziewane jest wzmożenie działań;
    - należy redukować działania uznane za mające mniejsze znaczenie;
    - ustalenie i wzmocnienie bezpieczeństwa wewnętrznego i zwiększenie personelu na służbie w celu ochrony przed sabotażem, działalnością wywrotowa, itp.;
    - identyfikacja rezerwowych urządzeń, zapasów, możliwości produkcyjnych i remontowych oraz utworzenie rezerw, jeśli to możliwe, do wykorzystania w czasie kryzysu i wojny;
    - informacja i poinstruowanie społeczeństwa o dobrowolnych lub obowiązkowych ograniczeniach w wykorzystaniu usług telekomunikacyjnych stosownie do sytuacji bieżącej

Planowanie Sieci

26. Systemy telekomunikacji cywilnej są przede wszystkim budowane i eksploatowane w celu spełniania zapotrzebowania społeczeństwa w czasie pokoju. Niemniej jednak planowanie w czasie pokoju ma także na celu opracowanie struktury sieci wystarczająco elastycznej, by mogła sprostać zapotrzebowaniu w czasie kryzysu i wojny oraz ograniczyć ewentualne uszkodzenia do stanu pogorszenia możliwego do naprawy.
27. W celu uzyskania koniecznego stopnia elastyczności, należy uwzględnić następujące środki, biorąc pod uwagę konieczność odpowiedniego zrównoważenia wymogów obronnych, wykonalności technicznej i ograniczeń finansowych:
    - w każdym kraju NATO należy wytyczyć kilka tras w oddzielnych rejonach geograficznych;
    - należy maksymalnie zróżnicować trasy łączności kablowej, mikrofalowej i satelitarnej pomiędzy krajami w uznaniu potencjalnych korzyści płynących z raczej sieci kablowych niż innych środków transmisji przy eksploatacji najważniejszych kanałów, w pewnych okolicznościach;
    - połączenia ważnych arterii w taki sposób, aby obejść punkty podatne na uszkodzenia oraz zwiększyć elastyczność sieci; urządzenia rezerwowe należy umieścić na odpowiednich stacjach wzmacniakowych;
    - należy wziąć pod uwagę fakt, że w sytuacji kryzysowej model ruchu będzie różnić się od normalnego w czasie pokoju w kategorii zwiększonego ruchu w celach podstawowych (żywność, surowce, spedycja, transport, itp.), a poza tym zwiększy się natężenie ruchu obronnego; musi istnieć wystarczająca pojemność umożliwiająca dostosowanie do zwiększonego ruchu; aby to osiągnąć, należy w efekcie ograniczyć inne rodzaje ruchu, które też mogą się zwiększyć;
    - normalną praktykę polegającą na kierowaniu ruchu przez jak największą dostępną liczbę tras (przy automatycznym przeciążeniu) należy kontynuować, ponieważ umożliwia do obsługę najważniejszego ruchu w wypadku awarii kilku tras;

    Dobrze zorganizowany, ciągły nadzór nad poszczególnymi częściami składowymi sieci w połączeniu z odpowiednim systemem sprawozdawczości i prawidłowo zorganizowanymi kanałami dyspozycyjnymi ma zasadnicze znaczenie dla nieprzerwanej eksploatacji sieci w warunkach kryzysowo-wojennych (por. Rozdział III).

Instalacje i Urządzenia Telekomunikacyjne

28. W celu osiągnięcia wymaganego stopnia przetrwalności, należy uwzględnić następujące środki, biorąc pod uwagę konieczność odpowiedniego zrównoważenia wymogów obronnych, wykonalności technicznej i ograniczeń finansowych:
    - aby zmniejszyć ryzyko poważnego nadwerężenia usług albo zniszczenia jednego lub kilku centrów, krajowe i międzynarodowe centra przełączające i ośrodki sterowania powinny mieć wzajemne wspomaganie, w uzasadnionym stopniu;
    - należy zapewnić odpowiedni poziom fizycznej ochrony wszystkich części sieci odpowiadających za żywotna łączność, a w szczególności centra przełączające i urządzenia komutacyjne, główne stacje wzmacniakowe, podmorskie kable do stacji końcowych i całość urządzeń stacji radiowych;
    - chociaż obecnie nie uważa się, by EMP (moc elektromagnetyczna) stanowiła poważne ryzyko, należy zawsze pamiętać o potrzebie ochrony przed możliwymi uszkodzeniami. Rozwój techniki i wymogi standaryzacji na polu kompatybilności elektromagnetycznej w pewnym stopniu zapewniają ochronę. Ale teoria i praktyka ochrony EMP to złożone sprawy wymagające wiedzy specjalistycznej;

15. Operatorzy powinni otrzymywać z maksymalnym wyprzedzeniem informacje dotyczące wymogów obronnych, tak by umożliwić im skuteczne wpasowanie ich w tok normalnej działalności (która ma przeważnie charakter komercyjny) oraz by uniknąć opóźnień i ponoszenia dodatkowych kosztów. Łączy się to z koniecznością stałych konsultacji między Operatorami i właściwymi Władzami Krajowymi.
16. Udogodnieniem dla poszczególnych krajów może być połączenie planowania w wypadku sytuacji kryzysowo-wojennej z planowaniem w sytuacjach wyjątkowych oraz w wypadku klęsk żywiołowych lub wywołanych działaniem człowieka. Mimo iż ten ostatni rodzaj planowania nie mieści się w zakresie niniejszego dokumentu, jego charakter będzie często podobny do planowania w wypadku sytuacji kryzysowo-wojennej: tego rodzaju połączenie może okazać się korzystne, szczególnie pod względem finansowym.
17. Istnieje potrzeba konsultacji dwu- i wielostronnych pomiędzy właściwymi władzami krajowymi i operatorami w celu zagwarantowania uwzględnienia wymogów NATO w procesie planowania, wdrażania i nieprzerwanej eksploatacji najważniejszych usług międzynarodowych. Tym niemniej, osiąganie celów NATO na polu telekomunikacji cywilnej w sytuacjach wyjątkowych, kryzysowych i wojennych nie przyniesie spodziewanych korzyści, jeżeli pozostałe Kraje Członkowskie nie podejmą stosownych działań na rzecz zapewnienia usług. Z uwagi na to pożądane jest, by Kraje członkowskie dokonywały wymiany informacji w temacie środków, jakie okazały się najbardziej skuteczne i dogodne do podwyższania potencjalnej dostępności sieci i usług telekomunikacyjnych w sytuacjach wyjątkowych, kryzysowych i wojennych.
18. Z uwagi na znaczne zróżnicowanie uwarunkowań w poszczególnych krajach wskazane jest, by CCPC zaleciło bardzo dokładną formę mechanizmu konsultacji, koordynacji i wymiany informacji. Istotnym elementem tego mechanizmu będzie zachęcanie Krajów Członkowskich do aktywnego uczestnictwa w planowaniu i pracach koordynacyjnych prowadzonych przez CCPC. Jeżeli rozwiązanie pewnych sytuacji w drodze rozmów dwustronnych okaże się niemożliwe, podobnie jak likwidacja niedociągnięć w zakresie łączności w sytuacjach wyjątkowych, kryzysowych i wojennych w toku normalnego rozwoju systemów międzynarodowych, sprawa niezwykle ważna będzie zwrócenie uwagi CCPC na te sprawy i uzyskać informacje i ewentualna koordynację ze strony CCPC.
19. Wyniki badań innych ciał międzynarodowych (takich jak Międzynarodowa Unia Telekomunikacyjna (ITU), CEPT, Unia Europejska, OECD, itp.) mogą mieć znaczenie dla NATO, ponieważ mogą wpłynąć na międzynarodowa politykę telekomunikacyjna i dostarczyć dodatkowych wskazówek i środków ochronnych. Z uwagi na to CCPC powinno zapoznać się z wynikami odpowiednich badań.

Koordynacja w Sytuacjach Kryzysowo-Wojennych

20. W sytuacjach kryzysowo-wojennych sieci i usługi telekomunikacyjne muszą poradzić sobie z nagłymi zmianami natężenia ruchu oraz pilną potrzebą wspomagania działań obronnych. Zakres szkód w sieci może różnić się znacznie w zależności od kraju oraz w obrębie poszczególnych krajów. W tych warunkach głównych działań operatorów polegających na budowaniu, konserwacji i przywracaniu łączności międzynarodowej nie jest możliwe bez odpowiedniej koordynacji.
21. W zależności od decyzji krajowych, operatorzy powinni zorganizować przejście z fazy kryzysu do z organizacji zaplanowanej na czas wojny. Do środków tych zalicza się:
    - uruchomienie środków bezpiecznej komunikacji w sprawach koordynacji na płaszczyźnie międzynarodowej; oraz nałożenie ograniczeń bezpieczeństwa na kanały używane zazwyczaj w czasie pokoju (PSTN, linie telegraficzne i telefoniczne) w celu zapobieżenia przecieków tajnych informacji dotyczących lokalizacji i zakresu uszkodzenia sieci;
    - zorganizowanie wymiany raportów ad hoc (TELINCREPS) i raportów sytuacyjnych (TELSITREPS) pomiędzy krajowymi ośrodkami sterowania;
    - nawiązanie kontaktów z odpowiednimi organami władz krajowych odpowiedzialnymi za podejmowanie decyzji w sytuacji, kiedy urządzenia komercyjne przestaną wystarczać do spełniania wymogów obronnych; należy określić priorytety.
22. W wypadku katastrofalnego uszkodzenia sieci użytku publicznego oraz kiedy planowana koordynacja w sytuacji wyjątkowych jest niemożliwa, potrzebne może okazać się wdrożenie awaryjnych środków koordynacji na szczeblu krajowym lub, jeśli to konieczne - na niższym szczeblu. Zadaniem tym można obarczyć Oficera Łącznikowego ds. Telekomunikacji (TLO) z poszczególnych krajów; TLO będzie pierwszym punktem kontaktowym.

Środki do Uwzględnienia

23. W ramach działań w czasie pokoju Operatorzy muszą reagować na szereg sytuacji mających wpływ na ich zdolność obsługi ruchu i świadczenia usług. Tryb działania Operatorów w czasie pokoju winien być kontynuowany w możliwym zakresie w razie sytuacji kryzysowej lub wojny. Tym niemniej już w czasie pokoju Operatorzy muszą planować i przygotowywać się do okoliczności wyjątkowych, jakie mogą zaistnieć w wypadku eskalacji kryzysu. Poniższe punkty zawierają opis kilku czynników, jakie należy rozważyć.

systemy łączności zostały zaprojektowane tak, by funkcje sterowania zarządzania siecią były uruchamiane automatycznie lub ręcznie. Funkcje sterowania można zastosować do różnych rodzajów ruchu lub do poszczególnych połączeń tego samego rodzaju w zależności od miejsca ich przeznaczenia i prawdopodobieństwa realizacji. Skutek oddziaływania funkcji sterowania na ruch może mieć charakter ekspansywny lub ochronny w zależności od rodzaju zastosowanej funkcji, punktu aplikacji i elementu ruchu stanowiącego przedmiot sterowania. Przykładem regulacji ekspansywnej byłoby udostępnienie większej ilości tras dla ważnych rozmów. Przykładem regulacji restryktywnej byłoby ograniczenie nacisku na urządzenia komutacyjne poprzez ograniczenie ilości dopuszczonego ruchu.

36. Bieżące doświadczenia wskazują, że w czasie kryzysu zapotrzebowanie klientów na publiczne usługi komutowane wzrasta. O ile nie zostaną wprowadzone funkcje sterowania w obrębie zarządzania siecią, liczba zrealizowanych połączeń będzie niższa niż normalnie Funkcje sterowania, które można będzie wykorzystać do zapewnienia realizacji połączenia lub realizacji najważniejszych połączeń, obejmują:
    - Wyłączenie najważniejszych połączeń z funkcji sterowania zarządzania sieci, tak by rozmowy te można było zrealizować w okresach krytycznych;
    - Specjalne zastosowanie funkcji sterowania zarządzania siecią umożliwiających identyfikację połączeń uprzywilejowanych, takie jak zapewnienie pierwszeństwa dostępu do wolnej pojemności;
    - Ukierunkowanie magistrali w celu sterowania liczba połączeń, zarówno wchodzących, jak i wychodzących;
    - Zapobieganie wybieraniu określonych numerów kierunkowych państw i miast oraz numerów kierunkowych centrali przez nieuprawnionych użytkowników, stacje i magistrale poprzez blokowanie połączeń na tych numerach (np. blokowanie numerów kierunkowych);
    - Rekonfiguracja sieci w celu zmiany trasy połączeń przez inne centra przełączające w tym samym kraju lub kraju tranzytowym;

Udostępnianie dodatkowych usług lub kanałów dla ważnych użytkowników w sytuacjach awaryjnych.

37. W czasie pokoju funkcje i techniki sterowania w ramach zarządzania siecią przyniosą operatorom sieci korzyści komercyjne, natomiast w czasie kryzysu lub wojny będą miały zasadnicze znaczenie dla nieprzerwanego świadczenia usług telekomunikacyjnych. Z uwagi na tę poważna rolę trzeba zapewnić ciągłość zatrudnienia u operatorów sieci publicznych w Ośrodkach Zarządzania Siecią (NMCs) oraz ulokować je w chronionych kwaterach daleko od potencjalnych celów ataku. Łącza komunikacyjne z NMCs z węzłami sieci winny charakteryzować się duża odpornością. Jeśli to możliwe, NMCs powinny dublować się lub należy zapewnić możliwość wykonywania ich funkcji na szczeblu regionalnym lub lokalnym albo w Międzynarodowych Centrach Przełączających (ISCs).

Uprzywilejowany Dostęp do Krajowych/Międzynarodowych Usług Telekomunikacyjnych dla Najważniejszych Użytkowników

38. W sytuacjach, w których środki zarządzania siecią nie sprawdzają się, trzeba zastosować funkcje sterowania, które będą usuwać próby połączeń z zatłoczonych centrów przełączających Może wystarczyć jedynie możliwość usuwania prób połączeń określonej grupy użytkowników i zawężenie dostępu wyłącznie do najważniejszych użytkowników. Należy zażądać, by operatorzy zaplanowali i przygotowali środki umożliwiające ograniczanie użytkowania publicznej sieci telefonicznej w sytuacjach katastrof na duża skalę w czasie pokoju oraz w czasie kryzysu i wojny. Ich uruchomienie należy przeprowadzać po kierownictwem władz krajowych. Z uwagi na to ostatnie Operatorzy mogą dodatkowo mieć możliwość wycofania usług i zmiany kierunku tras w sytuacjach podyktowanych ogólnymi potrzebami obronnymi.
39. Ważne jest, by użytkownicy uważani za pełniących ważne funkcje w ogólnym funkcjonowaniu społeczeństwa mieli zapewniony dostęp do sieci komutacyjnych użytku publicznego (w szczególności sieci telefonicznych) dzięki konkretnym środkom uzgodnionym z Operatorami. Władze centralne kraju (współpraca władz cywilnych i wojskowych) powinny być odpowiedzialne, po pierwsze za ustalenie, jakiej kategorii użytkownicy są najważniejsi dla sprawnego funkcjonowania społeczeństwa. Kategorie użytkowników obejmują odgrywających żywotną rolę dla ogólnego funkcjonowania społeczeństwa; ogólnie ważnych; oraz mało ważnych lub nieważnych. Przy określaniu kategorii użytkowników władze centralne kraju powinny brać pod uwagę funkcje, których spełnianie zależy od telekomunikacji krajowej, które są wyszczególnione w Rozdziale IV.
40. Na podstawie wytycznych uzyskanych od władz centralnych, organy władzy na szczeblu regionalnym powinny sporządzić spis najważniejszych użytkowników. Listy te powinny być przesyłane bezpośrednio do właściwych organizacji telekomunikacyjnych, które podejmą stosowne działania dla zapewnienia nieprzerwanego dostępu. Natomiast jeżeli chodzi o własne wymagania Operatorów niezbędne do spełnienia wymogu gotowości, powinni oni sporządzić sami odpowiednie listy i je realizować.

Przywrócenie Międzynarodowych Systemów Transmisji

41. Międzynarodowe systemy transmisji tworzą wzajemne połączenia między ISCs telekomunikacyjnych usług komutowanych użytku publicznego i można je kierować bezpośrednio między dwoma krajami lub krajami trzecimi - tranzytowymi. Ustalone i skoordynowane plany i procedury międzynarodowe zostały

- należy zapewnić w miarę możliwości alternatywne, oddzielne wloty kabli do centrów telekomunikacyjnych;
- przy podejmowaniu decyzji o lokalizacji najważniejszych instalacji telekomunikacyjnych, magazynów i warsztatów, należy wykorzystać naturalne ukształtowanie terenu dla dodatkowej ochrony;
- należy odpowiednio zorganizować rezerwy mocy i związane z tym zapasy paliw w głównych instalacjach;
- aby ułatwić przywrócenie łączności trzeba utworzyć rezerwę części zapasowych składowanych na miejscu;
- aby zminimalizować ryzyko wykorzystania instalacji radiowych w sieciach telekomunikacyjnych do lokalizacji, naprowadzania na cel, gromadzenia informacji i sabotażu, należy zastanowić się nad zmniejszeniem emisji radiowych za pomocą Sterowania Emisji, EMCON), w uzasadnionych wypadkach.

Usługi Pomocnicze

29. W czasie pokoju w procesie planowania usług pomocniczych należy poważnie zająć się wzrostem zapotrzebowania na takie usługi w czasie kryzysu i wojny. Aby sprostać temu zapotrzebowaniu, należy wziąć pod uwagę konkretne środki:
    - przy ocenie i zakupie urządzeń telekomunikacyjnych tam, gdzie inne czynniki są zrównane, należy zastosować preferencje do urządzeń uważanych za bardziej odporne w warunkach wojennych;
    - należy nabyć dodatkowe zapasy najważniejszych elementów urządzeń i rozprowadzić je między odpowiednimi lokalizacjami, tam gdzie można je będzie wykorzystać do szybkiego przywrócenia usług;
    - należy zapewnić urządzenia ruchome i możliwe do transportu, w tym awaryjne bloki energetyczne z pełna dokumentacją, wspomaganiem logistycznym i wyszkolonym personelem, albo zwiększyć ich liczbę do tymczasowego wykorzystania po ciężkich uszkodzeniach;
    - należy zorganizować skuteczne jednostki remontowe, które będą w stanie sprostać wymogom sytuacji kryzysowych i wojennych;
    - aby zwiększyć potencjał usług pomocniczych w warunkach kryzysowych i wojennych, należy poczynić przygotowania do używania urządzeń rezerwowych, zapasów, itp. zgodnie z założeniami punktu 25.

III. KONSERWACJA i EKSPLOATACJA

Zasady Ogólne

30. W sytuacji wyjątkowej, w czasie kryzysu i wojny publiczne sieci telekomunikacyjne powinny podołać zmianom w modelach ruchu oraz pilnym potrzebom wspomagania działań aliantów. W czasie wojny, nawet po ciężkich zniszczeniach, warunki w obrębie danego kraju mogą się tak różnić, że kiedy na wielu obszarach usługi są w stanie kompletnego zniszczenia, w innych możliwe jest ich normalne funkcjonowanie. W takich okolicznościach działania, cywilnych władz telekomunikacyjnych polegają głównie na zapewnieniu nieprzerwanego świadczenia najważniejszych krajowych usług dla kraju i zagranicy koordynując je, w miarę konieczności, z innymi organami administracyjnymi.
31. W normalnej sytuacji wzrost popytu na usługi międzynarodowe jest zaspokajany dzięki postępowi technologicznemu i zaawansowaniu technik operacyjnych oraz dzięki opracowaniu większych, przede wszystkim cyfrowych, systemów transmisji i systemów komutacyjnych, razem z wspólnym kanałem sygnalizacyjnym, dla zapewnienia wymaganej pojemności systemu. To spowodowało, że międzynarodowa sieć telekomunikacyjna charakteryzuje się wysokim stopniem połączenia i jest interakcyjna.

Zarządzanie Siecią

32. W kontekście niniejszego dokumentu Zarządzanie Siecią definiuje się jako zbiór działań potrzebnych do monitorowania i konserwacji części składowych sieci mających na celu zapewnienie maksymalnego wykorzystania usług świadczonych w sieci, w każdej sytuacji.
33. Do przeciążenia i zatorów sieci może dojść z kilku powodów. Przykładowo z powodu:
    - awarii elementów sieci, w tym uszkodzeń;
    - uwarunkowań zewnętrznych powodujących duża ilość połączeń (np. kryzysy naturalne albo spowodowane działaniem człowieka);
    - zatory w połączonych sieciach.
34. O ile nie zostaną szybko podjęte działania mające na celu kontrolowanie skutków takich wydarzeń, przeciążenia lub zatory mogą rozprzestrzeniać się spowodować degradację pozostałych części sieci krajowych i międzynarodowych Działania w ramach Zarządzania Siecią są prowadzone w celu ograniczenia wpływu takich skutków.
35. Dzięki funkcjom sterowania Zarządzania Siecią możliwa jest zmiana strumienia ruchu w sieciach, co winno być oparte na parametrach wydajności sieci, sygnalizujących potrzebę działania. Nowoczesne

użytkowników w sytuacji kryzysu i wojny musi być obowiązkową powinnością operatorów cywilnej sieci telekomunikacyjnej i dostawców usług. Władze krajowe powinny zapewnić, aby operatorzy sieci i dostawcy usług na całym obszarze NATO byli zobowiązani liczyć się z ta odpowiedzialnością w ich zwykłych działaniach handlowych w okresie pokoju.

52. W celu sprawowania ogólnego kierownictwa nad własnymi operatorami cywilnej sieci telekomunikacyjnej i dostawcami usług, Kraje powinny w swoim planowaniu wyszczególnić te funkcje, których podstawowe aspekty w przypadku stanu pogotowia lub wojny zależałyby od łączności cywilnej. Lista funkcji uważanych za istotne dla zwalczania kryzysu przez NATO, tak cywilnych jak i wojskowych, znajduje się na końcu niniejszej części opracowania (Paragraf 55). Lista ta nie jest· ułożona zgodnie z waga funkcji: Kraje musza zadecydować o względnej wartości funkcji na podstawie istniejącej sytuacji i warunków krajowych.
53. Chcąc wyjść naprzeciw wymaganiom jakie stawia tym funkcjom sieci i usług kryzys i wojna, operatorzy sieci i dostawcy usług w telekomunikacji cywilnej powinni zwracać szczególna uwagę na potrzebę szybkości dostawy sieci i usług; oraz, w zakresie określonym praktyka, przywrócenia tych sieci i usług tak szybko jak to możliwe po awarii, jeśli według priorytetów ustalonych przez Władze Krajowe jest to właściwe.
54. Niniejsza część Kompendium jest podzielona na następujące kategorie: nośniki transmisji, tryby działania, usługi działające w oparciu o sieć i inne usługi, które mogą działać niezależnie od sieci.

Nośniki transmisji

Nośnikami transmisji są wszelkie ośrodki, które są, lub mogą być, używane dla przenoszenia sygnału, zwykle w formie modulowanych fal radiowych, świetlnych lub akustycznych, z jednego punktu do drugiego, takie jak kabel, powietrze lub włókna optyczne. Typy środków transmisji zawierają między innymi skrętkę wieloparową. kabel koncentryczny, propagację troposferyczną, włókna optyczne, mikrofale, przekazy satelitarne i fale wysokiej częstotliwości.

Nośnikami transmisji używanymi w telekomunikacji były początkowo linie napowietrzne, a w miarę rozwoju zaczęto używać kabli wieloparowych, kabli koncentryczne, otwarta przestrzeń (dla HF, systemów mikrofalowych i systemów satelitarnych) oraz najnowszych nośników - kabli światłowodowych.

Kabel *typu skrętka*

Skrętka składa się z pary drutów miedzianych i jest zwykle używana do stworzenia pojedynczego kanału dla przekazu częstotliwości fonicznych pomiędzy dwoma punktami. Aby umożliwić działanie wielu kanałów, setki izolowanych drutów są połączone w jeden duży kabel, w którym każda z par drutów ma inny kod barwny dla łatwej identyfikacji. Podczas gdy skrętki są wystarczające do przekazu informacji głosowych i danych na małe dystanse, nie są one odpowiednie dla szybkiej transmisji danych na długie dystanse, ze względu na ich wrażliwość na zakłócenia (np. przesłuchy, interferencje, itp.) które powodują słabą jakość komunikacji.

Kabel *koncentryczny*

Ten typ kabla składa się z przewodzącego cylindra z izolacja wokół położonego centralnie drutu. Kabel koncentryczny jest ekranowany w celu zmniejszenia interferencji ze źródeł zewnętrznych. Kabel koncentryczny może przenosić na znaczne wyższej częstotliwości niż skrętka, zapewniając szybszą transmisję danych i będąc w stanie przenosić znacznie szersze pasmo. Kabel może zawierać wiele przewodów koncentrycznych plus grupy skręconych par, które mogą być używane do przekazywania sygnałów sterujących w przypadku usług przekazu na duże odległości (> 200 km).

Propagacja troposferyczna

W transmisji przy pomocy propagacji troposferycznej, troposfera jest używana w celu rozpraszania i odbijania fal radiowych z powrotem na ziemię. Z dwoma antenami o wysokiej kierunkowości skierowanymi na troposferę wystarczająca ilość energii fal radiowych jest odbijana z powrotem, co daje w efekcie bardzo pewny system komunikacji ponad-horyzontalnej z efektywnym zasięgiem pasma w zakresie 150 do 180 kilometrów. Takie systemy są używane w przypadkach gdy nie jest możliwe lub nie opłaca się użycie linii naziemnej lub mikrofalowej. Częstotliwości fal zawierają się w obrębie 900-5000 MHz i przenoszą kilkaset kanałów łączności fonicznej na krótsze dystanse. Podlegają one tłumieniu, co jest zwykle przezwyciężane przez użycie dwóch rozstawionych w pewnej odległości nadajników i odbiorników. Troposfera jest niższa warstwa atmosfery od poziomu morza do wysokości ok. 11 kilometrów.

Włókna optyczne

System transmisji włóknami optycznymi korzysta ze światła o ultra wysokich częstotliwościach dla przekazywania głosu, danych, obrazów i sygnałów wideo po plastykowym lub szklanym włóknie. System ten składa się ze źródła światła, włókien optycznych, oraz przyrządu wykrywającego światło. Systemy transmisji włóknami optycznymi oferują wyższe parametry od konwencjonalnych systemów okablowania, w tym:. szeroki zakres, niewielkie tłumienie, wysoka integralność danych, niewrażliwość na zakłócenia elektryczne i radiowe, wysokie poziomy bezpieczeństwa i większa trwałość. To sprawia,

uzgodnione przez Operatorów można wykorzystać do przywrócenia części normalnych systemów transmisji, które zostały stracone z powodu awarii lub planowej przerwy.

42. W czasie kryzysu i wojny stała realizacja planów dotyczących przywrócenia może być utrudniona z uwagi na kumulację uszkodzeń międzynarodowych systemów transmisji, jako że łącza przewidziane w planach przywrócenia mogą być już wykorzystane lub nie funkcjonować. Wówczas konieczne będzie zorganizowanie działań na rzecz przywrócenia ad hoc, przy użyciu najlepszych urządzeń, jakie jeszcze pozostały do dyspozycji. Konieczne będą konsultacje między operatorami telekomunikacji cywilnej oraz między nimi a krajowymi władzami cywilnymi i wojskowymi.
43. Priorytetów obowiązujących w czasie pokoju, które przede wszystkich uwzględniają interes ekonomiczny, nie da się zastosować w wielu sytuacjach w czasie kryzysu i wojny. W wypadku poważnych i skumulowanych uszkodzeń normalny cel - czyli przywrócenie operacyjności całego systemu - może być niewykonalny, a dostępne urządzenia trzeba wtedy rozdysponować zgodnie z zarządzeniem właściwych władz krajowych. Należy wziąć pod uwagę kanały cywilne i wojskowe zarejestrowane przez Agencję ds. Łączy Dalekosiężnych Paktu (ALLA) oraz inne wymagania cywilne, w tym usługi użyteczności publicznej. Poszczególne narody winny ustalić cywilne międzynarodowe kanały wydzielone, które uważa się za mające istotne znaczenie dla ogólnych możliwości obronnych Paktu i z uwagi na to których funkcjonowanie w czasie kryzysu i wojny należy zapewnić.

Łączność z Krajami Nie Należącymi do Paktu

44. W czasie kryzysu należy dołożyć wszelkich starań w celu zapewnienia nieprzerwanego użytkowania międzynarodowych usług telekomunikacyjnych, użytku publicznego i wydzielonych. W szczególności łączność dyplomatyczna oraz inne ważne rodzaje komunikacji pomiędzy członkami Paktu oraz między rządami krajów należących i nie należących do Paktu ma istotne znacznie dla podejmowania wysiłków na rzecz zapobiegania sytuacjom kryzysowym, a w wypadku braku powodzenia - koniecznych dla przywrócenia pokoju. Tym niemniej w czasie kryzysu i wojny konieczne może okazać się wprowadzenie środków kontrolnych w taki sposób, aby umożliwić podjęcie odpowiednich kroków w zakresie bezpośrednich i pośrednich torów telekomunikacyjnych między krajami należącymi do Paktu i nie będących jego członkami, zgodnie z panującymi warunkami.
45. W tym kontekście słowo "kontrola" oznacza regulację kanałów i ruchu jaki się w nich odbywa; nie ma to natomiast związku z treścią przekazywanych informacji.
46. Operatorzy, po otrzymaniu stosownych poleceń od właściwych władz krajowych, zastosują środki kontrolne wobec międzynarodowych usług telekomunikacyjnych, zarówno użytku publicznego jak i wydzielonych.
47. Kraje NATO będą musiały uzgodnić aspekty techniczne środków kontrolnych, jakie będą stosować Operatorzy. Mogą one stanowić przedłużenie normalnych funkcji zarządzania siecią w czasie pokoju, opisanych wyżej.
48. Mając na uwadze skuteczna kontrolę nad międzynarodowymi usługami telekomunikacyjnymi, zarówno użytku publicznego jak i wydzielonymi, ważne jest by kraje NATO jednocześnie uruchomiły uzgodnione przez siebie środki kontrolne zgodnie z odpowiednimi wytycznymi NATO.

Krajowe Sieci Awaryjne

49. Można zbudować sieci oddzielone od usług telekomunikacyjnych użytku publicznego do wykorzystania przez władze krajowe w sytuacji wyjątkowej, w czasie kryzysu lub wojny. Takie krajowe sieci awaryjne są zazwyczaj ograniczone pod względem pojemności ruchu. Po warunkiem przyjęcia odpowiedniego międzynarodowego systemu sygnalizacyjnego i możliwości uzyskania w wyniku tego dobrej jakości transmisji, uważamy za korzystne połączenie krajowych sieci awaryjnych w czasie pokoju lub w początkowym stadium sytuacji kryzysowej w celu umożliwienia komunikowania się przez najważniejszych użytkowników. Może się okazać konieczne udoskonalenie sieci dla pomieszczenia dodatkowego ruchu.
50. Aby wykorzystać łącza sprzęgające do realizacji połączeń w warunkach wojennych, łącza powinny być bardzo mocne i odporne, tak by zapewnić wysokie prawdopodobieństwo nieprzerwanej łączności Chodzi tu o alternatywny wybór trasy, wielobramkowa dystrybucja kanałów, a ponadto można rozważyć sposoby umocnienia sieci. Biorąc pod uwagę ograniczona pojemność krajowych sieci awaryjnych, poszczególne kraje mogą zechcieć sprawować pewnego rodzaju kontrolę nad połączeniami przychodzącymi z zewnątrz do ich sieci; półautomatyczne usługi łączenia, gdzie operator znajduje się w kraju docelowym, zaspokoi to zapotrzebowanie i zapewni dodatkowa pomoc w realizacji połączenia dla dzwoniącego Zatrudnieni operatorzy powinni być dwujęzyczni, oprócz języka ojczystego winni znać angielski lub francuski.

IV. USŁUGI TELEKOMUNIKACYJNE DLA NAJWAŻNIEJSZYCH UŻYTKOWNIKÓW

Informacje Ogólne

51. Sieci i usługi łączności cywilnej są częścią całości zasobów telekomunikacyjnych dostępnych dla NATO w przypadku stanu pogotowia, kryzysu lub wojny. Sprawne działanie tych sieci i usług dla dobra

satelitarne są coraz częściej wykorzystywane przez organizacje które najprawdopodobniej będą odgrywać kluczowa rolę w likwidacji stanów kryzysowych, sieci te mogą okazać się przydatne dla krajów NATO na wypadek rozerwania publicznych naziemnych krajowych i międzynarodowych sieci telekomunikacyjnych.

Sieci satelitarne maja szereg zalet. Główna zaletą jest to, że dzięki przemieszczaniu się terminali satelitarnych, mogą szybko świadczyć usługi odizolowanym użytkownikom. Sieci satelitarne oferują również wybór pomiędzy rozsyłaniem sygnału do kilku stacji odbiorczych a przesyłaniem sygnału pomiędzy dwoma terminalami. W porównaniu z innymi systemami działającymi w oparciu o fale radiowe, oferują szersze pasmo, mniejszą ilość błędów i wyższej jakości sygnały.

Sieci prywatne

Sieci prywatne są tworzone i używane zwykle przez jedną określoną organizację. Wyposażenie i sprzęt przełączajacy mogą albo należeć do operatora kablowego lub dostawcy usług, lub ewentualnie użytkownik takiej sieci może mieć możliwość wynajmu lub zakupienia sprzętu potrzebnego do transmisji.

Sieć prywatna jest skonfigurowana w taki sposób aby spełniała wymagania określonego użytkownika. Charakteryzuje się własnym systemem numerowym, który jest niezależny od publicznego i z tego powodu może zaoferować kilka poważnych atutów, takich jak stałe wybieranie według określonych numerów lub spisu telefonów użytkownika, połączenia stacja stacja przy pomocy urządzeń do transmisji pracujących w sieci i osobno bez potrzeby operatora, oraz optymalny routing rozmów telefonicznych. Organizacja może sprawować całkowita kontrolę nad siecią i zapewniać zasoby ludzkie i logistyczne dla potrzeb korzystania z sieci i jej utrzymywania. Możliwe jest również zlecanie niektórych aspektów utrzymania sieci na zewnątrz

Wirtualne Sieci Prywatne

Wirtualne Sieci Prywatne są odpowiednikiem sieci prywatnej, zaprojektowanej logicznie w ramach sieci publicznej i dzięki temu korzystającej z ekonomiczności skali i cech sieci publicznej. Wirtualna sieć prywatna eliminuje, lub częściowo eliminuje, potrzebę stałych linii dzierżawionych ponieważ zapewnia na żądanie obwody i zasoby, które mogą być dynamicznie przypisywane. Zasoby Wirtualnej Sieci Prywatnej są używane tylko w chwili transmisji informacji w sieci. Użytkownik ma dostęp do swego rodzaju rosnącej w miarę potrzeb sieci prywatnej przy znacznie mniejszej inwestycji i kosztach administracyjnych.

PLMN - Lądowa Publiczna Sieć Przenośna

PLMN jest stworzona i działa w celu dostarczania społeczeństwu usług ruchomej telekomunikacji naziemnej. PLMN może być uważana za rozszerzenie, lub jako integralna część stałej sieci (np. sieci PSTN lub publicznej sieci telekomunikacyjnej); jednakże, użytkownik końcowy nie jest ograniczony do tej sieci. Funkcjonalnie PLMN-y mogą być uważane za niezależne podmioty telekomunikacyjne bez względu na to czy istnieje jakiekolwiek połączenie ze stałą siecia.

PLMN-y zasadniczo składają się ze stałych elementów, które również stanowią połączenia pomiędzy stałymi sieciami, oraz systemu radiowego, który zapewnia komunikację dla ruchomych elementów obsługiwanych przez użytkowników. System radiowy może być całkowicie naziemny lub korzystać z usług satelitów i zwianych z nimi terminali naziemnych.

Chociaż jednym z obecnych ograniczeń analogowych PLMN jest zależność jakości sygnału od zjawiska cienia i efektów wielokrotnego odbicia od przedmiotów w terenie i wysokich budynków jak również możliwość spadku jakości sygnału wraz ze wzrostem odległości, prowadzone są badania nad tym jak poprawić tę sytuację. Powyższy efekt występuje w mniejszym stopniu w systemach cyfrowych.

Pośród usług telekomunikacyjnych, które mogą korzystać z PLMN są telefon, telex, fax i usługi przekazywania wiadomości. PLMN może również być znany jako „przenośne radio" lub „radio komórkowe".

Jednym z najważniejszych PLMN jest sieć GSM, system cyfrowy obejmujący dużą część Europy i stopniowo przyjmowany przez inne kraje.

Dalszy rozwój PLMN obejmuje komunikację ruchoma dla użytkowników indywidualnych z możliwością kontaktu z całym światem przy użyciu kieszonkowej stacji.

Ruchome sieci naziemne mogą być ograniczone do wyłącznego użytku przez departamenty i agencje rządowe, prywatne firmy lub inne grupy lub osoby. W niektórych wypadkach takie sieci mogą mieć połączenia ze stałymi sieciami publicznymi takimi jak PSTN, w oparciu o przepisy krajowe.

Sieć Zintegrowanych Usług Cyfrowych (ISDN)

ISDN jest zintegrowana siecią cyfrowa, w której te same przełączniki cyfrowe i ścieżki cyfrowe są używane do ustanowienia połączeń dla różnych typów informacji {np. głos, dane, wideo). Zasadniczo oparty na istniejącej zintegrowanej sieci cyfrowej, ISDN ustanawia połączenia cyfrowe pomiędzy użytkownikami końcowymi za pomocą określonego zestawu standardowych wielofunkcyjnych sieciowych interfejsów użytkownika. Sieć może integrować istniejącą sieć telefoniczna, sieć transmisji

że systemy transmisji włóknami optycznymi mogą zapewnić bardzo szybkie tempo transmisji i dlatego są w stanie przekazywać wiele rozmów jednocześnie.

Mikrofale

Systemy mikrofalowe posługują, się najwyższym zakresem w spektrum częstotliwości radiowych (powyżej 760 MHz). Mikrofale są najczęściej używane do komunikacji dalekiego zasięgu. Systemy mikrofal są odporne na negatywne oddziaływania którym podlegają druty miedziane i zapewniają szersze pasmo. Systemy transmisji składają się ze stacji przekaźnikowych, z których każda jest ustawiona tak aby utrzymywać bezpośrednią (w zasięgu wzroku) transmisję do swoich dwóch sąsiadujących stacji przekaźnikowych. Stacje przekaźnikowe otrzymują sygnały, wzmacniają je, a następnie przekazują je do następnej znajdującej się po drodze stacji przekaźnikowej.

Satelita

Systemy satelitarne używają albo satelitów geostacjonarnych albo innych satelitów orbitujących wokół Ziemi w celu przekazania transmisji od jednej stacji naziemnej do drugiej lub większej ilości stacji naziemnych. Satelita geostacjonarny jest zaprojektowany w ten sposób, aby działać jako telekomunikacyjny przekaźnik radiowy i zwykle jest umieszczony na orbicie geosynchronicznej 35,800 kilometrów ponad równikiem, tak, że z ziemi wydaje się, jakby się nie poruszał w przestrzeni. Inne satelity na orbicie okołoziemskiej, jak na przykład na orbicie polarnej, są również używane. Stacja naziemna jest zbiorem sprzętu telekomunikacyjnego i zawiera generatory sygnału, nadajnik, odbiornik i antenę, która otrzymuje (i zwykle transmituje) sygnały do / z satelity telekomunikacyjnego. Systemy satelitarne są idealne dla urządzeń nadawczych w krajowej i międzynarodowej komunikacji na duże odległości.

Fale radiowe o wysokiej częstotliwości

Komunikacja na duże odległości jest możliwa przy użyciu fal radiowych o wysokiej częstotliwości ponieważ częstotliwości te pozwalają falom radiowym odbijać się od jonosfery i z powrotem na ziemię, tyle razy ile jest potrzebne dla osiągnięcia przez nie miejsca przeznaczenia. Częstotliwości zawierają się zwykle w zakresie od 3 MHz do 30 MHz. Ze względu na ruchy i zmiany jonosfery, częstotliwości te podlegają wytłumieniu, zniekształceniom i okresowym zanikom. Konieczne jest działanie wykwalifikowanych operatorów lub profesjonalnych urządzeń aby utrzymać trwałe i pewne połączenia Dlatego też transmisja danych jest utrudniona, o ile nie zostaną zastosowane wyjątkowe środki ostrożności mające na celu wykrycie i korektę błędów.

Sieci

Sieć składa się z obwodów lub innych połączeń, za pomocą których połączone są między sobą punkty komunikacyjne w taki sposób, że jedno urządzenie przełączające może być połączone z innym urządzeniem przełączajacym w celu umożliwienia komunikacji pomiędzy użytkownikami. Poniższa część przedstawia opis różnych sieci dostępnych i mogących sprostać wymaganiom projektantów systemów telekomunikacyjnych.

Publiczna sieć telefoniczna

Publiczna sieć telefoniczna składa się z linii telekomunikacyjnych i central rozmieszczonych w ten sposób, aby umożliwić użytkownikom, na skalę całego świata, dokonywanie połączeń telefonicznych z dowolnym innym użytkownikiem systemu. Jest to najbardziej dostępna, i najszerzej używana sieć na świecie. Może się nią również odbywać, za pomocą odpowiedniego modemu, przekaz danych.

Publiczna komutowana sieć telekomunikacyjna

Publiczna komutowana sieć telekomunikacyjna składa się ze ścieżek transmisji i przełączników rozmieszczonych w ten sposób, że umożliwiają użytkownikom przekazywanie dane z jednego miejsca do drugiego. Ma szersze pasmo i szybkość przekazu danych niż publiczna sieć telefoniczna i jest ograniczona tylko przez właściwości używanych przełączników, nośników transmisji i końcowych urządzeń

Sieci satelitarne

Wprowadzenie do sieci telekomunikacji publicznej technik przekazu korzystających z geostacjonarnych i innych orbitujących wokół Ziemi satelitów doprowadziło do rozwoju wyspecjalizowanych usług satelitarnych dostarczanych przez prywatnie używane urządzenia, które są niezależne od sieci publicznych W ramach tych usług wykorzystuje się nieruchome lub przenośne terminale naziemne (które mogą być znane jako "małe stacje" lub "VSAT") na określonych pozycjach i jeden lub więcej satelitów. Pozycje mogą być określonymi stałymi punktami lub dowolnymi stałymi punktami w określonych obszarach, i są zwykle zlokalizowane blisko siedziby użytkownika lub jego miejsca pracy.

Poza wspieraniem dość powszechnych usług telekomunikacyjnych, inne zastosowania zawierają transmisje telewizyjne, komunikację z odległymi i wiejskimi obszarami, komunikację pomiędzy firmami (łącznie z transmisja danych i ich dystrybucja, faxami, poczta elektroniczna, tefekonferencjami i wideo konferencjami) oraz krótkotrwałe połączenia w sytuacjach zagrożenia. Takie wyspecjalizowane usługi

wzywanych do wypadków (policja, straż pożarna, karetka pogotowia i usługi szpitalne, itd.) gdzie pilny kontakt jest nieodzowny.

Usługi Telekonferencji i Wideo konferencji

Usługa telekonferencji zapewnia warunki konieczne dla konferencji w czasie rzeczywistym pomiędzy pojedynczymi osobami lub grupami osób znajdujących się w dwóch lub więcej miejscach, przy pomocy sieci telekomunikacyjnych. Usługa wideo konferencji jest typem usługi telekonferencji, w której mogą być wymieniane tak informacje głosowe jak i ruchomego obrazu z opcja obrazu nieruchomego, informacji informatyczno telekomunikacyjnych (np. fax) i sygnałów (np. identyfikacji mówiącego, prośba o zabranie głosu, itd.).

Usługi telefaxowe

Przekaz telefaxem (zwanym również faxem) jest procesem skanowania dokumentu, zamiany obrazu na sygnały elektroniczne dla celów transmisji do odległego odbiorcy i zamiany odebranych sygnałów w celu stworzenia kopii oryginalnie zeskanowanego obrazu. Telefax jest publiczna usługą faxów pomiędzy stacjami użytkowników oferowana dla celów transmisji dokumentów pomiędzy maszynami i może działać zarówno na sieciach komutowanych jak i sieciach przełączających pakiety(PSTN i ISDN).

Usługi głosowe

Usługi telefoniczne zapewniają możliwość elektronicznego przesyłania dźwięku lub mowy przy pomocy sieci. Systemy komunikacji głosowej przekazują słowa mówione w sposób analogowy, tj. odwzorowania danych w formie proporcjonalnych zmian sygnału elektrycznego, lub jako sygnał przetworzony cyfrowo dla transmisji w sieciach cyfrowych.

Usługa teletekstu

Usługa umożliwiająca korespondencję na zasadzie automatycznego przekazu z pamięci do pamięci w sieciach telekomunikacyjnych. Ma być uzupełnieniem i współdziałać z teleksem i usługami transmisji danych. Informacje są przekazywane w formacie strony aby mogły być albo wyświetlone na ekranie monitora albo użyte do tworzenia wydruku.

Usługi teleksowe

Usługi teleksowe dostarczają wolna komunikację tekstowa. Gdy używa się ich w trybie interaktywnym mogą zapewnić tę sama szybkość jak słowo mówione ale dodatkowo zapewniają również trwały zapis rozmowy. Dostępne funkcje to: przechowywanie i przesyłanie, adresowanie do wielu miejsc i wysyłka zgodnie z lista zaprogramowanych adresów do wszystkich bezpośrednio dostępnych odbiorców. Pomimo tego, że w chwili obecnej usługa ta jest wciąż osiągalna w Kanadzie i europejskich państwach NATO, nie świadczy się jej już w USA. Z upływem czasu, usługi telexowe będą prawdopodobnie zastąpione przez systemy komputerowego przekazu danych (patrz par. 54.(e)(ii) ale, tak długo jak pozostaje ona częścią ogólnie dostępnych usług przekazu wiadomości, powinno się wymagać, aby operatorzy sieci nadal dostarczali te usługi w stopniu na jaki pozwalają na to okoliczności.

Usługa poczty głosowej

Poczta głosowa jest telefonicznym odpowiednikiem poczty elektronicznej. Na systemy poczty głosowej składają się produkty sprzętowe i oprogramowanie, które mogą działać na większości prywatnych systemów telefonicznych i pozwalają użytkownikom wysyłać, otrzymywać i przekazywać wiadomości przy pomocy biurowych systemów telefonicznych i komputerowych.

Inne Środki Telekomunikacji

Transmisje (radiowe / telewizyjne)

Na usługi te składa się transmisja lądowa i satelitarna ze stacji nadawczych do bezpośredniego ogólnego odbioru, zwykle w formie dźwięku lub obrazów telewizyjnych. Usługi te pełnią ważną rolę w sytuacji kryzysu i wojny: mogą służyć między innymi do przekazywania alarmów ostrzegających przed atakiem, oraz do rozpowszechniania informacji i poleceń do społeczeństwa dla dobra ich bezpieczeństwa i morale.

Usługi łączności z ruchomymi odbiorcami (statki i samoloty)

Usługi dla statków i samolotów są świadczone przez stacje radiowe i stacje satelitarne aby zapewnić sprawne i oszczędne działanie transportu morskiego i lotniczego, dla wymiany korespondencji z załogami i pasażerami, i co najważniejsze, w nagłych wypadkach, dla zapewnienia bezpieczeństwa statków, samolotów i ich pasażerów oraz załogi. W warunkach rozległego zakłócenia pracy międzynarodowych publicznych sieci telekomunikacyjnych, stacje te mogą być pomocne przy przywracaniu komunikacji pomiędzy Krajami Członkowskimi Sojuszu.

Usługi teletekstu

Teletekst jest usługa nadawania tekstu i grafiki w standardowym sygnale telewizyjnym i wymaga specjalnego odbiornika. Informacje mogą być wyświetlane zamiast, lub być nałożone na normalny program.

Funkcje dostępne dzięki telekomunikacji

danych i sieć telexową. Może również być podstawa usług teletekstowych, telefaxowych i videotekstowych.

ISDN umożliwia elastyczne wykorzystanie szerokości pasma, wyższą jakość transmisji głosu, szybsze zestawianie połączenia, szybkość przekazu danych przekraczającą 56 Kbit/s i niższe koszty. Jest konieczne, aby użytkownik ustalił, że jego sprzęt jest kompatybilny z lokalnym przełącznikiem

Rodzaj informacji podlegającej transmisji

Sieci spełniają różne wymagania użytkowników. Różne tryby działania i określone usługi telekomunikacyjne są określone poniżej i są, używane w obrębie sieci w celu sprostania tym wymaganiom. Związek pomiędzy nimi jest zobrazowany w tabeli na stronach 25 - 27.

Głos

Głos jest przekazywaniem informacji przy pomocy mowy. Przykłady usług głosowych to telefon, poczta głosowa i telekonferencje.

Dane

Dane to transmisja informacji w formie binarnej, co pozwala na jej przechowywanie, przetwarzanie i przekazywanie przez maszyny. Do usług przekazywania danych zaliczają się telefax, przesyłanie komunikatów, obsługa komunikatów i telex.

Obraz

Informacje są przekazywane w formie obrazu. Typowymi przykładami tego typu usługi są telewizja cyfrowa i wideo konferencje.

Tryby Działania

Interaktywny

W telekomunikacji, mianem tym określa się przekaz głosu i obrazu w czasie rzeczywistym, zwykle gdy użytkownik mówi lub wprowadza dane i oczekuje nieomal natychmiastowej odpowiedzi z odległego punktu sieci zanim będzie kontynuował.

Przechowywanie i przekazywanie

Wiadomości są transmitowane i otrzymywane przez bezpośrednio sąsiadujące węzły routingu gdzie są zapisywane lub przechowywane a następnie retransmitowane do dalszych węzłów routingu lub do ostatecznego użytkownika.

Konkretne usługi

Usługi dzierżawienia łącza telekomunikacyjnego

Usługa dzierżawienia łącza telekomunikacyjnego to udostępnienie klientowi jednego lub więcej łączy do indywidualnego użytku. Łącza mogą być analogowe lub cyfrowe i być odpowiednie dla transmisji głosu, telegrafu, faxu lub danych. Międzynarodowe łącza dzierżawione spełniają, ogólnie przyjęte standardy i mogą korzystać albo z kabla, albo z połączenia satelitarnego. Prywatne łącza dzierżawione są wykorzystywane w dyplomacji i innych cywilnych organizacjach rządowych, przez władze wojskowe, organizacje związane z sektorem energii, finansów, nawigacji powietrznej i bezpieczeństwa, jak również maja również wiele innych zastosowań w sektorach przemysłowych i handlowych.

Usługi przesyłania komunikatów i obsługi poczty elektronicznej (MHS)

Usługi przesyłania komunikatów oferują komunikację typu użytkownik użytkownik pomiędzy indywidualnymi użytkownikami przy użyciu urządzeń zapamiętujących posiadających funkcje przechowywania i przesyłania, skrzynki pocztowej i/lub możliwości obsługi wiadomości (np. edycji, przetwarzania i zamiany informacji). Przykładem takich usług jest poczta elektroniczna. MHS może być opisany jako usługa wymiany komunkatów pomiędzy użytkownikami korzystając z usługi przechowywania i przesyłania w sieciach publicznych.

Usługi przesyłania danych mogą odbywać się na zasadzie zestawienia połączenia na czas sesji lub przełączania pakietów. Usługi takie są dostarczane przez sieć publiczna i są dostępne w szerokiej gamie szybkości przesyłania. Takie usługi mogą być używane nie tylko do przesyłania lub zarządzania danymi ale również do elektronicznego transferu pieniędzy i związanymi z tym usługami bankowymi, zdalnych alarmów i zarządzania urządzeniami

Publiczne usługi przesyłania *telegramów*

Usługi takie są oferowane użytkownikom przez operatorów publicznych sieci telekomunikacyjnych lub dostawców usług w celu transmisji telegramów oraz ich dostarczania do odbiorcy. Telegram (który to termin zawiera również radiotelegram) jest dokumentem pisanym, który ma być przekazany przy pomocy telegrafii, formy telekomunikacji w której przekazywane informacje po dojściu do adresata mają być nagrane jako stały dokument. Przesyłane informacje mogą być przedstawiane w innej formie albo mogą być przechowywane dla dalszego użytku.

Radiowy system *przywoławczy*

Usługa ta umożliwia użytkownikom, dzięki przenośnemu urządzeniu używanemu na danym obszarze, do otrzymywania komunikatu przez radio, po podaniu go z dowolnego telefonu w sieci publicznej. Do komunikatu może być dołączona ustna wiadomość lub zakodowany obraz wprowadzony przez dzwoniącego lub wygenerowany w sieci. Usługa ta ma specjalne zastosowanie w służbach publicznych

Electrical Industry Association (EIA), oraz Institute for Electrical and Electronic Engineers (IEEE). Główne organy rządowe związane z ustanawianiem standardów w telekomunikacji to National Institute; of Standards and Technology (NIST) oraz Federal Communications Commision (FCC).

- W Kanadzie, CRTC (Kanadyjska Komisja ds. Radia, T□' Telekomunikacji reguluje działania wszystkich dostawców powszechnych usług telekomunikacyjnych. Canadian Department of Communications jest odpowiedzialny za wydawanie licencji i zatwierdzanie wszelkich norm, telekomunikacyjnych.

62. Organy europejskie
    - W Europie, organy normatywne zostały połączone Wspólnie działają CEN (Europejski Komitet ds. Normalizacji), którego członkowie reprezentują kraje Wspólnoty Europejskiej i kraje EFTA, CENELEC (Europejski Komitet Norm Elektronicznych), również reprezentującego Wspólnotę Europejska i EFTA oraz ETSI (Instytutu Europejskich Standardów Telekomunikacyjnych)
    - Celem CEN i CENELEC w europejskiej normalizacji technologii informacji jest eliminacja różnic pomiędzy standardami krajowymi, a przez to eliminacja technicznych barier w handlu. ETSI jest aktywny w dziedzinie normalizacji w Europie. Uprawniona do przyłączenia się do ETSI jest każda organizacja wykazująca zainteresowanie normalizacja telekomunikacji europejskiej (administracje krajowe, operatorzy sieci publicznych, producenci, użytkownicy i dostawcy usług dla odbiorców prywatnych, instytucje badawcze, firmy konsultingowe).
63. Projekty technologii informacji są rozpatrywane osobno lub łącznie przez powyższe organy, w zależności od zakresu w jakim projekty te obejmują obszary, za które organy te są odpowiedzialne. W Europie za zarządzanie i przyznanie programu pracy jest odpowiedzialny ITSTC (Komitet Wykonawczy ds. Telekomunikacji Międzynarodowej, w którym każda z tych trzech organizacji posiada równa reprezentację.

Inne

64. Przedmioty gospodarcze posiadające znaczący udział na rynku mogą w rzeczywistości ustanawiać normy. Te, z kolei, mogą przybrać formę norm oficjalnych. Ponadto, istnieją organy dokonujące „wstępnych normalizacji", promujące normy w celu zapewnienia działań w zakresie rozwoju i wykorzystania norm. Przykładem takich organów są SPAG (Grupa Promocji i Wdrożenia Norm) oraz EMUG (European Manufacturing automation protocol Users' Group).
65. Organy ustalające normy krajowe mogą stworzyć własne normy ale, gdzie to będzie stosowne, będą koordynowały swoje działania z organami, o których mowa powyżej.

Standardy NATO dla urządzeń CIS i użytkowników cywilnych

66. Aby wypełnić swoje zadanie, NATO, obejmuje swoim zasięgiem rozległe obszary geograficzne, jest w ogromnej mierze zależne od zdolnych przetrwać, niezawodnych i zgodnych ze wszystkimi standardami wszystkich. urządzeń CIS. Przy planowaniu w wypadkach zagrożenia cywilnego, celach konsultacji i likwidowania kryzysu, jak również w celach wojskowych NATO w dużej mierze polega na infrastrukturze międzynarodowej telekomunikacji cywilnej. Sieci cywilne są w coraz większym stopniu oparte na powszechnych, światowych standardach i NATO zaakceptowało potrzebę posługiwania się nimi w największym możliwym stopniu zamiast tworzenia własnych standardów.
67. W przypadkach gdy istnieje rzeczywista potrzeba stworzenia przez NATO swoich własnych standardów, aby spełnić określone wymagania, niezbędna jest wczesna odpowiednia koordynacja takich standardów z właściwymi organami krajowymi, operatorami sieci i jednocześnie dostawcami usług lub innymi firmami telekomunikacyjnymi. MAS (Wojskowa Agencja Normatywna) jest odpowiedzialna za zagadnienia norm wojskowych oraz Standardowych Umów NATO, które mogły być stworzone przez grupę taka jak EUROCOM.
68. Obowiązkiem CCPC jest planowanie w zakresie utrzymania niezbędnych międzynarodowych usług telekomunikacyjnych. Organizacja ta korzysta z normalizacji, która, w zasadzie, przyczynia się do sprawnego łączenia międzynarodowych sieci publicznych i która zapewnia potrzebne narzędzie dla zarządzania siecią (np. jeśli chodzi o wdrożenie środków umożliwiających dostęp na preferencyjnych warunkach). Także połączenie pomiędzy ENs (Krajowymi Sieciami Awaryjnymi) opierają się na ogólnie używanych standardach.

Podsumowanie

69. Jeśli chodzi o urządzenia CIS, należy w maksymalnym stopniu korzystać ze standardów polecanych przez ITU i ISO oraz ograniczyć do minimum użytkowanie niestandardowych interfejsów. Należy szerzyć świadomość istnienia odpowiednich norm.
70. CCPC może i pragnie zapewnić pomoc.

VI. ĆWICZENIA

Wstęp

71. Głównym celem Ćwiczeń Zwalczania Kryzysu przez NATO w których uczestniczą kwatera główna NATO, narody, dowództwa wojskowe i cywilne organizacje ds. zagrożenia jest przetestowanie,

55. Funkcje (cywilne i wojskowe), oparte na telekomunikacji cywilnej i posiadające znaczenie dla opanowania kryzysu przez NATO.
    1. cele militarne
    2. ochrona społeczeństwa "obrona cywilna", np. publiczny system ostrzegania
    3. cele dyplomatyczne i inne istotne cele rządowe
    4. cele obrony kraju., w tym najistotniejsze cele rządowe
    5. usługi świadczone przez władze lokalne w nagłych wypadkach; w tym policje, straż pożarną, itd.
    6. odbudowa usług telekomunikacyjnych
    7. usługi komunalne takie jak energia, zaopatrzenie w wodę, itp.
    8. usługi medyczne (szpitale, karetki pogotowia, itp.)
    9. ratownictwo powietrzne i morskie
    10. gałęzie przemysłu wspierające wysiłek wojenny (broń, amunicja, elektronika, chemikalia, żywność, itd.)
    11. transport krajowy i międzynarodowy, taki jak:
        - lotniska i usługi lotnicze (w szczególności sieć Aeronautical Fixed Telcommunication Network - AFTN oraz sieć Societe Internationale des Telecommunications Aeronautique - SITA)
        - usługi drogowe
        - usługi portowe i marynarki wojennej
        - systemy kolei
        - wewnętrzne drogi wodne
    12. usługi meteorologiczne (w szczególności telekomunikacyjna sieć meteorologiczna)
    13. transmisje telewizyjne i radiowe oraz usługi prasowe (radio, telewizja, agencje prasowe, itp.)

V. STANARDY

Informacje ogólne

56. Postęp technologiczny pozwolił na stworzenie na przestrzeni ostatnich dekad systemów telekomunikacji i informacji oraz sieci, które mogą przetwarzać i przenosić bardzo duże ilości informacji, oraz posiadają coraz większa zdolność do komunikowania się na duże dystanse, z duża ilością użytkowników, na większa ilość sposobów, z większymi prędkościami i przy coraz większej niezawodności.
57. Ponieważ zaangażowanych jest wiele krajowych i międzynarodowych organizacji, jest konieczne aby zapewnić kompatybilność i uniwersalność ich sieci w celu zagwarantowania wydajnego korzystania z usług cywilnej telekomunikacji międzynarodowej: dlatego też standaryzacja jest kluczowym zagadnieniem w rozwoju telekomunikacji i technologii informacji.

Organizacje odpowiedzialne za przestrzeganie norm

58. Podczas gdy łączność posiada ustalone normy już od wielu lat, do 1985 r. proces normalizacji technologii informacji był przeprowadzany głównie w ramach organów ogólnie odpowiedzialnych za normy krajowe i międzynarodowe. Tradycyjny podział na organy odpowiedzialne za sprawy elektryczne i inne nie pasuje do technologii, która łączy w sobie więcej dziedzin. Ponadto, prędkość rozwoju technologii informacji oraz ogromna złożoność specyfikacji technicznych używanych w technologii informacji wymagają innych mechanizmów.

Organy międzynarodowe

59. Sektor Normalizacji (Standardisation Sector, wcześniej CCITT) Związku Telekomunikacji Międzynarodowej (1TU - International Telecommunication Union) jest odpowiedzialny za normalizację usług telekomunikacji publicznej. Zakres jego działań obejmuje tak tradycyjne usługi telegraficzne i telefoniczne, jak i najnowsze technologie. Nie obejmuje on swoim działaniem prywatnych lokalnych sieci i tylko w ograniczonym zakresie określa wymagania dotyczące sprzętu, który ma być podłączony do sieci publicznych. Ponadto, Sektor Radiokomunikacji (wcześniej CCIR) przeprowadza określony zakres podobnych działań związanych z wykorzystaniem radiokomunikacji.
60. ISO (Międzynarodowa Organizacja Normalizacji) określa obowiązujace na całym świecie normy dla każdego przedmiotu nie podlegającego specjalistycznej agencji; IEC (Międzynarodowy Komitet Elektrotechniczny) ustala światowe standardy dla obszaru elektrotechniki. Od 1987 obie organizacje współpracują ze sobą w Połączonym Komitecie Technicznym 1 (JTC 1), który jest głównym organem określającym standardy dotyczące technologii informacji. Jednakże, zastosowaniem technologii zajmuje się ISO. Członkowie JTC 1 są organizacjami określającymi normy krajowe.
61. Organy w USA i Kanadzie
    - Rząd Stanów Zjednoczonych tradycyjnie odgrywał minimalna rolę w ustanawianiu standardów dla przemysłu telekomunikacyjnego, pozwalając tej gałęzi przemysłu decydować o właściwych normach wszędzie gdzie to możliwe. Główne organizacje przemysłowe odpowiedzialne w Stanach Zjednoczonych za normalizację to między innymi: American National Standards Institute (ANSI),

- koordynacji i rozwoju do powszechnego formatu, zdarzeń zaprojektowanych i zaproponowanych przez twórców ćwiczeń, które mają wpływ na usługi międzynarodowe; zapewnić, że zostały stworzone zgodnie z trybem wydarzeń w komunikacji cywilnej;
- przygotowania i wydania Wytycznych dla każdego z ćwiczeń, które zgodnie z Kompendium CCPC i materiałami krajowymi, mogą przyczynić się do bardziej realistycznej symulacji;
- utrzymania ścisłych związków podczas etapu planowania ćwiczeń z ALLA i jej Grupowymi Ćwiczeniami Praktycznymi, oraz jeśli istnieje taka potrzeba, z innymi agencjami NATO; oraz
- ocenić rezultaty ćwiczeń i wnioski jakie one przyniosły w celu włączenia ich do Raportu dotyczącego pierwszych wrażeń i ostatecznej oceny ćwiczeń, który ma być przesłany do CCPC.

78. Biorąc pod uwagę fakt, że udział TOs w dowolnym z Ćwiczeń Zwalczania Kryzysu, nie ma na celu wyłącznie wsparcia SCEPC i organizacji ALLA/NALLA, ale może również pomóc w osiągnięciu ich własnych celów, jest pożądane aby te cele ćwiczeń TOs zostały z wyprzedzeniem przedstawione planującym ćwiczenia.
79. W planowaniu krajowych aspektów ćwiczenia, równolegle z działaniami EPT, ważne jest aby TOs nie dodawały tak wielu dodatkowych celów i zdarzeń, że uczestnicy symulacji nie będą w stanie dostatecznie się zaangażować w taka grę międzynarodową.

Planowanie zdarzeń

80. Na zdarzenia komunikacyjne składają się głównie sytuacje symulowane, mające wpływ na szeroką gamę usług TOs. Zdarzenia są oparte na uprzednio zaplanowanym rozwoju sytuacji, który powstaje ze scenariusza ćwiczenia i który ma zasadnicze znaczenie dla ramowych celów ćwiczenia. Wydarzenie może zwykle mieć wpływ na więcej niż jeden z Krajów. Zdarzenia komunikacyjne muszą być zaplanowane na tyle zgodnie z realiami na ile to możliwe i być dobrze udokumentowane.
81. Liczba i typy zdarzeń powinny zapewniać wystarczający zakres pozwalający grającym wyznaczyć innowacyjne rozwiania dla każdego ze zdarzeń. Dostępne powiriny być również w pełni zaplanowane i skoordynowane wydarzenia rezerwowe, które można wprowadzać gdy zachodzi taka potrzeba.
82. Zgodnie z ogólna dokumentacja NATO dotycząca ćwiczeń, gra typu „utrata łączności" może występować w trzech różnych wariantach:
    - Gra Rzeczywista - gra ćwiczebna, która zasadza się na kontrolowanym rzeczywistym przerwaniu łączności lub kontrolowanym rzeczywistym ogłoszeniu określonych komunikatów o stanie wojny;
    - Symulowana Gra Rzeczywista - gra ćwiczebna, która polega na kontrolowanej odmowie dostępu i użytkowania wybranych typów komunikacji biorącym udział w grze lub przez nich; oraz
    - Gra na Papierze - gra ćwiczebna, która jest przeprowadzana w odpowiedzi na wprowadzenie hipotetycznych wydarzeń l zdarzeń. Ten typ gry nie wpływa fizycznie na urządzenia lub przepływ komunikacji. Ogólnie, w ćwiczeniach, całość gry TO jest Gra na Papierze.

Instrukcje do Ćwiczeń

83. EPT powinna przygotować krótką instrukcję zwaną „Wytycznymi" zajmującą się sprawami specyficznymi dla każdego z ćwiczeń i zawierającą odwołania dla uczestników do odpowiednich fragmentów stałej dokumentacji. Wytyczne powinny zawierać:
    - nazwę, datę i trwanie ćwiczenia;
    - cele wybrane dla tego ćwiczenia;
    - zakres udziału TOs i ich punkty kontaktowe;
    - bezpieczne drogi komunikacyjne;
    - raporty z odbytych ćwiczeń, oraz
    - wszelkie aspekty ćwiczenia wymagające specjalnej uwagi uczestników lub Distaff.

Organizacja Ćwiczenia

84. Każdy z krajów biorących udział w ćwiczeniu NATO powinien opracować i zorganizować co najmniej jeden element ćwiczenia, który reprezentowałby jego krajowe Centrum Zwalczania Kryzysu. Jednakże, ze względu na strukturę organizacyjna niektórych TOs, może zaistnieć potrzeba stworzenia więcej niż jednego elementu ćwiczenia. Każdy z elementów ćwiczenia powinien składać się z grających i Distaff. Szczegóły uczestnictwa TO w każdym z ćwiczeń, będą przedstawione wg „Wytycznych" opisanych w paragrafie 83

Grający i Distaff

85. Grający zajmują się zdarzeniami, w miarę jak maja one miejsce. Będą oni łączyli swoje siły z siłami kolegów z innych Krajów by utrzymać świadczenie usług. Gdzie będzie to wymagane, będą działać zgodnie z instrukcjami otrzymanymi od NATO / Władz krajowych i ich Distaff.
86. W każdej z drużyn biorących udział w grze powinni znaleźć się odpowiedni specjaliści, którzy razem będą w stanie razem zająć się pełną gamą funkcji składających się na cele ćwiczenia. Jest zalecane, mając na uwadze sprawny przebieg kooperacji, aby grający byli w stanie co najmniej radzić sobie z takimi sprawami jak, polityka, wyjście z okresu kryzysu i wojny, oraz zagadnieniach technicznych, takich jak odbudowa połączeń i zarządzanie ruchem w sieci.

rozwinięcie i ocena przygotowania, gotowości, procedur i planów Sojuszu na wypadek konieczności sprostania sytuacjom stanu pogotowia, kryzysu i wojny. Muszą być przeprowadzane ćwiczenia NATO w tym zakresie aby zapewnić, że procedury zwalczania kryzysu istniejące w NATO mogą być sprawnie realizowane. Operatorzy telekomunikacji cywilnej mogą być wezwani do udziału w takich i innych ćwiczeniach NATO. Ponadto, dokonujący się rozwój komunikacji doprowadził do stworzenia gamy urządzeń telekomunikacyjnych, które NATO może zechcieć użyć i które, z tego powodu, powinny być testowane i wykorzystywane.

Cel

72. Głównym celem tej części opracowania jest przedstawienie wytycznych dotyczących celów, planowania, prowadzenia i oceny symulacji komunikacji cywilnej w likwidacji stanów kryzysowych przez NATO oraz inne ćwiczenia w oderwaniu od ich politycznego i wojskowego środowiska. Ta część zawiera również definicje ról uczestników ćwiczeń i personelu zarządzającego (DISTAFF), które, w połączeniu z wytycznymi podanymi dla każdego ćwiczenia i krajowymi materiałami instruktażowymi, pomogą uczestnikom w efektywniejszym udziale. Zasady podane w tej części mogą również być wykorzystywane przy planowaniu ćwiczeń Krajowej Telekomunikacji Cywilnej.

Zadania

73. Władze krajowe i operatorzy cywilni sieci telekomunikacyjnych uczestniczą w zwalczaniu stanów kryzysowych przez NATO oraz innych ćwiczeniach aby osiągnąć następujące cele:
    - utrzymać standard ich pomocy dla NATO w sytuacjach stanu pogotowia, kryzysu i wojny;
    - ćwiczenie procedur nie będących w codziennym użytku;
    - ćwiczenie opanowywania sytuacji, w których, w celu najlepszego wykorzystania sprzętu komunikacyjnego, wymagana jest koordynacja działań pomiędzy władzami cywilnymi, wojskowymi i sztabu NATO;
    - umożliwienie TOs przećwiczenia zarządzania siecią w sytuacjach stanu pogotowia, kryzysu i wojny, oraz
    - polepszyć związki pomiędzy TOs w celu poprawy ich zdolności do wspierania działań NATO.

Wytyczne

74. Celem stosownych władz krajowych oraz TOs w ćwiczeniach zwalczania kryzysu przez NATO jest ćwiczenie procedur i ustaleń, które stosuje się w sytuacji stanu pogotowia, kryzysu i wojny. Ze względu na ograniczenia czasowe i zasoby personelu dostępne w pojedynczym ćwiczeniu, nie jest możliwe przećwiczenie w pełnym zakresie wszystkich zadań wymienionych poniżej. dla każdego z ćwiczeń należy dokonać starannego doboru zadań i zakresu w jakim mają być wykonywane aby ostatecznie na przestrzeni lat osiągnąć je wszystkie.
75. Poprzez używanie stosownych bezpiecznych i nie zapewniających bezpieczeństwa systemów komunikacji i przekazywania informacji przećwiczyć:
    - procedury przejścia do stanu kryzysu i wojny zgodnie z odpowiednimi planami;
    - ustanowienie i sprawdzenie priorytetów w zmieniających się sytuacjach zgodnie z ustaleniami z właściwymi krajowymi władzami cywilnymi i wojskowymi;
    - zbieranie, porządkowanie i przekazywanie informacji dotyczących statusu stosownych infrastruktur telekomunikacji cywilnej;
    - środki zarządzania siecią w celu rekonfiguracji przepływu informacji w ramach publicznych sieci komutowanych gdy będą pod wpływem określonych wydarzeń lub systemów transmisji;
    - ustalenia dotyczących utrzymania istotnych usług telekomunikacji międzynarodowej zgodnie z wytycznymi władz krajowych po konsultacji, gdzie stosowne, z NATO;
    - procedury mające wspierać organizację ALLA/NALLA;
    - porozumienie się i konsultację z ekspertami w ramach TOs w celu uzyskania porady i pomocy co do wykorzystania telekomunikacji cywilnej dla potrzeb wsparcia NATO.

Planowanie ćwiczeń

76. Zespół Planowania Ćwiczeń, jest grupą ekspertów podlegających CCPC, którzy mogą być powoływani w celu planowania i koordynacji, na poziomie NATO, udziału krajowych władz Komunikacji Cywilnej i TOs we wszystkich ćwiczeniach NATO, w których władze krajowe zdecydują się brać udział.
    Grafik działań w każdym ćwiczeniu zależeć będzie od natury i czasu trwania ćwiczenia i będzie skoordynowany pomiędzy CCPC i właściwymi organami NATO.
    Zespół Planowania Ćwiczeń musi określić na wczesnym etapie procesu planowania, najbardziej właściwy okres w ramach czasowych ćwiczenia. Należy dążyć do tego aby wszystkie TOs brały udział w ćwiczeniach w tym samym okresie i na tym samym poziomie.
77. Zasadniczo, CCPC daje Zespołowi Planowania Ćwiczeń następujące zadania:
    - identyfikacji i przedstawienia CCPC celów dla każdego z ćwiczeń oraz wysiłku, który powinien być włożony w celu osiągnięcia ich przez TOs;
    - określenia i polecenia CCPC najwłaściwszego okresu i stopnia uczestnictwa w symulacji międzynarodowej komunikacji cywilnej;

Załącznik 3

PLANOWANIE DZIAŁAŃ NATO NA WYPADEK ZAGROŻEŃ CYWILNYCH
Bruksela kwiecień 1996 r.

Wstęp

1. Od momentu zakończenia II Wojny Światowej nasze państwa były w stanie osiągnąć wysoki standard życia i opieki społecznej. Doszliśmy do tego by przyjmować za rzecz naturalną takie sprawy jak elektryczność, bieżącą wodę, usuwanie śmieci i wszelkiego rodzaju żywność dostępną w lokalnych supermarketach.
2. Przyjmujemy również za rzecz naturalną, że jeśli zdarzy się jakiś wypadek, policja, straż pożar-na i pogotowie przybędą natychmiast by nas uratować.
3. Jednak od czasu do czasu, przypominamy sobie, że może zdarzyć się katastrofa. Mexico City, Seveso, Bhopal, Czernobyl i Armenia nie są już tylko nazwani geograficznymi. Przypominają one szokujące skutki katastrof spowodowanych przez człowieka lub naturę.
4. Sposób postępowania w celu ochrony naszych społeczeństw wystawionych na skutki zagrożeń (kryzysy, wojna, zagrożenia w czasach pokoju takie jak katastrofy) nazywane jest Planowaniem Działań na Wypadek Zagrożeń Cywilnych (Civil Emergency Planning). Niniejsza informacja na temat Programu Działań na wypadek Zagrożeń Cywilnych (CEP) skupia się na:
   - zmianach w podejściu do CEP od momentu utworzenia Sojuszu;
   - roli CEP w NATO;
   - Narzędziach Planowania dostępnych dla Sojuszu, i
   - Przygotowaniach do Zarządzania w stanie Kryzysu, które zostały opracowane przez wspólnotę cywilną NATO.

Trochę historii

5. Przed wyjaśnieniem roli NATO w Planowaniu Działań na Wypadek Zagrożeń Cywilnych (CEP), konieczne jest cofniecie się do roku 1948, kiedy to rozmowy na temat utworzenia NATO właśnie się rozpoczęły. W tym też roku, Minister Spraw Zagranicznych Norwegii napisał list do swego brytyjskiego kolegi sugerując ,że współpraca która istniała między państwami Sojuszu w odniesieniu do floty handlowej w czasie II Wojny Światowej winna być kontynuowana w ramach nowego NATO. Porozumienie zostało osiągnięte i już w 1950 roku, tylko rok od momentu utworzenia NATO, odbyło się pierwsze spotkanie Rady Planowania NATO ds. Żeglugi Oceanicznej. Od tej chwili, Planowanie Działań na Wypadek Zagrożeń Cywilnych stanowiło integralną część strategii NATO
6. W pierwszych latach historii NATO, pomimo tego spektakularnego startu, wydawało się jednak być za mało miejsca dla racjonalnego planowania gotowości cywilnej. W tamtym czasie, strategia NATO była definiowana przez takie terminy jak „Masowy odwet" lub „Zapewnioną wzajemną zagładę" (MAD). Mówiąc krótko, wierzono, że jakakolwiek konfrontacja musiała by zakończyć się masową wymianą ataków nuklearnych. Niemniej jednak, pomimo takiej "pewności zagłady", NATO odczuwało potrzebę zaplanowania wzajemnej pomocy między krajami członkowskimi NATO, lub to co z nich pozostałoby, w odbudowie zorganizowanego społeczeństwa po wojnie nuklearnej. W tym celu zostało utworzonych kilka komitetów, między innymi Komitet ds. Artykułów Przemysłowych oraz Komitet Planowania ds. Ropy Naftowej.
7. W roku 1962. Prezydent USA John F. Kennedy oraz jego Sekretarz Obrony McNamara zaczęli stawiać pytania odnośnie moralnej akceptacji strategii, która zasadniczo była oparta na zasadzie wzajemnego samobójstwa. Bez wątpienia kubański kryzys rakietowy dostarczył impulsu do poszukiwania strategii, która mogłaby zastąpić pełne zaufanie do broni nuklearnej. Była to jednak bardzo długa i żmudna batalia w NATO. Dopiero w grudniu 1967 roku Komitet Planowania Obronnego przyjmuje nową strategię znaną jako „Elastyczna odpowiedź". Francja nigdy nie podpisała się pod tą strategią, i to przyczyniło się do wycofania się Francji ze Zintegrowanych Struktur Militarnych NATO, a w konsekwencji do przeniesienia Kwatery NATO z Paryża do Brukseli. NATO przetrwało ten prawdopodobnie najpoważniejszy kryzys wewnętrzny w jego historü. Rada NATO - razem z Francją - w tym samym czasie poparła raport belgijskiego Ministra Spraw Zagraniczizych Pierre Harmel'a, stwierdzający miedzy innymi, że:

   „Sojusz atlantycki ma dwie *główne funkcje. Jego pierwszą funkcją jest utrzymanie odpowiedniej siły militarnej i politycznej solidarności by powstrzymać agresję i inne formy nacisku oraz obrona terytoriów krajów członkowskich jeśli agresja będzie miała miejsce"* oraz

   „W tym klimacie Sojusz może realizować swoją drugą funkcję, dążąc do *osiągnięcia postępu w osiągnięciu bardziej stabilnych związków,* w *których zasadnicze kwestie polityczne mogą być rozwiązywane. Bezpieczeństwo militarne oraz odprężenie polityczne nie* są *sprzeczne lecz się uzupełniają".*

87. W płynnym przeprowadzeniu ćwiczenia dopomoże poinformowanie w skrócie grających, przed rozpoczęciem ćwiczenia, o ich obowiązkach i funkcjach. Personel DISTAFF powinien również być wyznaczony i poinstruowany z odpowiednim wyprzedzeniem przed rozpoczęciem każdego z ćwiczeń. Muszą być oni dostępni w punktach ćwiczeń w odpowiedniej liczbie aby kierować gra w sposób pozwalający osiągnać maksymalny zysk z ćwiczenia.
88. DISTAFF są odpowiedzialni za kontrolowanie ćwiczenia i zapewnienie, że grający przestrzegają zasad ustalonych dla danego ćwiczenia. DISTAFF i grający powinni być osobnymi podmiotami. Do funkcji Distaffu należy:
    - wprowadzanie w życie zdarzeń;
    - koordynacja przebiegu gry wraz z distaffem innych uczestników;
    - dostarczanie grającym w miarę rozwoju ćwiczenia, jeśli to potrzebne; scenariusza / informacji o sytuacji;
    - symulowanie wkładu w rozwój wydarzeń od organizacji nie biorących udziału w ćwiczeniu, jeśli jest to potrzebne;
    - monitorowanie i kontrola działań grających;
    - zapewnienie, że akcje takie są realistyczne w istniejącej w tym czasie sytuacji, oraz
    - zapewnienie, że akcje grających i wszelkie potrzebne dane statystyczne są zachowane dla celów analizy po zakończeniu ćwiczenia.

Przebieg gry

89. Aby zapobiec nieporozumieniom, żadne zdarzenie nie powinno być zmieniane ani usuwane bez uprzedniego poinformowania o tym DISTAFFU. Wszelkie zmiany musza być skoordynowane pomiędzy wszystkimi DISTAFF z odpowiednim wyprzedzeniem przed czasem wprowadzenia zdarzenia.
90. Wszyscy grający i DISTAFF powinni mieć możliwość przedstawienia swoich uwag na temat ćwiczenia i płynącej z niego lekcji. Każdy TO przygotuje Raport dotyczący pierwszych wrażeń i ostatecznej oceny ćwiczeń, koncentrujący na aspektach krajowych dla potrzeb swoich własnych władz. Ponadto, każdy TO powinien przygotować raport dotyczący pierwszych wrażeń oraz koordynacji i dostarczyć go do CCPC. Terminy, do których takie raporty powinny być przedstawione będą zamieszczone w „Wytycznych".

Plan Działań Cywilnych na Wypadek Zagrożeń w Nowej Koncepcji Strategicznej

16. Jest to mniej więcej miejsce, gdzie Sojusz znajduje się w chwili obecnej. Po przyjęciu przez szefów państw NATO Nowej Koncepcji Strategicznej w 1991 roku, dokonano przeglądu podstawowych zasad Planu Działań na Wypadek Zagrożeń Cywilnych. Jesienią 1992 roku, Rada Północno - Atlantycka uzgodniła, że Plan Działań na Wypadek Zagrożeń Cywilnych skoncentruje się na następujących czterech głównych działaniach:
    - ochrona ludności;
    - ciągłość Rządów;
    - ochrona gospodarek krajowych; i
    - cywilne wsparcie dla wojska.

Ochrona ludności

17. Prawdopodobnie Obrona Cywilna jest najbardziej znanym obszarem programu działań na wypadek zagrożeń cywilnych. Instytucjonalnym zadaniem Obrony Cywilnej było zabezpieczenie ludzi przed bezpośrednimi skutkami wojny. Działania Obrony Cywilnej obejmują systemy wykrywania, ostrzegania i ochrony ludności oraz usługi ratownicze obejmujące karetki pogotowia ratunkowego i straż pożarną. Obecnie, w większości państw obrona cywilna również może być użyta w czasie pokoju dla wszystkich większych niebezpieczeństw, poczynając od pożarów, wypadków kolejowych i zanieczyszczeń chemicznych, do powodzi, huraganów, tornad i trzęsień ziemi.
18. Biorąc pod uwagę, że trwałe zagrożenie nuklearne zniknęło, wspólne zainteresowanie tym szczególnym aspektem gotowości cywilnej zostało zmniejszone[1] . Jednakże, rola NATO będzie kontynuowana by stanowić jedno z forów wymiany informacji i doświadczeń, szczególnie w odniesieniu do stanu gotowości przed katastrofą i analiz po katastrofie.

Ciągłość Rządów

19. Plan Działań na Wypadek Zagrożeń Cywilnych jest czymś więcej niż Obroną Cywilną. Jego drugim ważnym obszarem jest zapewnienie Ciągłości Rządów. aby umożliwić im dalsze funkcjonowanie i utrzymanie kontroli w sytuacjach zagrożenia. Ważność tego zadania wynika z faktu, że rządy ponoszą odpowiedzialność za działania mające na celu rozwiązywanie kryzysów, a kolektywne podejmowanie decyzji jest możliwe tylko wtedy, gdy wszystkie rządy są w stanie właściwie funkcjonować (Zarządzanie w stanie kryzysu). W tym kontekście, NATO-wski Komitet ds. Planowania Działań na Wypadek Zagrożeń Cywilnych działa jako forum wymiany informacji na temat planów poszczególnych państw.

Ochrona gospodarek krajów

20. Koncepcja nowej strategii Sojuszu stwierdza, że przerwanie przepływu zasobów życiowych może wpływać bezpośrednio na bezpieczeństwo Sojuszu. Zabezpieczenie dostępności zasobów życiowych nazywane jest Zarządzaniem Zasobami. Zarządzanie zasobami obejmuje określenie podstawowych gałęzi przemysłu i analizę ich potrzeb. Podstawowym zadaniem w tym względzie jest ocena zagrożeń bezpieczeństwa dla Sojuszu, które mogą powstać w wyniku potencjalnego przerwania przepływu zasobów życiowych oraz zajęcie się skutkami takiego przerwania, jeśli się pojawi.

Cywilne wsparcie dla wojska

21. Wsparcie cywilne dla wojska będzie, jak stwierdzono w Nowej Koncepcji Strategicznej i Nowej Koncepcji Wzmocnienia, szczególnie ważne dla osiągnięcia pożądanej elastyczności i mobilności sił Sojuszu. Transport i ruch sił oraz późniejsze wsparcie, byłyby realizowane w ramach odpowiedzialności poszczególnych państw podczas gdy odpowiednie wykorzystanie środków transportu cywilnego, byłoby zapewnione poprzez maksymalne wykorzystanie normalnego komercyjnego transportu. Jednakże, gdyby rynek komercyjny nie był w stanie sprostać tym wymaganiom, konieczne byłoby na czas kryzysu i wojny powołanie zastępczych władz państwowych ds. zagrożeń. Władze państwowe, w koordynacji z cywilnymi i wojskowymi władzami NATO muszą określić w jaki sposób najlepiej udostępnić, koordynować i wdrażać korzystanie z cywilnych i wojskowych środków transportu powietrznego, morskiego i lądowego.

Struktury Komitetu CEP

22. We wstępie Planu Działań na Wypadek Zagrożeń Cywilnych (CEP) były opisane środki podjęte przez *państwo* aby zabezpieczyć własne społeczeństwo w czasach zagrożeń (kryzysy, wojna oraz zagrożenia czasu pokoju, takie jak katastrofy). Chociaż CEP i zasoby cywilne pozostają pod kontrolą państw, uznano, że plany poszczególnych szesnastu państw będą bardziej skuteczne jeśli będą skoordynowane dla osiągnięciu wspólnego celu. Dlatego też, Rada Północno-Atlantycka, najwyższy organ decyzyjny NATO, utworzyła dziewięć Rad ds. Planowania Działań na Wypadek Zagrożeń Cywilnych oraz Komitetów, podlegających Naczelnemu Komitetowi ds. Planowania Działań na Wypadek Zagrożeń Cywilnych (SCEPC). Są one odpowiedzialne za skoordynowane planowanie w odniesieniu do:

---

[1] Ponieważ wiele działań odnoszących się do CEP i podejmowanych we współpracy z Krajami Partnerskimi dotyczy działań Obrony Cywilnej, działania NATO w dziedzinie Obrony Cywilnej ponownie wzrosły od roku 1994.

„Ostatecznym celem politycznym Sojuszu jest osiągnięcie sprawiedliwego i trwałego ładu pokojowego w Europie któremu towarzyszyłyby gwarancje bezpieczeństwa.".

Podczas gdy strategia militarna była streszczana słowami „Elastyczna Odpowiedź", to powyższa doktryna polityczna była zawarta w słowach „Zapobieganie i Odprężenie".

Podstawy Planowania Działań na Wypadek Zagrożeń Cywilnych

8. W połączeniu, Raport Harmel'a i strategia elastycznej odpowiedzi stworzyły całkowicie nowe podstawy dla Planowania Działań na Wypadek Zagrożeń Cywilnych. Obecnie zadaniem Sojuszu nie była już odbudowa po wojnie nuklearnej, ale pomoc społeczeństwu i wsparcie wysiłków obronnych podczas przewlekłej wojny konwencjonalnej. W tym czasie struktura komitetu przyjęła jego obecną formę. Jedynym wyjątkiem było utworzenie Wspólnego Komitetu Medycznego w 1992 roku. Rady Planowania i Komitety (PB&Cs) opracowały plany ustanowienia w NATO w okresie kryzysu tzw. Cywilnych Agencji na Czas Wojny. Wyznaczono główne kwatery, zapewniono utrzymanie łączności oraz wyznaczono i przeszkolono do pracy w NATO na czas wojny najlepszych ekspertów z biznesu, przemysłu i administracji rządowej. Stworzone struktury organizacyjne były testowane na corocznych sesjach i szkoleniach.

Szybkie Wzmocnienie

9. W 1978 roku nowe istotne zadanie przydzielono Programowi Działań w Przypadku Zagrożeń Cywilnych. W tym roku, na spotkaniu na szczycie w Waszyngtonie przyjęto Długoterminowy Program Obronny, obejmujący ideę Szybkiego Wzmocnienia, która wymagała przemieszczenia z USA i Kanady do Europy miliona żołnierzy oraz jedenastu milionów ton sprzętu w czasie 90 dni. Nie wchodząc dalej w szczegóły na temat Planu Szybkiego Wzmocnienia, można powiedzieć, że plan był największą pojedynczą operacją transportową kiedykolwiek rozważaną. Było oczywiste od początku, że przemieszczenie takie nie mogłoby być zrealizowane bez szerokiego użycia transportu cywilnego.
10. Prawie wszystkie PB&Cs były zaangażowane w planowanie. Rady Planowania ds. transportu dokonały wyboru odpowiedniej floty powietrznej i morskiej oraz opracowały szczegółowe plany skoordynowania dostaw towarów drogą morską i powietrzną oraz dostarczenia ich w wyznaczone miejsce. Komitety zaopatrzenia badały jak zapewnić wojskom paliwo, żywność i amunicję, podczas gdy Komitet Planowania ds. łączności cywilnej sprawdził wymagania łącznościowe by zapewnić odpowiednią koordynację. Komitet ds. Obrony Cywilnej był jedynym, którego plany pozostały całkowicie nie zmienione przez Plan Szybkiego Wzmocnienia.

Nowa era

11. Po upadku muru berlińskiego 9 listopada 1989 roku, wydarzenia potoczyły się bardzo szybko. W dniu 6 lipca 1990 roku, szefowie państw i rządów należących do NATO spotkali się w Londynie i wydali oświadczenie, które zaczynało się od stwierdzenia:

    „Europa weszła w nową obiecującą erę"

    i kończyło się następującymi słowami:

    „Dzisiaj nasz *Sojusz rozpoczyna poważną transformację. Współpracując ze wszystkimi krajami Europy, jesteśmy zdecydowani stworzyć trwały pokój na tym kontynencie.*".

Nowa koncepcja strategiczna Sojuszu

12. Na spotkaniu w Rzymie 7 listopada 1991 roku, szefowie państw i rządów NATO ogłosili nową koncepcję strategiczną Sojuszu, po raz pierwszy podaną publicznie, określającą siebie jako strategię „Dialogu, współpracy i utrzymania wspólnej zdolności obronnej".
13. Artykuł 6 nowej koncepcji strategicznej jest najbardziej fundamentalnym, stwierdza on, że *„Jednolite, masowe i potencjalnie natychmiastowe zagrożenie, które było główną troską Sojuszu w ciągu, jego pierwszych czterdziestu lat istnienia zniknęło."*

    Artykuły 8 i 9 dalej rozwijają to oświadczenie stwierdzając, że:

    "Groźba jednoczesnego zmasowanego ataku na wszystkich europejskich frontach NA TO została w sposób skuteczny oddalona i zatem nie będzie już *dłużej koncentrować na sobie strategii Sojusz*u". oraz

    „nadal istniejące zagrożenia dla bezpieczeństwa Sojuszu są wielorakie i wielokierunkowe, powodując trudności w *ich przewidywaniu i ocenie".*
14. Szczególnie interesujący dla strategów od Zagrożeń Cywilnych jest artykuł 13, stwierdzający: *„Wpływ na interesy bezpieczeństwa Sojuszu mogą wywierać inne zagrożenia, szerszej natury, włączając w to rozprzestrzenianie broni masowego rażenia, zakłócenia przepływu zasobów życiowych oraz* działania *terrorystyczne i sabotażowe"*
15. Strategia ta miała bezpośrednie znaczenie dla Planowania Działań na Wypadek Zagrożeń Cywilnych oraz przypisywała coraz większe znaczenie Zarządzaniu w Stanie Kryzysu i formułowała wskazówki dla sił Sojuszu, stwierdzając, że siły te będą wymagały *„zwiększenia elastyczności i mobilności oraz zapewnienia możliwości powiększenia kiedy zajdzie konieczność"* oraz, że *„Zasoby cywilne w tym kontekście będą coraz istotniejsze"*

- Komitet ds. Stanów Alarmowych, koordynujący sprawy związane z NATO-wskim Systemem Zapobiegania; oraz
- Naczelny Komitet Cywilnego Planowania na Wypadek Zagrożeń, doradzający Radzie w sposób skoordynowanv odnośnie wszystkich spraw dotyczących zasobów cywilnych i ludności.

Konsultacje z innymi komitetami, jak na przykład z Komitetem Koordynującym Weryfikacje, mogą mieć miejsce gdy zajdzie taka potrzeba.

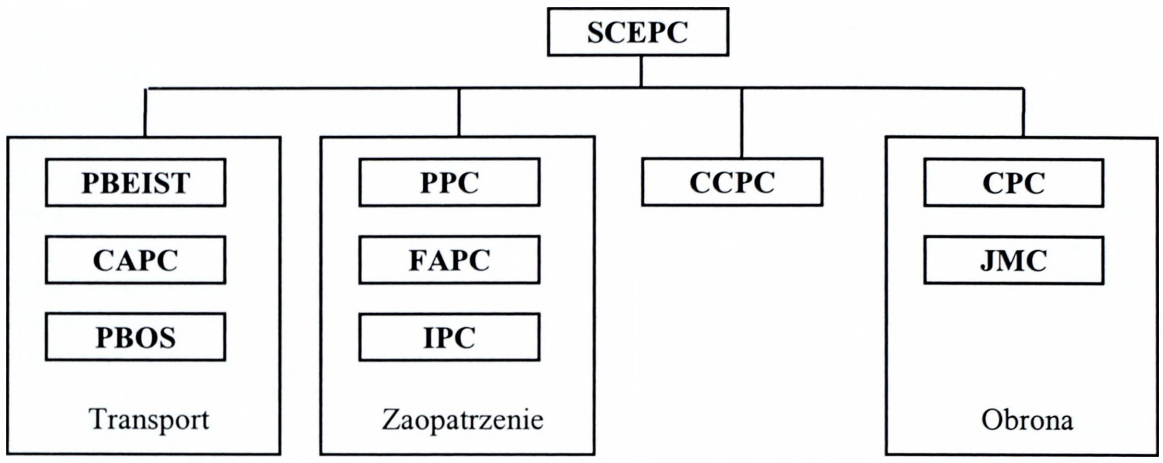
30. Zapobieganie kryzysom oraz przygotowania do zarządzania w stanie kryzysu w ramach NATO mają za zadanie dostarczać decydentom NATO możliwie najpełniejszych informacji koniecznych do podjęcia decyzji oraz możliwie najszerszego wyboru opcji reakcji na kryzys. Osoby zajmujące się planowaniem działań na Wypadek Zagrożeń Cywilnych dostarczałyby informacji i możliwych opcji dotyczących zasobów cywilnych dla jednostki zajmującej się Przygotowaniami do Zarządzania w Stanie Kryzysu.
31. We wczesnych stadiach kryzysu, SCEPC będzie się konsultował z Przewodniczącymi PB&Cs lub innymi wysokiego szczebla ekspertami z biznesu / przemysłu oraz rządu / administracji w sprawie pojawiających się problemów i interpretacji sytuacji z punktu widzenia Sojuszu.
32. W usprawiedliwionych sytuacjach, SCEPC powoływałoby w Kwaterze Głównej NATO komórkę Kryzysową ds. Zagrożeń Cywilnych, kierowaną przez Dyrektora Planowania Działań na Wypadek Zagrożeń, w celu monitorowania sytuacji i wsparcia komitetu w jego zadaniach dotyczących zarządzania w stanie kryzysu. Na początku personel CECC składałby się z członków Personelu Międzynarodowego (IS), Wojskowego Personelu Międzynarodowego, oraz członków PB&Cs. W usprawiedliwionych sytuacjach, CECC byłby powiększony o ekspertów z biznesu /przemysłu oraz rządu / administracji.
33. W sytuacji dużego kryzysu, SCEPC może zdecydować o potrzebie wzrostu liczby wezwanych ekspertów i zorganizowania ich w wyspecjalizowanych sekcjach. Struktura i skład tych sekcji nie może być określony z góry, ale będzie zależał od wymagań sytuacji, np. wyspecjalizowanie się na jednym polu działalności lub pokierowanie określoną kwestią obejmującą kilka pól działalności. Całkowita wielkość, struktura i skład takiej sekcji będzie zależał od szczegółowych wymogów stanu kryzysu.
34. Podsumowując, przygotowania do zarządzania w stanie kryzysu dotyczącego Zagrożeń składają się z następujących opcji:
    - konsultacja z i / lub wezwanie wysokiej klasy ekspertów;
    - konsultacja z i / lub wezwanie Przewodniczącego i / lub Rad Planowania i Komitetów;
    - utworzenie przez SCEPC, Komórki Kryzysowej ds. Zagrożeń (CECC), wzmocnionej w razie potrzeby przez ekspertów oraz
    - możliwość poszerzenia komórki zarządzania w stanie kryzysu, o wyspecjalizowane sekcje.
35. Wszystkie Rady Planowania i Komitety mają określone obszary doradztwa w czasach kryzysu, a kraje członkowskie Sojuszu wyznaczyły potencjalnych doradców dla NATO.

Komórka Kryzysowa ds. Zagrożeń Cywilnych

36. Zadania CECC, niezależnie od jej potencjalnej wielkości i składu, obejmowałyby między innymi:
    - Monitorowanie i ocena sytuacji jako podstawy polityki decyzyjnej wyższych władz NATO;
    - Doradzanie i pomoc Radzie / DPC, SCEPC, Głównym Dowódcom NATO, innym właściwym organom oraz krajom członkowskim w jaki sposób najlepiej wykorzystać w danej sytuacji istniejące zasoby cywilne;
    - Utrzymanie łączności z delegacjami krajowymi w Kwaterze NATO oraz z SHAPE i gdy zażąda tego SCEPC, ustanowienie łączności z organizacjami międzynarodowymi w zależności od potrzeb;
    - Doradztwo odnośnie sposobów pokonywania problemów wynikających z legislacyjnych i innych różnic występujących w poszczególnych krajach, na rzecz koordynacji zasobami i współdziałania;
    - Przeprowadzenie, na życzenie, odpowiednich studiów wykonalności na rzecz działań krajowych i NATO;
    - Przygotowanie tematów do dyskusji i konsultacji w SCEPC (np. poszerzenie CECC, żądanie podjęcia Środków Zapobiegawczych);
    - Podjęcie właściwych działań przez personel w następstwie decyzji podjętych w Radzie / DPC lub w SCEPC;
    - Na podstawie Raportów o Aktualnej Sytuacji pochodzących z państw przedstawiających ocenę sytuacji cywilnej, przyczynianie się do opracowania pełnej oceny polityczno - militarnej oraz wkład w odprawy nt. aktualnej sytuacji, odbywające się w Radzie / DPC, Komitecie Wojskowym i SCEPC;
    - Zapewnienie, na życzenie państw, uzgodnionego wsparcia oraz międzynarodowej koordynacji.
37. W związku z potrzebą elastyczności, wielkość, struktura i skład CECC nie mogą być z góry ustalone Jednakże, w CECC będzie zawsze istnieć potrzeba ogólnej koordynacji i administracyjnego wsparcia działań, które będą realizowane w Sekcji Koordynacyjnej. Wszystkie inne wyspecjalizowane sekcje mające powstać w stanie kryzysu w CECC będą utworzone zgodnie z potrzebami ocenionymi przez SCEPC. W zasadzie, będą one zorganizowane w zależności od zadań, które mają być zrealizowane.

- Europejskiego Transportu Śródlądowego Naziemnego (PBEIST);
- Transportu Oceanicznego (PBOS);
- Lotnictwa Cywilnego (PPC);
- Planowania w Sektorze Naftowym (PPC);
- Żywności i Rolnictwa (FAPC) Gotowości Przemysłu (IPC);
- Telekomunikacji Cywilnej (CCPC) Obrony Cywilnej (CPC) oraz
- Planowania Medycznego (JMC).

23. PB&Cs spotykają się raz lub dwa razy w roku na Sesjach Plenarnych a częściej w grupach roboczych lub specjalnych podkomitetach. Członkami są eksperci z odpowiednich ministerstw państw członkowskich.



Rys. 1. Struktura Komitetu CEP

Zadanie koordynacyjne Naczelnego Komitetu Planowania Działań na Wypadek Zagrożeń Cywilnych

24. Całkowita koordynacja między różnymi obszarami planowania jest prowadzona przez Naczelny Komitet Planowania Działań na Wypadek Zagrożeń(SCEPC). SCEPC, który informuje bezpośrednio Radę, spotyka się na Stałych Sesjach każdego miesiąca i składa się z członków delegacji poszczególnych krajów członkowskich w NATO. Stałym Sesjom przewodniczy Dyrektor Planowania Działań Cywilnych na Wypadek Zagrożeń, wspierany przez personel Dyrekcji Cywilnego Planowania Działań na Wypadek Zagrożeń.
26. Dwa razy w roku odbywają się Posiedzenia Plenarne SCEPC. Przy takich okazjach przedstawicielami państw są zazwyczaj szefowie krajowych ministerstw lub agencji, odpowiadających za koordynację planowanych działań na wypadek zagrożeń cywilnych.
27. Sesjom Plenarnym przewodniczy Sekretarz Generalny lub w jego imieniu Asystent Sekretarza Generalnego ds. Infrastruktury, Logistyki i Cywilnego Planowania Działań na Wypadek Zagrożeń.

Planowanie Działań Cywilnych na Wypadek Zagrożeń i Cykl Przeglądów

27. Aby osiągnąć bardziej strukturalne podejście do planowania na wypadek zagrożeń, Rada Północno-Atlantycka zainicjowała Cywilne Planowanie na Wypadek Zagrożeń i Cykl Przeglądów, które obejmują okres czterech lat.
28. Zgodnie z procedurami obowiązującymi w Planowaniu Działań Cywilnych na Wypadek Zagrożeń i Cyklem Przeglądów, ministrowie spraw zagranicznych NATO dostarczają wskazówek dla poszczególnych okresów planowania. Te wskazówki określają cele nie tylko dla działań na wypadek zagrożeń cywilnych na poziomie NATO, ale także dla planowania na poziomie poszczególnych państw. SCEPC tworzy indywidualne programy robocze oparte na tych Zaleceniach Ministerialnych dla każdego PB&Cs. One z kolei opracowują raporty odnośnie osiągniętych postępów. Jako następny ważny krok w Cyklu Przeglądów, SCEPC wydaje Kwestionariusz dot. Planowania Działań Iza Wypadek Zagrożeń, w którym poszczególne państwa określają swoje postępy oraz stan cywilnej gotowości. Odpowiedzi państw na kwestionariusz są przesyłane do Kwatery NATO i one, razem z raportami PB&Cs dotyczącymi postępów, tworzą podstawy dla Raportu na temat Stanu Gotowości Cywilnej. Raport ten jest potem przedkładany Radzie na Sesji Ministerialnej do rozpatrzenia razem z zaproponowanymi nowymi Ministerialnymi Zaleceniami dla CEP w następnym okresie planowania.

Przygotowania do Zarządzania w Stanie Kryzysu

29. W czasach kryzysu będzie wzrastać potrzeba podjęcia przez państwa skoordynowanych działań. W sytuacjach kryzysu i napięć, NATO wykorzysta swoje Przygotowania do Zarządzania w Stanie Kryzysu. Cywilna struktura NATO w czasach pokoju z jej różnymi komitetami wspierającymi Radę byłaby ograniczona w stanach kryzysu do tylko czterech Komitetów. Tymi komitetami są:
    - Komitet Wojskowy, doradzający Radzie w sposób skoordynowany w sprawach wojskowych;
    - Komitet Polityczny, doradzający Radzie w sposób skoordynowany w sprawach politycznych;

Art. 8.

1. Prezydent Rzeczypospolitej Polskiej, na wniosek Rady Ministrów, w drodze rozporządzenia, znosi stan wojenny, jeżeli ustaną przyczyny, dla których stan wojenny został wprowadzony, oraz zostanie przywrócone normalne funkcjonowanie państwa.

Przepisy art. 4 ust. 1 i 3 stosuje się odpowiednio do rozporządzenia, o którym mowa w ust. 1.

Rozdział 2
ZASADY DZIAŁANIA ORGANÓW WŁADZY PUBLICZNEJ

Art. 9.

W czasie stanu wojennego organy władzy publicznej działają w dotychczasowych strukturach organizacyjnych państwa i w ramach przysługujących im kompetencji, z zastrzeżeniem przepisów niniejszej ustawy.

Art. 10.

1. Jeżeli w czasie stanu wojennego wystąpi konieczność obrony państwa, obroną tą kieruje Prezydent Rzeczypospolitej Polskiej we współdziałaniu z Radą Ministrów.
2. Prezydent Rzeczypospolitej Polskiej w czasie stanu wojennego w szczególności:
   1) postanawia, na wniosek Rady Ministrów, o przejściu organów władzy publicznej na określone stanowiska kierowania;
   2) postanawia, na wniosek Rady Ministrów, o stanach gotowości bojowej sił zbrojnych Rzeczypospolitej Polskiej, zwanych dalej "Siłami Zbrojnymi";
   3) określa, na wniosek Rady Ministrów, zadania sił zbrojnych w czasie stanu wojennego;
   4) może mianować, na wniosek Prezesa Rady Ministrów, Naczelnego Dowódcę sił zbrojnych;
   5) zatwierdza, na wniosek Naczelnego Dowódcy sił zbrojnych, plany operacyjnego użycia sił zbrojnych;
   6) uznaje, na wniosek Naczelnego Dowódcy sił zbrojnych, określone obszary Rzeczypospolitej Polskiej za strefy bezpośrednich działań wojennych.

Art. 11.

1. Rada Ministrów w czasie stanu wojennego w szczególności:
   1) zarządza uruchomienie systemu kierowania obroną państwa;
   2) zarządza przejście na wojenne, określone w odrębnych przepisach, zasady działania organów władzy publicznej;
   3) określa, na wniosek Naczelnego Dowódcy sił zbrojnych, zasady działania organów władzy publicznej w strefie bezpośrednich działań wojennych;
   4) może zawiesić funkcjonowanie organów władzy publicznej w strefie bezpośrednich działań wojennych;
   5) może przekazać organom wojskowym określone kompetencje organów władzy publicznej w strefie bezpośrednich działań wojennych.
2. Jeżeli w czasie stanu wojennego Rada Ministrów nie może zebrać się na posiedzenie, konstytucyjne kompetencje Rady Ministrów wykonuje Prezes Rady Ministrów.

Art. 12.

Minister Obrony Narodowej w czasie stanu wojennego w szczególności:
   1) dokonuje oceny zagrożeń wojennych i możliwości obronnych oraz formułuje i przedstawia właściwym organom propozycje dotyczące obrony państwa;
   2) koordynuje realizację zadań organów administracji rządowej i jednostek samorządu terytorialnego wynikających z zadań dotyczących obrony państwa;
   3) przedstawia właściwym organom potrzeby w zakresie świadczeń organów państwowych i jednostek samorządu terytorialnego, przedsiębiorców i innych jednostek organizacyjnych oraz osób fizycznych, na rzecz sił zbrojnych i obrony państwa;
   4) sprawuje ogólny nadzór nad realizacją zadań obronnych wykonywanych przez organy administracji rządowej i jednostki samorządu terytorialnego;
   5) organizuje mobilizacyjne rozwinięcie, uzupełnianie i wyposażanie sił zbrojnych;
   6) współdziała z ministrem właściwym do spraw wewnętrznych w zakresie świadczeń, o których mowa w pkt 3;
   7) koordynuje realizację zadań państwa-gospodarza wynikających z umów międzynarodowych.

Art. 13.

1. W czasie stanu wojennego wojewoda kieruje realizacją zadań obronnych i obroną cywilną na terenie województwa.
2. Wojewoda w czasie stanu wojennego w szczególności:
   1) ocenia zagrożenia;
   2) wprowadza, w zakresie nienależącym do właściwości innych organów, ograniczenia wolności i praw człowieka i obywatela oraz łagodzi i uchyla te ograniczenia;

Załącznik nr 4

USTAWA
z dnia 29 sierpnia 2002 r.
O STANIE WOJENNYM ORAZ O KOMPETENCJACH NACZELNEGO DOWÓDCY SIŁ ZBROJNYCH I ZASADACH JEGO PODLEGŁOŚCI KONSTYTUCYJNYM ORGANOM RZECZYPOSPOLITEJ POLSKIEJ.
(Dz. U. z dnia 25 września 2002 r.)

Rozdział 1
PRZEPISY OGÓLNE

Art. 1.

Ustawa określa tryb wprowadzenia i zniesienia stanu wojennego, zasady działania organów władzy publicznej oraz zakres ograniczeń wolności i praw człowieka i obywatela w czasie stanu wojennego, a także kompetencje Naczelnego Dowódcy sił zbrojnych i zasady jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej.

Art. 2.

1. W razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami terrorystycznymi, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, Prezydent Rzeczypospolitej Polskiej może, na wniosek Rady Ministrów, wprowadzić stan wojenny na części albo na całym terytorium państwa.
2. We wniosku, o którym mowa w ust. 1, Rada Ministrów określa przyczyny i obszar, na którym ma być wprowadzony stan wojenny, a także odpowiednie do stopnia i charakteru zagrożenia, w zakresie dopuszczonym niniejszą ustawą, rodzaje ograniczeń wolności i praw człowieka i obywatela.

Art. 3.

1. Prezydent Rzeczypospolitej Polskiej niezwłocznie rozpatruje wniosek, o którym mowa w art. 2 ust. 1, a następnie wydaje rozporządzenie o wprowadzeniu stanu wojennego albo postanawia odmówić wydania takiego rozporządzenia. Rozporządzenie o wprowadzeniu stanu wojennego Prezydent Rzeczypospolitej Polskiej przedstawia Sejmowi w ciągu 48 godzin od jego podpisania.
2. W rozporządzeniu, o którym mowa w ust. 1, określa się przyczyny wprowadzenia oraz obszar, na którym wprowadza się stan wojenny, a także - w zakresie dopuszczonym niniejszą ustawą - rodzaje ograniczeń wolności i praw człowieka i obywatela.

Art. 4.

1. Stan wojenny obowiązuje od dnia ogłoszenia rozporządzenia, o którym mowa w art. 3 ust. 1, w Dzienniku Ustaw Rzeczypospolitej Polskiej.
2. W przypadku uchylenia rozporządzenia, o którym mowa w art. 3 ust. 1, przez Sejm Rzeczypospolitej Polskiej uchwałę Sejmu w tej sprawie niezwłocznie ogłasza się w Dzienniku Ustaw Rzeczypospolitej Polskiej.
3. Rozporządzenie Prezydenta Rzeczypospolitej Polskiej o wprowadzeniu stanu wojennego oraz inne akty prawne dotyczące tego stanu podaje się do publicznej wiadomości, w drodze obwieszczenia właściwego wojewody, przez rozplakatowanie w miejscach publicznych, a także w sposób zwyczajowo przyjęty na danym obszarze.

Art. 5.

Redaktorzy naczelni dzienników oraz nadawcy programów radiowych i telewizyjnych są obowiązani do niezwłocznego, nieodpłatnego podania do publicznej wiadomości rozporządzenia Prezydenta Rzeczypospolitej Polskiej o wprowadzeniu stanu wojennego i innych aktów prawnych dotyczących tego stanu przekazanych im przez wojewodę właściwego ze względu na siedzibę redakcji lub nadawcy.

Art. 6.

Minister właściwy do spraw zagranicznych notyfikuje Sekretarzowi Generalnemu Organizacji Narodów Zjednoczonych i Sekretarzowi Generalnemu Rady Europy wprowadzenie i przyczyny wprowadzenia stanu wojennego, a także jego zniesienie.

Art. 7.

1. Wprowadzenie stanu wojennego wywołuje skutki określone w niniejszej ustawie i w innych przepisach dotyczących stanu wojennego w stosunku do organów władzy publicznej, obywateli polskich zamieszkałych lub czasowo przebywających na obszarze, na którym został wprowadzony stan wojenny, osób prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej mających siedzibę lub prowadzących działalność gospodarczą na obszarze objętym stanem wojennym.
2. W przypadku gdy niniejsza ustawa, a także inne ustawy albo ratyfikowane umowy międzynarodowe nie stanowią inaczej oraz nie zabrania tego powszechnie uznany zwyczaj międzynarodowy, przepis ust. 1 stosuje się również do cudzoziemców przebywających na obszarze, na którym został wprowadzony stan wojenny, oraz do ich mienia, jak również mienia innych państw.

Art.19.

W czasie stanu wojennego można zawiesić prawo do:

1) strajków pracowniczych i innych form protestu w odniesieniu do określonych kategorii pracowników lub w określonych dziedzinach;
2) strajków i innych niż strajki form akcji protestacyjnych rolników;
3) akcji protestacyjnych studentów organizowanych przez studenckie samorządy, stowarzyszenia lub organizacje.

Art. 20.

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

Art. 21.

1. W czasie stanu wojennego może być wprowadzona:
   1) cenzura prewencyjna środków społecznego przekazu obejmująca materiały prasowe w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe (Dz. U. Nr 5, poz. 24, z 1988 r. Nr 41, poz. 324, z 1989 r. Nr 34, poz. 187, z 1990 r. Nr 29, poz. 173, z 1991 r. Nr 100, poz. 442, z 1996 r. Nr 114, poz. 542, z 1997 r. Nr 88, poz. 554 i Nr 121, poz. 770, z 1999 r. Nr 90, poz. 999, z 2001 r. Nr 112, poz. 1198 oraz z 2002 r. Nr 153, poz. 1271), z zastrzeżeniem ust. 7;
   2) kontrola zawartości przesyłek, listów, paczek i przekazów przekazywanych w ramach usług pocztowych o charakterze powszechnym lub usług kurierskich;
   3) kontrola treści korespondencji telekomunikacyjnej i rozmów telefonicznych lub sygnałów przesyłanych w sieciach telekomunikacyjnych;
   4) emisja sygnałów uniemożliwiających nadawanie lub odbiór przekazów radiowych, telewizyjnych lub dokonywanych poprzez urządzenia i sieci telekomunikacyjne, których treść może zwiększyć zagrożenie bezpieczeństwa lub obronności państwa.
2. Funkcję organów cenzury i kontroli pełnią właściwi wojewodowie, którzy mogą nakazać organom administracji publicznej działającym na obszarze województwa wykonywanie czynności technicznych niezbędnych do prowadzenia cenzury lub kontroli.
3. Organy cenzury i kontroli są uprawnione do zatrzymywania w całości lub w części publikacji, przesyłek pocztowych i kurierskich oraz korespondencji telekomunikacyjnej, a także do przerywania rozmów telefonicznych i transmisji sygnałów przesyłanych w sieciach telekomunikacyjnych, jeżeli ich zawartość lub treść może zwiększyć zagrożenie bezpieczeństwa lub obronności państwa.
4. Zatrzymane publikacje, przesyłki lub korespondencję telekomunikacyjną doręcza się adresatom po zniesieniu stanu wojennego, z zastrzeżeniem ust. 5.
5. Zatrzymane publikacje, przesyłki pocztowe i kurierskie oraz korespondencję telekomunikacyjną, których treść lub zawartość pochodzi z przestępstwa, była przeznaczona do popełnienia przestępstwa albo została objęta zakazem posiadania, organ cenzury i kontroli przekazuje niezwłocznie, a najpóźniej bezpośrednio po zniesieniu stanu wojennego, organom właściwym do prowadzenia postępowania karnego lub orzeczenia przepadku rzeczy.
6. Decyzje organów cenzury i kontroli są ostateczne i mogą być zaskarżone bezpośrednio do Naczelnego Sądu Administracyjnego. Nie stosuje się przepisu art. 34 ust. 3 ustawy z dnia 11 maja 1995 r. o Naczelnym Sądzie Administracyjnym (Dz. U. Nr 74, poz. 368 i Nr 104, poz. 515, z 1997 r. Nr 75, poz. 471, Nr 106, poz. 679, Nr 114, poz. 739 i Nr 144, poz. 971, z 1998 r. Nr 162, poz. 1126, z 1999 r. Nr 75, poz. 853, z 2000 r. Nr 2, poz. 5, Nr 48, poz. 552, Nr 60, poz. 704 i Nr 91, poz. 1008, z 2001 r. Nr 49, poz. 508 i 509, Nr 98, poz. 1070 i Nr 101, poz. 1113 oraz z 2002 r. Nr 113, poz. 984 i Nr 141, poz. 1177).
7. Cenzura prewencyjna nie obejmuje należących do kościołów i innych związków wyznaniowych środków społecznego przekazu stanowiących źródła informacji na temat religii i służących wypełnianiu funkcji religijnych.
8. Rada Ministrów, w drodze rozporządzenia, określi:
   1) tryb postępowania organów cenzury i kontroli, uwzględniając potrzebę zapewnienia sprawności i szybkości działania;
   2) organy właściwe w sprawach, o których mowa w ust. 1 pkt 4, oraz tryb postępowania tych organów, uwzględniając potrzebę zapewnienia niejawności stosowanych metod i technik działania.

3) występuje z wnioskami do właściwych organów o wprowadzenie ograniczeń wolności i praw człowieka i obywatela, jak również o ich złagodzenie lub uchylenie;
4) określa zadania wynikające z przepisów stanu wojennego;
5) koordynuje i kontroluje działalność organów władzy publicznej, przedsiębiorców oraz innych jednostek organizacyjnych działających na obszarze województwa;
6) może nakładać zadania i nakazywać jednostkom samorządu terytorialnego dokonywanie określonych wydatków, na zasadach określonych w odrębnych przepisach.

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

Art. 14.

1. Jeżeli organy gminy, powiatu lub samorządu województwa nie wykazują dostatecznej skuteczności w wykonywaniu zadań publicznych lub w realizacji działań wynikających z przepisów o wprowadzeniu stanu wojennego, Prezes Rady Ministrów, na wniosek właściwego wojewody, może zawiesić te organy do czasu zniesienia stanu wojennego lub na czas określony i ustanowić w ich miejsce zarząd komisaryczny sprawowany przez komisarza rządowego.
2. Komisarza rządowego powołuje i odwołuje Prezes Rady Ministrów na wniosek wojewody.
3. Komisarz rządowy z dniem powołania przejmuje wykonywanie zadań i kompetencji zawieszonych organów gminy, powiatu lub samorządu województwa.
4. Stan zawieszenia organów gminy, powiatu lub samorządu województwa ustaje z upływem czasu określonego przez Prezesa Rady Ministrów oraz z mocy prawa z dniem zniesienia stanu wojennego.

Art. 15.

Decyzje wydane przez organy władzy publicznej na podstawie niniejszej ustawy lub przepisów wykonawczych podlegają natychmiastowemu wykonaniu. Przepisy o postępowaniu egzekucyjnym w administracji stosuje się odpowiednio.

Rozdział 3
NACZELNY DOWÓDCA SIŁ ZBROJNYCH

Art. 16.

1. Naczelny Dowódca sił zbrojnych podlega Prezydentowi Rzeczypospolitej Polskiej.
2. Naczelny Dowódca sił zbrojnych dowodzi siłami Zbrojnymi oraz innymi podporządkowanymi jednostkami organizacyjnymi.
3. Naczelny Dowódca sił zbrojnych w szczególności:
   1) dowodzi siłami, o których mowa w ust. 2, w celu odparcia zbrojnej napaści na terytorium Rzeczypospolitej Polskiej;
   2) zapewnia współdziałanie podległych mu sił zbrojnych z siłami sojuszniczymi w planowaniu i prowadzeniu działań wojennych;
   3) określa, w ramach swojej właściwości, potrzeby sił zbrojnych w zakresie wsparcia ich przez pozamilitarną część systemu obronnego państwa,
   4) wyznacza organy wojskowe do realizacji zadań administracji rządowej i samorządowej w strefie bezpośrednich działań wojennych oraz określa, z wyjątkiem postanowień Rady Ministrów, o których mowa w art. 11 ust. 1 pkt 5, ich zadania i kompetencje.

Art. 17.

Naczelny Dowódca sił zbrojnych przejmuje dowodzenie siłami, o których mowa w art. 16 ust. 2, z chwilą jego mianowania przez Prezydenta Rzeczypospolitej Polskiej, o ile Prezydent Rzeczypospolitej Polskiej nie określi innego terminu przejęcia dowodzenia.

Rozdział 4
ZAKRES OGRANICZEŃ WOLNOŚCI I PRAW CZŁOWIEKA I OBYWATELA

Art. 18.

1. Na obszarze, na którym został wprowadzony stan wojenny, ograniczeniom wolności i praw człowieka i obywatela podlegają wszystkie osoby fizyczne zamieszkałe lub przebywające tam chociażby czasowo, a także ograniczenia te stosuje się odpowiednio wobec osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej mających siedzibę lub prowadzących działalność na obszarze objętym stanem wojennym.
2. Rodzaje ograniczeń wolności i praw człowieka i obywatela określone w rozporządzeniu, o którym mowa w art. 3 ust. 1, powinny odpowiadać charakterowi oraz intensywności zagrożeń stanowiących przyczyny wprowadzenia stanu wojennego, a także zapewniać skuteczne przywrócenie normalnego funkcjonowania państwa.

publicznych oraz po zasięgnięciu opinii Prezesa Narodowego Banku Polskiego w odniesieniu do bankowych systemów telekomunikacyjnych - w przypadku ograniczeń określonych w ust. 1 pkt 5;
5) ministra właściwego do spraw wewnętrznych oraz Ministra Obrony Narodowej w odniesieniu do żołnierzy zawodowych - w przypadku ograniczeń określonych w ust. 1 pkt 6;
6) właściwego wojewodę - w przypadku stosowania ograniczenia określonego w ust. 1 pkt 3 do szkół, z wyłączeniem szkół wyższych.

3. W rozporządzeniach, o których mowa w ust. 2, określa się szczegółowy tryb i sposoby oraz obszarowy, podmiotowy i przedmiotowy zakres wprowadzenia i stosowania ograniczeń wolności i praw człowieka i obywatela, uwzględniając w możliwym stopniu minimalizację indywidualnych i społecznych uciążliwości wynikających ze stosowania tych ograniczeń.

Art. 25.

1. W czasie stanu wojennego można:
   1) nakładać na przedsiębiorców dodatkowe zadania, których realizacja jest niezbędna dla bezpieczeństwa lub obronności państwa oraz zapewnienia zaopatrzenia ludności;
   2) wprowadzić zarząd komisaryczny, o którym mowa w odrębnych przepisach, dla przedsiębiorców, w tym z udziałem kapitału zagranicznego, jeżeli przedmiotem ich działalności jest wytwarzanie wyrobów lub świadczenie usług o szczególnym znaczeniu dla bezpieczeństwa lub obronności państwa;
   3) nałożyć na osoby fizyczne i osoby prawne prowadzące gospodarstwa rolne obowiązek wykonywania świadczeń polegających na dostawach na rzecz określonych podmiotów produktów rolno-spożywczych oraz na uprawie określonych gatunków roślin i hodowli zwierząt;
   4) wprowadzić najem lokali i budynków na podstawie decyzji administracyjnej o przydziale w stosunku do wszystkich lokali i budynków, a w uzasadnionych przypadkach także dokwaterowywanie osób do lokalu mieszkalnego lub budynku;
   5) wprowadzić zajęcie nieruchomości niezbędnych dla sił zbrojnych lub obrony państwa.
2. Określone w ust. 1 ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniu, o którym mowa w art. 3 ust. 1, wprowadza się i stosuje w drodze:
   1) rozporządzeń Rady Ministrów - w przypadku ograniczeń określonych w ust. 1 pkt 3-5;
   2) decyzji organów administracji rządowej - w przypadku ograniczeń określonych w ust. 1 pkt 1 i 2.
3. W rozporządzeniach, o których mowa w ust. 2 pkt 1, określa się szczegółowy tryb i sposoby oraz obszarowy, podmiotowy i przedmiotowy zakres wprowadzenia i stosowania ograniczeń wolności i praw człowieka i obywatela, uwzględniając w możliwym stopniu minimalizację indywidualnych i społecznych uciążliwości wynikających ze stosowania tych ograniczeń.

Art. 26.

1. W czasie stanu wojennego może być wprowadzony:
   1) całkowity albo częściowy zakaz lub ograniczenie przewozu osób i rzeczy w transporcie drogowym, kolejowym, lotniczym, morskim i żegludze śródlądowej;
   2) całkowity albo częściowy zakaz lotów polskich i obcych statków powietrznych nad terytorium lądowym i morzem terytorialnym Rzeczypospolitej Polskiej;
   3) całkowity albo częściowy zakaz lub ograniczenie ruchu polskich i obcych jednostek pływających na morskich wodach wewnętrznych, na morzu terytorialnym i na śródlądowych drogach wodnych;
   4) całkowity albo częściowy zakaz lub ograniczenie ruchu wszelkich pojazdów na drogach publicznych;
   5) obowiązek wykonywania przez przewoźników przewozu na potrzeby obronności i bezpieczeństwa państwa.
2. Określone w ust. 1 ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniu, o którym mowa w art. 3 ust. 1, wprowadza się i stosuje w drodze rozporządzeń wydawanych przez:
   1) ministrów właściwych do spraw transportu i gospodarki morskiej, w porozumieniu z Ministrem Obrony Narodowej i ministrem właściwym do spraw wewnętrznych - w przypadku ograniczeń określonych w ust. 1 pkt 1 i 3-5;
   2) Ministra Obrony Narodowej, w porozumieniu z ministrami właściwymi do spraw transportu i gospodarki morskiej - w przypadku ograniczenia określonego w ust. 1 pkt 2.
3. W rozporządzeniach, o których mowa w ust. 2, określa się szczegółowy tryb i sposoby oraz obszarowy, podmiotowy i przedmiotowy zakres wprowadzenia i stosowania ograniczeń wolności i praw człowieka i obywatela, uwzględniając w możliwym stopniu minimalizację indywidualnych i społecznych uciążliwości wynikających ze stosowania tych ograniczeń.

Art. 27.

1. W czasie stanu wojennego można zająć lub zarekwirować na potrzeby obronne państwa środki transportu drogowego, kolejowego, lotniczego oraz statki morskie i żeglugi śródlądowej.

Art. 22.

1. W czasie stanu wojennego mogą być zawieszone prawa do:
   1) organizowania i przeprowadzania wszelkiego rodzaju zgromadzeń;
   2) organizowania i przeprowadzania imprez masowych oraz prowadzonych w ramach działalności kulturalnej imprez artystycznych i rozrywkowych niebędących imprezami masowymi;
   3) zrzeszania się poprzez nakazanie okresowego zaniechania działalności zarejestrowanych stowarzyszeń, partii politycznych, związków zawodowych, organizacji społeczno-zawodowych rolników, organizacji pracodawców, ruchów obywatelskich oraz innych dobrowolnych zrzeszeń i fundacji, których działalność może utrudnić realizację zadań obronnych.
2. Przepis ust. 1 pkt 1 nie dotyczy zgromadzeń organizowanych przez kościoły i inne związki wyznaniowe oraz organizacje religijne działające w obrębie świątyń, budynków kościelnych, w innych pomieszczeniach służących organizowaniu i publicznemu sprawowaniu kultu, a także zgromadzeń organizowanych przez organy państwa lub organy samorządu terytorialnego.
3. Pozwolenia na zbiórki publiczne na obszarze, na którym wprowadzono stan wojenny, mogą być udzielane tylko wówczas, gdy w ocenie organu właściwego do udzielenia pozwolenia przeprowadzenie zbiórki nie utrudni realizacji celów wprowadzenia stanu wojennego.

Art. 23.

1. Na obszarze obowiązywania stanu wojennego na osobę, która ukończyła 18 lat, przebywającą w miejscu publicznym może być nałożony obowiązek posiadania przy sobie dowodu osobistego lub innego dokumentu stwierdzającego tożsamość, a na osobę uczącą się, która nie ukończyła 18 lat - legitymacji szkolnej.
2. W czasie stanu wojennego mogą być wprowadzone nakazy lub zakazy:
   1) przebywania lub opuszczania w ustalonym czasie oznaczonych miejsc, obiektów i obszarów;
   2) uzyskania zezwolenia organów administracji publicznej na zmianę miejsca pobytu stałego i czasowego;
   3) zgłoszenia w ustalonym terminie organom ewidencji ludności lub Policji przybycia do określonej miejscowości;
   4) utrwalania przy pomocy środków technicznych wyglądu lub innych cech określonych miejsc, obiektów lub obszarów.

Art. 24.

1. W czasie stanu wojennego mogą być wprowadzone ograniczenia wolności i praw człowieka i obywatela w zakresie:
   1) dostępu do towarów konsumpcyjnych, poprzez całkowitą lub częściową reglamentację zaopatrzenia ludności;
   2) wolności działalności gospodarczej, poprzez nakazanie okresowego zaniechania prowadzenia działalności gospodarczej określonego rodzaju albo ustanowienie obowiązku uzyskania zezwolenia na rozpoczęcie działalności gospodarczej określonego rodzaju;
   3) działalności edukacyjnej, poprzez okresowe zawieszenie zajęć dydaktycznych w szkołach, włącznie ze szkołami wyższymi, z wyjątkiem szkół duchownych i seminariów duchownych;
   4) obrotu krajowymi środkami płatniczymi, obrotu dewizowego oraz działalności kantorowej;
   5) funkcjonowania systemów łączności oraz działalności telekomunikacyjnej i pocztowej, poprzez nakazanie wyłączenia urządzeń łączności lub zawieszenia świadczenia usług, na czas określony, a także poprzez nakazanie niezwłocznego złożenia do depozytu właściwego organu administracji rządowej radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych lub ustalenie innego sposobu ich zabezpieczenia przed wykorzystaniem w sposób zagrażający bezpieczeństwu lub obronności państwa;
   6) prawa posiadania broni palnej, amunicji i materiałów wybuchowych oraz innych rodzajów broni lub określonych przedmiotów, poprzez nakazanie niezwłocznego złożenia do depozytu właściwego organu administracji rządowej albo zakazanie noszenia;
   7) dostępu do informacji publicznej.
2. Określone w ust. 1 ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniu, o którym mowa w art. 3 ust. 1, wprowadza się i stosuje w drodze rozporządzeń wydawanych przez:
   1) Radę Ministrów - w przypadku ograniczeń określonych w ust. 1 pkt 1, 2 i 7;
   2) właściwego ministra - w przypadku jeżeli ograniczenie określone w ust. 1 pkt 3 dotyczy szkół jemu podległych;
   3) ministra właściwego do spraw finansów publicznych, po zasięgnięciu opinii Prezesa Narodowego Banku Polskiego - w przypadku ograniczenia określonego w ust. 1 pkt 4;
   4) ministra właściwego do spraw łączności, działającego w porozumieniu z ministrem właściwym do spraw wewnętrznych, Ministrem Obrony Narodowej i ministrem właściwym do spraw finansów

6) wbrew nakazowi określonemu w art. 23 ust. 2 pkt 3 nie zgłasza w ustalonym terminie organowi ewidencji ludności lub Policji przybycia do określonej miejscowości;
7) wbrew zakazowi określonemu w art. 23 ust. 2 pkt 4 utrwala przy pomocy środków technicznych wygląd lub inną cechę określonego miejsca, obiektu lub obszaru;
8) wbrew nakazowi określonemu w art. 24 ust. 1 pkt 1 narusza zasady reglamentacji żywności;
9) wbrew obowiązkowi określonemu w art. 24 ust. 1 pkt 2 nie stosuje się do nakazu okresowego zaniechania prowadzenia działalności gospodarczej określonego rodzaju albo bez wymaganego zezwolenia rozpoczyna działalność gospodarczą określonego rodzaju;
10) wbrew zakazowi określonemu w art. 24 ust. 1 pkt 3 organizuje lub przeprowadza zajęcia dydaktyczne w szkołach;
11) wbrew zakazowi określonemu w art. 24 ust. 1 pkt 4 nie stosuje się do wprowadzonych ograniczeń w obrocie krajowymi środkami płatniczymi, obrocie dewizowym oraz działalności kantorowej;
12) wbrew obowiązkowi określonemu w art. 24 ust. 1 pkt 5 nie stosuje się do nakazu wyłączenia na czas określony urządzeń łączności lub zawieszenia usług albo nakazu niezwłocznego złożenia do depozytu radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych lub innego sposobu ich zabezpieczenia;
13) wbrew obowiązkowi określonemu w art. 24 ust. 1 pkt 6 nie stosuje się do nakazu niezwłocznego złożenia do depozytu broni palnej, amunicji, materiałów wybuchowych, innych rodzajów broni lub określonych przedmiotów albo zakazu ich noszenia;
14) wbrew obowiązkowi określonemu w art. 24 ust. 1 pkt 7 nie stosuje się do wprowadzonych ograniczeń w dostępie do informacji publicznej;
15) wbrew obowiązkowi określonemu w art. 25 ust. 1 pkt 1 uchyla się od wykonania dodatkowego zadania gospodarczego;
16) wbrew obowiązkowi określonemu w art. 25 ust. 1 pkt 3 nie wykonuje świadczenia polegającego na dostawie na rzecz określonego podmiotu produktów rolno-spożywczych, nie uprawia określonego gatunku roślin lub nie hoduje określonego gatunku zwierząt albo utrudnia lub udaremnia wykonywanie tego obowiązku przez osobę do tego zobowiązaną;
17) w warunkach określonych w art. 25 ust. 1 pkt 4 uniemożliwia osobie uprawnionej zajęcie przydzielonego lokalu lub budynku albo uporczywie utrudnia korzystanie z przydzielonej części lokalu mieszkalnego lub budynku;
18) wbrew obowiązkowi określonemu w art. 26 ust. 1 pkt 1 nie stosuje się do całkowitego lub częściowego zakazu przewozu osób lub rzeczy w transporcie drogowym, kolejowym, lotniczym, morskim lub żegludze śródlądowej albo do ograniczenia w tym przewozie;
19) wbrew obowiązkowi określonemu w art. 26 ust. 1 pkt 2 nie stosuje się do całkowitego albo częściowego zakazu lotów polskich i obcych statków powietrznych nad terytorium lądowym lub morzem terytorialnym Rzeczypospolitej Polskiej;
20) wbrew obowiązkowi określonemu w art. 26 ust. 1 pkt 3 nie stosuje się do całkowitego albo częściowego zakazu ruchu polskich i obcych jednostek pływających na morskich wodach wewnętrznych, morzu terytorialnym lub na śródlądowych drogach wodnych albo do ograniczenia w tym ruchu;
21) wbrew obowiązkowi określonemu w art. 26 ust. 1 pkt 4 nie stosuje się do całkowitego albo częściowego zakazu ruchu pojazdów na drodze publicznej, albo do ograniczenia w tym ruchu;
22) wbrew obowiązkowi określonemu w art. 26 ust. 1 pkt 5 nie wykonuje przewozu na potrzeby obronności i bezpieczeństwa państwa;
23) wbrew obowiązkowi określonemu w art. 29 ust. 1 uchyla się od wykonywania pracy - podlega karze aresztu albo grzywny.

2. Rozpoznawanie spraw określonych w ust. 1 następuje w trybie przepisów o postępowaniu w sprawach o wykroczenia w postępowaniu przyśpieszonym.

Art. 34.

1. Niewykonane w całości lub w części do dnia zniesienia stanu wojennego lub uchylenia odpowiednich ograniczeń wolności i praw człowieka i obywatela kary za przestępstwa i wykroczenia wymierzone na podstawie przepisów ustawy podlegają wykonaniu.
2. Postępowania w sprawach, o których mowa w art. 31-33, wszczęte i niezakończone orzeczeniem kończącym postępowanie do dnia zniesienia stanu wojennego lub uchylenia odpowiednich ograniczeń wolności i praw człowieka i obywatela, prowadzi się na podstawie przepisów ustawy, a wymierzone kary podlegają wykonaniu.
3. Po zniesieniu stanu wojennego postępowanie w sprawach o wykroczenia określone w niniejszej ustawie prowadzi się na zasadach ogólnych.

2. Ministrowie właściwi do spraw transportu i gospodarki morskiej, w porozumieniu z Ministrem Obrony Narodowej i ministrem właściwym do spraw wewnętrznych, w drodze rozporządzenia, określą tryb zajmowania lub rekwirowania oraz zwrotu środków transportu, o których mowa w ust. 1, a także organy właściwe w tych sprawach, z uwzględnieniem konieczności udokumentowania przeprowadzonej czynności i wydania stosownego potwierdzenia posiadaczowi środka transportu, a także pouczenia o możliwości ubiegania się o odszkodowanie za szkody wynikłe z wprowadzonego ograniczenia.

Art. 28.

1. W czasie stanu wojennego można:
   1) zamykać lub ograniczać ruch osobowy i towarowy przez przejścia graniczne;
   2) wprowadzić szczególne zasady wydawania dokumentów uprawniających obywateli polskich do przekraczania granicy państwowej;
   3) wprowadzić szczególne zasady wydawania dokumentów uprawniających cudzoziemców do przekraczania granicy państwowej oraz przebywania na terytorium Rzeczypospolitej Polskiej.
2. Określone w ust. 1 ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniu, o którym mowa w art. 3 ust. 1, wprowadza i stosuje, w drodze rozporządzenia, minister właściwy do spraw wewnętrznych, w porozumieniu z ministrem właściwym do spraw zagranicznych i Ministrem Obrony Narodowej, uwzględniając w możliwym stopniu minimalizację indywidualnych i społecznych uciążliwości wynikających ze stosowania tych ograniczeń.

Art. 29.

1. W czasie stanu wojennego może być wprowadzony powszechny obowiązek wykonywania pracy przez osoby, które ukończyły 16 lat, a nie przekroczyły 65 lat i są zdolne do wykonywania pracy ze względu na stan zdrowia oraz warunki osobiste i rodzinne.
2. Ograniczenie, o którym mowa w ust. 1, wprowadza Rada Ministrów, w drodze rozporządzenia, określając kategorie osób niepodlegających powszechnemu obowiązkowi wykonywania pracy oraz tryb i warunki dokonywania przeniesień osób do pracy w innych miejscowościach, uwzględniając minimalizację uciążliwości wynikających dla tych osób ze stosowania tego ograniczenia.

Art. 30.

W czasie stanu wojennego redaktorzy naczelni dzienników oraz nadawcy programów radiowych i telewizyjnych są obowiązani, na żądanie organów administracji publicznej, do nieodpłatnego, niezwłocznego publikowania lub zamieszczania komunikatów, decyzji i postanowień tych organów związanych z obronnością państwa i bezpieczeństwem obywateli.

Rozdział 5
PRZEPISY KARNE

Art. 31.

Kto w czasie stanu wojennego, będąc członkiem stowarzyszenia, partii politycznej, związku zawodowego, organizacji społeczno-zawodowej rolników, organizacji pracodawców, ruchów obywatelskich lub innych dobrowolnych zrzeszeń lub fundacji, których działalność została zawieszona, nie zaprzestał udziału w ich działalności, podlega karze pozbawienia wolności do lat 3.

Art. 32.

1. Kto w czasie stanu wojennego organizuje strajk, akcję protestacyjną lub inną formę protestu, o których mowa w art. 19 pkt 1-3, albo nimi kieruje, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
2. Kto w czasie stanu wojennego w celu przeprowadzenia strajku, akcji protestacyjnej lub innej formy protestu, o których mowa w ust. 1, albo w czasie ich trwania przemocą, groźbą bezprawną lub podstępem zmusza inną osobę do zaniechania wykonywania pracy, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
3. Kto w czasie stanu wojennego w celu przeprowadzenia strajku, akcji protestacyjnej lub innej formy protestu, o których mowa w ust. 1, niszczy, uszkadza lub czyni niezdatnymi do użytku obiekty lub urządzenia przedsiębiorców, instytucji lub innych jednostek organizacyjnych albo uniemożliwia lub utrudnia prawidłowe ich funkcjonowanie, podlega karze pozbawienia wolności od roku do lat 10.

Art. 33.

1. Kto w czasie stanu wojennego:
   1) wbrew zakazowi określonemu w art. 22 ust. 1 pkt 1 organizuje lub przeprowadza zgromadzenie;
   2) wbrew zakazowi określonemu w art. 22 ust. 1 pkt 2 organizuje lub przeprowadza imprezę masową albo inną imprezę artystyczną lub rozrywkową, niebędącą imprezą masową;
   3) wbrew obowiązkowi określonemu w art. 23 ust. 1 nie posiada przy sobie dowodu osobistego lub innego dokumentu stwierdzającego tożsamość;
   4) wbrew nakazowi lub zakazowi określonemu w art. 23 ust. 2 pkt 1 przebywa lub nie opuszcza w ustalonym czasie oznaczonego miejsca, obiektu lub obszaru;
   5) wbrew nakazowi określonemu w art. 23 ust. 2 pkt 2 zmienia miejsce pobytu stałego lub czasowego bez wymaganego zezwolenia;

1) warunki i tryb planowania i finansowania zadań wykonywanych w ramach przygotowań obronnych państwa realizowanych przez organy administracji rządowej i organy samorządu terytorialnego, sposób ich nakładania oraz właściwość organów w tych sprawach, w tym ujętych w planowaniu operacyjnym i programach obronnych,
2) organizację i tryb przygotowania systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa, oraz warunki funkcjonowania organów władzy publicznej na stanowiskach kierowania,
3) stany gotowości obronnej państwa, ich rodzaje, warunki wprowadzania, zadania związane z podwyższaniem gotowości obronnej państwa i tryb ich realizacji, organizację i zadania w zakresie tworzenia systemu stałych dyżurów na potrzeby podwyższania gotowości obronnej państwa oraz właściwość organów w tych sprawach,
4) obiekty szczególnie ważne dla bezpieczeństwa i obronności państwa, ich kategorie, a także zadania w zakresie ich szczególnej ochrony oraz właściwość organów w tych sprawach,
5) organizację i warunki przygotowania oraz funkcjonowania systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania o skażeniach promieniotwórczych na terytorium Rzeczypospolitej Polskiej oraz właściwość organów w tych sprawach,
6) warunki i sposób przygotowania i wykorzystania transportu morskiego, samochodowego, lotniczego, żeglugi śródlądowej oraz drogownictwa na potrzeby obronne państwa, a także ich ochrony w czasie wojny oraz właściwość organów w tych sprawach,
7) warunki i sposób przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa oraz właściwość organów w tych sprawach,
8) warunki i sposób przygotowania i wykorzystania publicznej i niepublicznej służby zdrowia na potrzeby obronne państwa oraz właściwość organów w tych sprawach,
9) organizację szkolenia obronnego w państwie, podmioty objęte tym szkoleniem, zadania w zakresie planowania i realizacji szkolenia obronnego oraz właściwość organów w tych sprawach,
10) zakres i sposób prowadzenia przez organy administracji rządowej i samorządu terytorialnego kontroli realizacji zadań obronnych wykonywanych przez jednostki organizacyjne i przedsiębiorców.";

4) skreśla się art. 7-10;
5) w art. 11:
   a) ust. 1 otrzymuje brzmienie:
      „1. Prezydent Rzeczypospolitej Polskiej wykonuje zadania w zakresie bezpieczeństwa i obronności przy pomocy Biura Bezpieczeństwa Narodowego.",
   b) ust. 3 otrzymuje brzmienie:
      „3. Biurem Bezpieczeństwa Narodowego kieruje sekretarz stanu wyznaczony przez Prezydenta Rzeczypospolitej Polskiej.";
6) w art. 18 w ust. 2 po wyrazie „określa" dodaje się przecinek i wyrazy „w drodze rozporządzenia,";
7) art. 20 otrzymuje brzmienie:„Art. 20.
   1. Kierowanie sprawami obronności w województwie należy do wojewody.
   2. Wojewoda w ramach kierowania, o którym mowa w ust. 1, wykonuje zadania w zakresie i na zasadach określonych w ustawach, a w szczególności:
      1) określa szczegółowe kierunki działania dla kierowników zespolonych służb, inspekcji i straży, organów administracji niezespolonej oraz jednostek samorządu terytorialnego w zakresie realizacji zadań obronnych,
      2) kieruje realizacją przedsięwzięć związanych z podwyższaniem gotowości obronnej państwa wykonywanych przez starostów, wójtów lub burmistrzów (prezydentów miast), przedsiębiorców oraz inne jednostki organizacyjne i organizacje społeczne mające swoją siedzibę na terenie województwa,
      3) koordynuje przedsięwzięcia niezbędne dla zabezpieczenia mobilizacji jednostek wojskowych i wykonywania świadczeń na rzecz obrony,
      4) kieruje realizacją przedsięwzięć związanych z przygotowaniem stanowisk kierowania dla organów terenowych,
      5) organizuje wykorzystanie miejscowych sił i środków na potrzeby obronności państwa i obszaru województwa, w tym ochrony ludności oraz dóbr materialnych i kultury przed środkami rażenia, jak również niesienia pomocy poszkodowanym,
      6) kontroluje i ocenia wykonywanie zadań obronnych przez organy, podmioty, jednostki organizacyjne i organizacje, o których mowa w pkt 1 i 2,
      7) organizuje edukację społeczeństwa dotyczącą przygotowania obronnego oraz prowadzi szkolenia i ćwiczenia obronne.";
8) skreśla się art. 21.

Rozdział 6
ZMIANY W PRZEPISACH OBOWIĄZUJĄCYCH I PRZEPISY KOŃCOWE
Art. 35.

W ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2002 r. Nr 21, poz. 205, Nr 74, poz. 676, Nr 81, poz. 732 i Nr 113, poz. 984 i 985) wprowadza się następujące zmiany:

1) po art. 4 dodaje się art. 4a w brzmieniu:

„Art. 4a.

1. Prezydent Rzeczypospolitej Polskiej, stojąc na straży suwerenności i bezpieczeństwa państwa, nienaruszalności i niepodzielności jego terytorium, w szczególności:
   1) zatwierdza, na wniosek Prezesa Rady Ministrów, strategię bezpieczeństwa narodowego,
   2) wydaje, na wniosek Prezesa Rady Ministrów, w drodze postanowienia, Polityczno-Strategiczną Dyrektywę Obronną Rzeczypospolitej Polskiej oraz inne dokumenty wykonawcze do strategii bezpieczeństwa narodowego,
   3) zatwierdza, na wniosek Rady Ministrów, plany krajowych ćwiczeń systemu obronnego i kieruje ich przebiegiem,
   4) postanawia, na wniosek Prezesa Rady Ministrów, o wprowadzeniu albo zmianie określonego stanu gotowości obronnej państwa,
   5) może zwracać się do wszystkich organów władzy publicznej, administracji rządowej i samorządowej, przedsiębiorców, kierowników innych jednostek organizacyjnych oraz organizacji społecznych o informacje mające znaczenie dla bezpieczeństwa i obronności państwa,
   6) inicjuje i patronuje przedsięwzięciom ukierunkowanym na kształtowanie postaw patriotycznych i obronnych w społeczeństwie.
2. Informacje, o których mowa w ust. 1 pkt 5, przekazywane są bezzwłocznie.";

2) art. 5 otrzymuje brzmienie:

„Art. 5.

Prezydent Rzeczypospolitej Polskiej, sprawując zwierzchnictwo nad siłami Zbrojnymi Rzeczypospolitej Polskiej, w szczególności:
1) określa, na wniosek Ministra Obrony Narodowej, główne kierunki rozwoju sił zbrojnych Rzeczypospolitej Polskiej oraz ich przygotowań do obrony państwa,
2) uczestniczy w odprawach kierowniczej kadry Ministerstwa Obrony Narodowej i sił zbrojnych Rzeczypospolitej Polskiej i może je zwoływać.";

3) art. 6 otrzymuje brzmienie:

„Art. 6.

1. Do zadań Rady Ministrów wykonywanych w ramach zapewniania zewnętrznego bezpieczeństwa państwa i sprawowania ogólnego kierownictwa w dziedzinie obronności kraju należy w szczególności:
   1) opracowywanie projektów strategii bezpieczeństwa narodowego,
   2) planowanie i realizacja przygotowań obronnych państwa zapewniających jego funkcjonowanie w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny, w tym planowanie przedsięwzięć gospodarczo-obronnych oraz zadań wykonywanych na rzecz sił zbrojnych Rzeczypospolitej Polskiej i wojsk sojuszniczych,
   3) przygotowywanie systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa, i organów władzy publicznej do funkcjonowania na stanowiskach kierowania,
   4) utrzymywanie stałej gotowości obronnej państwa, wnioskowanie do Prezydenta Rzeczypospolitej Polskiej o jej podwyższanie w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny oraz o jej obniżanie stosownie do zmniejszania stopnia zagrożenia,
   5) określanie obiektów szczególnie ważnych dla bezpieczeństwa państwa, w tym obronności, oraz przygotowywanie ich szczególnej ochrony,
   6) przygotowanie na potrzeby obronne państwa i utrzymywanie w stałej gotowości jednolitych systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania,
   7) przygotowanie systemu stałych dyżurów na czas zewnętrznego zagrożenia bezpieczeństwa państwa i wojny,
   8) określanie zasad wykorzystania służby zdrowia i infrastruktury technicznej państwa na potrzeby obronne, w tym sposobu zabezpieczania przestrzeni powietrznej i wód terytorialnych w razie zewnętrznego zagrożenia bezpieczeństwa i w czasie wojny,
   9) zapewnianie funkcjonowania systemu szkolenia obronnego w państwie,
   10) prowadzenie kontroli stanu przygotowań obronnych w państwie.
2. Rada Ministrów określa, w drodze rozporządzenia, tryb realizacji zadań, o których mowa w ust. 1, w szczególności:

Załącznik 5

USTAWA
z dnia 21 czerwca 2002 r.
O STANIE WYJĄTKOWYM
(Dz.U. z 2002 r. Nr 113, poz. 985, Nr 153, poz. 1271).

Rozdział 1
PRZEPISY OGÓLNE
Art. 1

Ustawa określa tryb wprowadzenia i zniesienia stanu wyjątkowego, a także zasady działania organów władzy publicznej oraz zakres, w jakim mogą być ograniczone wolności i prawa człowieka i obywatela w czasie stanu wyjątkowego.

Art. 2.

1. W sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami terrorystycznymi, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego.
2. We wniosku, o którym mowa w ust. 1, Rada Ministrów określa przyczyny wprowadzenia i niezbędny czas trwania stanu wyjątkowego oraz obszar, na jakim stan wyjątkowy powinien być wprowadzony, a także odpowiednie do stopnia i charakteru zagrożenia, w zakresie dopuszczonym niniejszą ustawą, rodzaje ograniczeń wolności i praw człowieka i obywatela.

Art. 3.

1. Prezydent Rzeczypospolitej Polskiej niezwłocznie rozpatruje wniosek, o którym mowa w art. 2 ust. 1, a następnie wydaje rozporządzenie o wprowadzeniu stanu wyjątkowego na czas oznaczony nie dłuższy niż 90 dni lub postanawia odmówić wydania takiego rozporządzenia. Rozporządzenie o wprowadzeniu stanu wyjątkowego Prezydent Rzeczypospolitej Polskiej przedstawia Sejmowi w ciągu 48 godzin od jego podpisania.
2. W rozporządzeniu o wprowadzeniu stanu wyjątkowego określa się przyczyny wprowadzenia, czas trwania i obszar, na jakim wprowadza się stan wyjątkowy.

Opracowano na podstawie: Dz.U. z 2002 r. Nr 113, poz. 985, Nr 153, poz. 1271. oraz, w zakresie dopuszczonym niniejszą ustawą, rodzaje ograniczeń wolności i praw człowieka i obywatela.

Art. 4.

1. Stan wyjątkowy obowiązuje od dnia ogłoszenia rozporządzenia, o którym mowa w art. 3 ust. 1, w Dzienniku Ustaw Rzeczypospolitej Polskiej.
2. W przypadku uchylenia rozporządzenia, o którym mowa w art. 3 ust. 1, przez Sejm Rzeczypospolitej Polskiej, uchwałę Sejmu w tej sprawie niezwłocznie ogłasza się w Dzienniku Ustaw Rzeczypospolitej Polskiej.
3. Rozporządzenie Prezydenta Rzeczypospolitej Polskiej o wprowadzeniu stanu wyjątkowego oraz inne akty prawne dotyczące tego stanu podaje się do publicznej wiadomości, w drodze obwieszczenia właściwego wojewody, przez rozplakatowanie w miejscach publicznych, a także w sposób zwyczajowo przyjęty na danym obszarze.

Art. 5.

1. Jeżeli pomimo zbliżającego się upływu czasu, na jaki został wprowadzony stan wyjątkowy nie ustały przyczyny wprowadzenia tego stanu oraz nie zostało przywrócone normalne funkcjonowanie państwa, Prezydent Rzeczypospolitej Polskiej może, w drodze rozporządzenia, przedłużyć czas trwania stanu wyjątkowego na okres nie dłuższy niż 60 dni.
2. Prezydent Rzeczypospolitej Polskiej, na wniosek Rady Ministrów, w drodze rozporządzenia, znosi stan wyjątkowy przed upływem czasu, na jaki został wprowadzony, jeżeli ustaną przyczyny wprowadzenia tego stanu oraz zostanie przywrócone normalne funkcjonowanie państwa.
3. Przepisy art. 2-4 stosuje się odpowiednio do rozporządzenia, o którym mowa w ust. 1.
4. Przepisy art. 4 ust.1 i 3 stosuje się odpowiednio do rozporządzenia, o którym mowa w ust. 2.

Art. 6.

Redaktorzy naczelni dzienników oraz nadawcy programów radiowych i telewizyjnych są obowiązani do niezwłocznego, nieodpłatnego podania do publicznej wiadomości rozporządzenia Prezydenta Rzeczypospolitej Polskiej o wprowadzeniu stanu wyjątkowego i innych aktów prawnych dotyczących tego stanu, przekazanych im przez wojewodę właściwego ze względu na siedzibę redakcji lub nadawcy.

Art. 7.

Minister właściwy do spraw zagranicznych notyfikuje Sekretarzowi Generalnemu Organizacji Narodów Zjednoczonych oraz Sekretarzowi Generalnemu Rady Europy wprowadzenie i zniesienie stanu wyjątkowego.

Art. 36.

W ustawie z dnia 31 stycznia 1989 r. o gospodarce finansowej przedsiębiorstw państwowych (Dz. U. z 1992 r. Nr 6, poz. 27, z 1993 r. Nr 18, poz. 82, z 1994 r. Nr 121, poz. 591 i z 1995 r. Nr 154, poz. 791) w art. 10 skreśla się wyrazy "i Komitet Obrony Kraju".

Art. 37.

W ustawie z dnia 14 grudnia 1995 r. o urzędzie Ministra Obrony Narodowej (Dz. U. z 1996 r. Nr 10, poz. 56 i Nr 102, poz. 474, z 1997 r. Nr 121, poz. 770 i Nr 141, poz. 944, z 1999 r. Nr 11, poz. 95 oraz z 2001 r. Nr 123, poz. 1353 i Nr 154, poz. 1800) dotychczasową treść art. 8 oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Szef Sztabu Generalnego Wojska Polskiego odpowiada za organizację i przygotowanie do działań organu dowodzenia i stanowiska dowodzenia Naczelnego Dowódcy sił zbrojnych.".

Art. 38.

Tracą moc:

1) dekret z dnia 12 grudnia 1981 r. o stanie wojennym (Dz. U. Nr 29, poz. 154, z 1982 r. Nr 3, poz. 18 oraz z 1989 r. Nr 34, poz. 178);
2) ustawa z dnia 25 stycznia 1982 r. o szczególnej regulacji prawnej w okresie stanu wojennego (Dz. U. Nr 3, poz. 18 i Nr 41, poz. 272 oraz z 1983 r. Nr 66, poz. 297);
3) ustawa z dnia 18 grudnia 1982 r. o szczególnej regulacji prawnej w okresie zawieszenia stanu wojennego (Dz. U. Nr 41, poz. 273 oraz z 1983 r. Nr 66, poz. 297).

Art. 39.

Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

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

2. Rodzaje ograniczeń wolności i praw człowieka i obywatela określone w rozporządzeniach, o których mowa w art. 3 ust. 1 i art. 5 ust. 1, powinny odpowiadać charakterowi oraz intensywności zagrożeń stanowiących przyczyny wprowadzenia stanu wyjątkowego, a także zapewniać skuteczne przywrócenie normalnego funkcjonowania państwa.

Art. 16.

1. W czasie stanu wyjątkowego mogą być zawieszone prawa do:
   1) organizowania i przeprowadzania wszelkiego rodzaju zgromadzeń,
   2) organizowania i przeprowadzania imprez masowych oraz prowadzonych w ramach działalności kulturalnej imprez artystycznych i rozrywkowych, niebędących imprezami masowymi,
   3) strajków pracowniczych i innych form protestu w odniesieniu do określonych kategorii pracowników lub w określonych dziedzinach,
   4) strajków i innych niż strajki form akcji protestacyjnych rolników,
   5) akcji protestacyjnych studentów organizowanych przez studenckie samorządy, stowarzyszenia lub organizacje,
   6) zrzeszania się poprzez:
      a) ustanowienie zakazu tworzenia i rejestracji nowych stowarzyszeń, partii politycznych, związków zawodowych, organizacji społeczno-zawodowych rolników, organizacji pracodawców, ruchów obywatelskich oraz innych dobrowolnych zrzeszeń i fundacji,
      b) nakazanie okresowego zaniechania działalności zarejestrowanych stowarzyszeń, partii politycznych, związków zawodowych, organizacji społeczno-zawodowych rolników, organizacji pracodawców, ruchów obywatelskich oraz innych dobrowolnych zrzeszeń i fundacji, których działalność może zwiększyć zagrożenie konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego.
2. Przepis ust. 1 pkt 1 nie dotyczy zgromadzeń organizowanych przez kościoły i inne związki wyznaniowe oraz organizacje religijne działające w obrębie świątyń, budynków kościelnych, w innych pomieszczeniach służących organizowaniu i publicznemu sprawowaniu kultu, a także zgromadzeń organizowanych przez organy państwa lub organy samorządu terytorialnego.
3. Pozwolenia na zbiórki publiczne na obszarze, na którym wprowadzono stan wyjątkowy, mogą być udzielane tylko wówczas, gdy w ocenie organu właściwego do udzielenia pozwolenia przeprowadzenie zbiórki nie utrudni realizacji celów wprowadzenia stanu wyjątkowego.

Art. 17.

1. W czasie stanu wyjątkowego może być odosobniona osoba mająca ukończone 18 lat, w stosunku do której zachodzi uzasadnione podejrzenie, że pozostając na wolności będzie prowadziła działalność zagrażającą konstytucyjnemu ustrojowi państwa, bezpieczeństwu obywateli lub porządkowi publicznemu albo gdy odosobnienie jest niezbędne dla zapobieżenia popełnienia czynu karalnego lub uniemożliwienia ucieczki po jego popełnieniu. Nie narusza to immunitetów wynikających z odrębnych przepisów.
2. Odosobniona może być również osoba, która ukończyła 17 lat, jeżeli przeprowadzona uprzednio z nią rozmowa ostrzegawcza okazała się nieskuteczna.
3. Odosobnienie następuje na podstawie decyzji wojewody właściwego ze względu na miejsce pobytu stałego lub czasowego osoby odosobnionej i jest wykonywane przez właściwego komendanta wojewódzkiego Policji, w drodze zatrzymania tej osoby i przymusowego doprowadzenia do ośrodka odosobnienia podległego Ministrowi Sprawiedliwości.
4. Wojewoda, o którym mowa w ust. 3, wszczyna postępowanie w sprawach odosobnienia na wniosek właściwych organów prokuratury, Policji, Agencji Bezpieczeństwa Wewnętrznego, Straży Granicznej, Żandarmerii Wojskowej lub Wojskowych Służb Informacyjnych.
5. Decyzję w sprawie odosobnienia doręcza się osobie odosobnionej niezwłocznie, nie później niż w ciągu 48 godzin od chwili jej wydania. Decyzję tę uchyla się niezwłocznie, jeżeli ustaną przyczyny uzasadniające odosobnienie.
6. Decyzje w sprawach odosobnienia są ostateczne i mogą być zaskarżone bezpośrednio do Naczelnego Sądu Administracyjnego w trybie i na zasadach określonych w odrębnych przepisach, z tym że sąd wyznacza rozprawę w terminie 7 dni od daty otrzymania skargi. Nie stosuje się przepisu art. 34 ust. 3 ustawy z dnia 11 maja 1995 r. o Naczelnym Sądzie Administracyjnym (Dz.U. Nr 74, poz. 368 i Nr 104, poz. 515, z 1997 r. Nr 75, poz. 471, Nr 106, poz. 679, Nr 114, poz. 739 i Nr 144, poz. 971, z 1998 r. Nr 162, poz. 1126, z 1999 r. Nr 75, poz. 853, z 2000 r. Nr 2, poz. 5, Nr 48, poz. 552, Nr 60, poz. 704 i Nr 91, poz. 1008, z 2001 r. Nr 49, poz. 508 i 509, Nr 98, poz. 1070 i Nr 101, poz. 1113 oraz z 2002 r. Nr 113, poz. 984).]
7. Decyzje w sprawach odosobnienia są ostateczne i mogą być zaskarżone bezpośrednio do sądu administracyjnego w trybie i na zasadach określonych w odrębnych przepisach, z tym że sąd wyznacza rozprawę w terminie 7 dni od daty otrzymania skargi. Nie stosuje się przepisów art. 52 § 3 i 4 ustawy

Rozdział 2
ZASADY DZIAŁANIA ORGANÓW WŁADZY PUBLICZNEJ

Art. 8.

W czasie stanu wyjątkowego organy władzy publicznej działają w dotychczasowych strukturach organizacyjnych państwa i w ramach przysługujących im kompetencji, z zastrzeżeniem przepisów niniejszej ustawy.

Art. 9.

Działania przywracające konstytucyjny ustrój państwa, bezpieczeństwo obywateli lub porządek publiczny, a w szczególności koordynację i kontrolę funkcjonowania administracji rządowej i samorządowej wykonują:

1) Prezes Rady Ministrów - w przypadku wprowadzenia stanu wyjątkowego na obszarze większym niż obszar jednego województwa,
2) właściwy wojewoda - w przypadku wprowadzenia stanu wyjątkowego na obszarze lub części obszaru jednego województwa.

Art. 10.

Prezes Rady Ministrów jest obowiązany do informowania na bieżąco Prezydenta Rzeczypospolitej Polskiej o skutkach wprowadzenia stanu wyjątkowego oraz o rodzaju i rezultatach działań podejmowanych w celu przywrócenia normalnego funkcjonowania państwa.

Art. 11.

1. W czasie stanu wyjątkowego Prezydent Rzeczypospolitej Polskiej, na wniosek Prezesa Rady Ministrów, może postanowić o użyciu oddziałów i pododdziałów sił zbrojnych Rzeczypospolitej Polskiej do przywrócenia normalnego funkcjonowania państwa, jeżeli dotychczas zastosowane siły i środki zostały wyczerpane.
2. Użycie oddziałów i pododdziałów sił zbrojnych Rzeczypospolitej Polskiej, o którym mowa w ust. 1, nie może zagrozić ich zdolności do realizacji zadań wynikających z Konstytucji Rzeczypospolitej Polskiej i ratyfikowanych umów międzynarodowych.
3. W przypadku, o którym mowa w ust. 1, oddziały i pododdziały sił zbrojnych Rzeczypospolitej Polskiej pozostają pod dowództwem przełożonych służbowych i wykonują zadania wyznaczone przez Ministra Obrony Narodowej w uzgodnieniu z ministrem właściwym do spraw wewnętrznych. Żołnierzom wyznaczonym do tych oddziałów i pododdziałów przysługują, w zakresie niezbędnym do wykonania ich zadań, uprawnienia policjantów określone w art. 15-17 ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 2002 r. Nr 7, poz. 58, Nr 19, poz. 185, Nr 74, poz. 676, Nr 81, poz. 731 i Nr 113, poz. 984).
4. Rada Ministrów, w drodze rozporządzenia, określi szczegółowe zasady użycia oddziałów i pododdziałów sił zbrojnych Rzeczypospolitej Polskiej w czasie stanu wyjątkowego, uwzględniając stopień i rodzaj zagrożeń stanowiących przyczyny wprowadzenia i trwania stanu wyjątkowego.

Art. 12.

1. Jeżeli organy gminy, powiatu lub samorządu województwa nie wykazują dostatecznej skuteczności w wykonywaniu zadań publicznych lub w realizacji działań wynikających z przepisów o wprowadzeniu stanu wyjątkowego, Prezes Rady Ministrów, na wniosek właściwego wojewody, może zawiesić te organy do czasu zniesienia stanu wyjątkowego lub na czas określony i ustanowić w ich miejsce zarząd komisaryczny sprawowany przez komisarza rządowego.
2. Komisarza rządowego powołuje i odwołuje Prezes Rady Ministrów na wniosek wojewody.
3. Komisarz rządowy z dniem powołania przejmuje wykonywanie zadań i kompetencji zawieszonych organów gminy, powiatu lub samorządu województwa.
4. Stan zawieszenia organów gminy, powiatu lub samorządu województwa ustaje z upływem czasu określonego przez Prezesa Rady Ministrów oraz z mocy prawa z dniem zniesienia stanu wyjątkowego.

Art. 13.

W czasie stanu wyjątkowego organy porządku i bezpieczeństwa publicznego mogą w celu przywrócenia porządku publicznego wkroczyć na teren szkoły wyższej bez wezwania przez rektora, którego należy niezwłocznie o tym zawiadomić.

Art. 14.

Decyzje wydane przez organy władzy publicznej na podstawie niniejszej ustawy lub przepisów wykonawczych podlegają natychmiastowemu wykonaniu. Przepisy o postępowaniu egzekucyjnym w administracji stosuje się odpowiednio.

Rozdział 3
ZAKRES OGRANICZEŃ WOLNOŚCI I PRAW CZŁOWIEKA I OBYWATELA

Art. 15.

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

2. Funkcję organów cenzury i kontroli pełnią właściwi wojewodowie, którzy mogą nakazać organom administracji publicznej działającym na obszarze województwa wykonywanie czynności technicznych, niezbędnych do prowadzenia cenzury lub kontroli.
3. Organy cenzury i kontroli są uprawnione do zatrzymywania w całości lub w części publikacji, przesyłek pocztowych i kurierskich oraz korespondencji telekomunikacyjnej, a także do przerywania rozmów telefonicznych i transmisji sygnałów przesyłanych w sieciach telekomunikacyjnych, jeżeli ich zawartość lub treść może zwiększyć zagrożenie konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego.
4. Zatrzymane publikacje, przesyłki lub korespondencję telekomunikacyjną doręcza się adresatom po zniesieniu stanu wyjątkowego, z zastrzeżeniem ust. 5.
5. Zatrzymane publikacje, przesyłki pocztowe i kurierskie oraz korespondencję telekomunikacyjną, których treść lub zawartość pochodzi z przestępstwa, była przeznaczona do popełnienia przestępstwa albo została objęta zakazem posiadania, organ cenzury i kontroli przekazuje, niezwłocznie a najpóźniej bezpośrednio po zniesieniu stanu wyjątkowego, organom właściwym do prowadzenia postępowania karnego lub orzeczenia przepadku rzeczy.
6. Decyzje organów cenzury i kontroli są ostateczne i mogą być zaskarżone bezpośrednio do Naczelnego Sądu Administracyjnego. Nie stosuje się przepisu art. 34 ust. 3 ustawy o Naczelnym Sądzie Administracyjnym.
7. Cenzura prewencyjna nie obejmuje należących do kościołów i innych związków wyznaniowych, środków społecznego przekazu, stanowiących źródła informacji na temat religii i służących wypełnianiu funkcji religijnych.
8. Rada Ministrów, w drodze rozporządzenia, określi:
   1) tryb postępowania organów cenzury i kontroli uwzględniając potrzebę zapewnienia sprawności i szybkości działania,
   2) organy właściwe w sprawach, o których mowa w ust. 1 pkt 4, oraz tryb postępowania tych organów uwzględniając potrzebę zapewnienia niejawności stosowanych metod i technik działania.

Art. 21.

W czasie stanu wyjątkowego mogą być wprowadzone ograniczenia wolności i praw człowieka i obywatela w zakresie:

1) dostępu do towarów konsumpcyjnych, poprzez całkowitą lub częściową reglamentację zaopatrzenia ludności,
2) wolności działalności gospodarczej, poprzez nakazanie okresowego zaniechania prowadzenia działalności gospodarczej określonego rodzaju albo ustanowienie obowiązku uzyskania zezwolenia na rozpoczęcie działalności gospodarczej określonego rodzaju,
3) działalności edukacyjnej, poprzez okresowe zawieszenie zajęć dydaktycznych w szkołach wyłącznie ze szkołami wyższymi, z wyjątkiem szkół duchownych i seminariów duchownych,
4) obrotu krajowymi środkami płatniczymi, obrotu dewizowego oraz działalności kantorowej,
5) transportu drogowego, kolejowego i lotniczego oraz w ruchu jednostek pływających na morskich wodach wewnętrznych i na morzu terytorialnym, a także na śródlądowych drogach wodnych,
6) funkcjonowania systemów łączności oraz działalności telekomunikacyjnej i pocztowej, poprzez nakazanie wyłączenia urządzeń łączności lub zawieszenia świadczenia usług, na czas określony, a także poprzez nakazanie niezwłocznego złożenia do depozytu właściwego organu administracji rządowej radiowych i telewizyjnych urządzeń nadawczych i nadawczoodbiorczych lub ustalenie innego sposobu ich zabezpieczenia przed wykorzystaniem w sposób zagrażający konstytucyjnemu ustrojowi państwa, bezpieczeństwu obywateli albo porządkowi publicznemu,
7) prawa posiadania broni palnej, amunicji i materiałów wybuchowych oraz innych rodzajów broni lub określonych przedmiotów, poprzez nakazanie niezwłocznego złożenia do depozytu właściwego organu administracji rządowej albo zakazanie noszenia,
8) dostępu do informacji publicznej.

Art. 22.

1. Rada Ministrów, z zastrzeżeniem ust. 2 i 3, określa, w drodze rozporządzeń, szczegółowy tryb i sposoby oraz obszarowy, podmiotowy i przedmiotowy zakres wprowadzenia i stosowania ograniczeń wolności i praw człowieka i obywatela ustalonych przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniach, o których mowa w art. 3 ust. 1 i art. 5 ust. 1, uwzględniając w możliwym stopniu minimalizację indywidualnych i społecznych uciążliwości wynikających ze stosowania tych ograniczeń.
2. Jeżeli stan wyjątkowy został wprowadzony na obszarze jednego województwa lub jego części, określone w ust. 1 kompetencje Rady Ministrów przejmuje właściwy wojewoda.
3. Określone w art. 21 ograniczenia wolności i praw człowieka i obywatela ustalone przez Prezydenta Rzeczypospolitej Polskiej w rozporządzeniach, o których mowa w art. 3 ust. 1 i art. 5 ust. 1, wprowadza się i stosuje w drodze rozporządzeń wydawanych przez:

z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. Nr 153, poz. 1270).

8. W czasie odosobnienia nie może być rozwiązany stosunek pracy z osobą odosobnioną, chyba że przed odosobnieniem zaistniały z jej winy okoliczności uzasadniające rozwiązanie stosunku pracy bez wypowiedzenia. Termin do wniesienia środków prawnych przeciwko rozwiązaniu stosunku pracy liczy się w tych przypadkach od dnia zakończenia odosobnienia.
9. Do pobytu osób odosobnionych w ośrodkach odosobnienia stosuje się odpowiednio przepisy Kodeksu karnego wykonawczego dotyczące praw i obowiązków tymczasowo aresztowanych, wykonywania tymczasowego aresztowania oraz nadzoru penitencjarnego.
10. Minister Sprawiedliwości w porozumieniu z ministrem właściwym do spraw wewnętrznych, w drodze rozporządzenia, tworzy i znosi ośrodki odosobnienia z uwzględnieniem odpowiedniego stopnia zabezpieczenia ośrodków oraz izolacji odosobnionych.

Art. 18.

1. Na obszarze obowiązywania stanu wyjątkowego na osobę, która ukończyła 18 lat, przebywającą w miejscu publicznym może być nałożony obowiązek posiadania przy sobie dowodu osobistego lub innego dokumentu stwierdzającego tożsamość, a na osobę uczącą się, która nie ukończyła 18 lat - legitymacji szkolnej.
2. W czasie stanu wyjątkowego mogą być wprowadzone nakazy lub zakazy: nowe brzmienie ust. 6 w art. 17 wchodzi w życie z dn. 1.01.2004 r. (Dz.U. 2002 r. Nr 153, poz. 1271)
   1) przebywania lub opuszczania w ustalonym czasie oznaczonych miejsc, obiektów i obszarów,
   2) uzyskania zezwolenia organów administracji publicznej na zmianę miejsca pobytu stałego i czasowego,
   3) zgłoszenia w ustalonym terminie organom ewidencji ludności lub Policji przybycia do określonej miejscowości,
   4) utrwalania przy pomocy środków technicznych wyglądu lub innych cech określonych miejsc, obiektów lub obszarów.

Art. 19.

1. W czasie stanu wyjątkowego na wezwanie organów prokuratury, Policji, Agencji Bezpieczeństwa Wewnętrznego, Straży Granicznej, Żandarmerii Wojskowej lub Wojskowych Służb Informacyjnych, osoba mająca ukończone 17 lat jest obowiązana do udziału we wskazanym miejscu w rozmowie ostrzegawczej. Wezwanie to może być przekazane w dowolnej udokumentowanej formie.
2. Do udziału w rozmowie ostrzegawczej można wezwać tylko taką osobę, co do której zachodzi uzasadnione podejrzenie, że nie będzie przestrzegać porządku prawnego.
3. Jeżeli osoba wezwana na rozmowę ostrzegawczą nie zgłosi się dobrowolnie na wskazane miejsce, a fakt otrzymania wezwania nie budzi wątpliwości, może być przymusowo doprowadzona przez organ wzywający.
4. Jeżeli podejrzenie, o którym mowa w ust. 2, dotyczy osoby nie mającej ukończonych 17 lat, wezwanie przekazuje się i przeprowadza rozmowę ostrzegawczą z rodzicami lub rodzicem albo opiekunem prawnym tej osoby. Przepis ust. 3 stosuje się odpowiednio.
5. Rozmowa ostrzegawcza polega na udzieleniu pouczenia o prawnych i osobistych skutkach nieprzestrzegania porządku prawnego oraz niestosowania się do ustalonych na czas stanu wyjątkowego ograniczeń wolności i praw człowieka i obywatela. Osoby obecne przy rozmowie potwierdzają przebieg rozmowy podpisami na protokóle.
6. W przypadku określonym w ust. 4, rozmowa ostrzegawcza odbywa się w obecności osoby, której podejrzenie dotyczy, jeżeli takie jest życzenie rodzica lub opiekuna prawnego tej osoby.

Art. 20.

1. W czasie stanu wyjątkowego może być wprowadzona:
   1) cenzura prewencyjna środków społecznego przekazu obejmująca materiały prasowe w rozumieniu ustawy z dnia 26 stycznia 1984 r. Prawo prasowe (Dz.U. z 1984 r. Nr 5, poz. 24, z 1988 r. Nr 41, poz. 324, z 1989 r. Nr 34, poz. 187, z 1990 r. Nr 29, poz. 173, z 1991 r. Nr 100, poz. 442, z 1996 r. Nr 114, poz. 542, z 1997 r. Nr 88, poz. 554 i Nr 121, poz. 770, z 1999 r. Nr 90, poz. 999 i z 2001 r. Nr 112, poz. 1198), z zastrzeżeniem ust. 7,
   2) kontrola zawartości przesyłek, listów, paczek i przekazów przekazywanych w ramach usług pocztowych o charakterze powszechnym lub usług kurierskich,
   3) kontrola treści korespondencji telekomunikacyjnej i rozmów telefonicznych lub sygnałów przesyłanych w sieciach telekomunikacyjnych,
   4) emisja sygnałów uniemożliwiających nadawanie lub odbiór przekazów radiowych, telewizyjnych lub dokonywanych poprzez urządzenia i sieci telekomunikacyjne, których treść może zwiększyć zagrożenie konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego.

złożenia do depozytu radiowych i telewizyjnych urządzeń nadawczych i nadawczo-odbiorczych lub innego sposobu ich zabezpieczenia,

17) wbrew obowiązkowi określonemu w art. 21 pkt 7 nie stosuje się do nakazu niezwłocznego złożenia do depozytu broni palnej, amunicji, materiałów wybuchowych, innych rodzajów broni lub określonych przedmiotów, albo zakazu ich noszenia,

18) wbrew obowiązkowi określonemu w art. 21 pkt 8 nie stosuje się do wprowadzonych ograniczeń w dostępie do informacji publicznej - podlega karze aresztu albo grzywny.

2. Rozpoznawanie spraw, określonych w ust. 1, następuje w trybie przepisów o postępowaniu w sprawach o wykroczenia w postępowaniu przyśpieszonym.

Art. 24.

1. Niewykonane w całości lub w części do dnia zniesienia stanu wyjątkowego lub uchylenia odpowiednich ograniczeń wolności i praw człowieka i obywatela kary za wykroczenia wymierzone na podstawie przepisów ustawy podlegają wykonaniu.
2. Postępowania w sprawach o wykroczenia określone w niniejszej ustawie, wszczęte i niezakończone orzeczeniem kończącym postępowanie do dnia zniesienia stanu wyjątkowego lub uchylenia odpowiednich ograniczeń wolności i praw człowieka i obywatela, prowadzi się na podstawie przepisów ustawy, a wymierzone kary podlegają wykonaniu.
3. Po zniesieniu stanu wyjątkowego postępowanie w sprawach o wykroczenia określone w niniejszej ustawie prowadzi się na zasadach ogólnych.

Rozdział 5

ZMIANY W PRZEPISACH OBOWIĄZUJĄCYCH I PRZEPISY KOŃCOWE

Art. 25.

W ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz.U. z 2002 r. Nr 21, poz. 205, Nr 74, poz. 676, Nr 81, poz. 732 i Nr 113, poz. 984) w art. 174 dodaje się ust. 4 w brzmieniu: „4. Jednostki organizacyjne, o których mowa w ust. 1 i 2, Rada Ministrów może objąć militaryzacją również w razie wprowadzenia stanu wyjątkowego na całym terytorium Rzeczypospolitej Polskiej.".

Art. 26.

Traci moc ustawa z dnia 5 grudnia 1983 r. o stanie wyjątkowym (Dz.U. Nr 66, poz. 297, z 1989 r. Nr 34, poz. 178 oraz z 1997 r. Nr 81, poz. 512 i Nr 88, poz. 554).

Art. 27.

Ustawa wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia.

1) właściwego ministra - w przypadku jeżeli ograniczenie określone w art. 21 pkt 3 dotyczy szkół jemu podległych,
2) ministra właściwego do spraw finansów publicznych po zasięgnięciu opinii Prezesa Narodowego Banku Polskiego - w przypadku ograniczenia określonego w art. 21 pkt 4,
3) ministrów właściwych do spraw transportu i gospodarki morskiej działających w porozumieniu z Ministrem Obrony Narodowej oraz ministrem właściwym do spraw wewnętrznych - w przypadku ograniczeń określonych w art. 21 pkt 5,
4) ministra właściwego do spraw łączności działającego w porozumieniu z ministrem właściwym do spraw wewnętrznych, Ministrem Obrony Narodowej i ministrem właściwym do spraw finansów publicznych oraz po zasięgnięciu opinii Prezesa Narodowego Banku Polskiego w odniesieniu do bankowych systemów telekomunikacyjnych - w przypadku ograniczeń określonych w art. 21 pkt 6,
5) ministra właściwego do spraw wewnętrznych oraz Ministra Obrony Narodowej w odniesieniu do żołnierzy zawodowych - w przypadku ograniczeń określonych w art. 21 pkt 7,
6) właściwego wojewodę - w przypadku stosowania ograniczenia określonego w art. 21 pkt 3 do szkół, z wyłączeniem szkół wyższych, oraz stosowania ograniczeń określonych w art. 21 pkt 1, 2 i 5, jeżeli stan wyjątkowy wprowadzono na obszarze jednego województwa lub jego części.

4. W rozporządzeniach, o których mowa w ust. 3, określa się szczegółowy tryb i sposoby oraz obszarowy, podmiotowy i przedmiotowy zakres wprowadzenia i stosowania ograniczeń wolności i praw człowieka i obywatela, uwzględniając w możliwym stopniu minimalizację indywidualnych i społecznych uciążliwości wynikających ze stosowania tych ograniczeń.

Rozdział 4
PRZEPISY KARNE
Art. 23.

1. Kto w czasie stanu wyjątkowego:
   1) wbrew zakazowi określonemu w art. 16 ust. 1 pkt 1 organizuje lub przeprowadza zgromadzenie,
   2) wbrew zakazowi określonemu w art. 16 ust. 1 pkt 2 organizuje lub przeprowadza imprezę masową albo inną imprezę artystyczną lub rozrywkową, niebędącą imprezą masową,
   3) wbrew zakazowi określonemu w art. 16 ust. 1 pkt 3-5 uczestniczy w strajku lub innej akcji protestacyjnej pracowników lub rolników, albo akcji protestacyjnej studentów zorganizowanej przez studenckie samorządy, stowarzyszenia lub organizacje,
   4) wbrew zakazowi określonemu w art. 16 ust. 1 pkt 6 lit. a) tworzy stowarzyszenie, partię polityczną, związek zawodowy, organizację społeczno-zawodową rolników, organizację pracodawców, ruch obywatelski, dobrowolne zrzeszenie lub fundację,
   5) wbrew nakazowi określonemu w art. 16 ust. 1 pkt 6 lit. b) uczestniczy w działalności zarejestrowanego stowarzyszenia, partii politycznej, związku zawodowego, organizacji społeczno-zawodowej rolników, organizacji pracodawców, ruchu obywatelskiego, dobrowolnego zrzeszenia lub fundacji,
   6) wbrew obowiązkowi określonemu w art. 18 ust. 1 nie posiada przy sobie dowodu osobistego lub innego dokumentu stwierdzającego tożsamość,
   7) wbrew nakazowi lub zakazowi określonemu w art. 18 ust. 2 pkt 1 przebywa lub nie opuszcza w ustalonym czasie oznaczonego miejsca, obiektu lub obszaru,
   8) wbrew nakazowi określonemu w art. 18 ust. 2 pkt 2 zmienia miejsce pobytu stałego lub czasowego bez wymaganego zezwolenia,
   9) wbrew nakazowi określonemu w art. 18 ust. 2 pkt 3 nie zgłasza w ustalonym terminie organowi ewidencji ludności lub Policji przybycia do określonej miejscowości,
   10) wbrew zakazowi określonemu w art. 18 ust. 2 pkt 4 utrwala przy pomocy środków technicznych wygląd lub inną cechę określonego miejsca, obiektu lub obszaru,
   11) wbrew nakazowi określonemu w art. 21 pkt 1 narusza zasady reglamentacji zaopatrzenia ludności,
   12) wbrew obowiązkowi określonemu w art. 21 pkt 2 nie stosuje się do nakazu zaniechania prowadzenia działalności gospodarczej określonego rodzaju, albo bez wymaganego zezwolenia rozpoczyna działalność gospodarczą określonego rodzaju,
   13) wbrew zakazowi określonemu w art. 21 pkt 3 organizuje lub przeprowadza zajęcia dydaktyczne w szkołach,
   14) wbrew zakazowi określonemu w art. 21 pkt 4 nie stosuje się do wprowadzonych ograniczeń w obrocie krajowymi środkami płatniczymi, obrocie dewizowym oraz działalności kantorowej,
   15) wbrew obowiązkowi określonemu w art. 21 pkt 5 nie stosuje się do ograniczeń w transporcie drogowym, kolejowym lub lotniczym, albo w ruchu jednostek pływających na morskich wodach wewnętrznych, morzu terytorialnym lub na śródlądowych drogach wodnych,
   16) wbrew obowiązkowi określonemu w art. 21 pkt 6 nie stosuje się do nakazu wyłączenia na czas określony urządzeń łączności lub zawieszenia świadczenia usług, albo nakazu niezwłocznego

Rozdział 2
ZASADY DZIAŁANIA ORGANÓW WŁADZY PUBLICZNEJ

Art. 7.

W czasie stanu klęski żywiołowej organy władzy publicznej działają w dotychczasowych strukturach organizacyjnych państwa i w ramach przysługujących im kompetencji, z zastrzeżeniem przepisów niniejszej ustawy.

Art. 8.

W czasie stanu klęski żywiołowej działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia kierują:

1) wójt (burmistrz, prezydent miasta) - jeżeli stan klęski żywiołowej wprowadzono tylko na obszarze gminy,
2) starosta - jeżeli stan klęski żywiołowej wprowadzono na obszarze więcej niż jednej gminy wchodzącej w skład powiatu,
3) wojewoda - jeżeli stan klęski żywiołowej wprowadzono na obszarze więcej niż jednego powiatu wchodzącego w skład województwa,
4) minister właściwy do spraw wewnętrznych lub inny minister do zakresu działania którego należy zapobieganie skutkom danej klęski żywiołowej lub ich usuwanie, a w przypadku wątpliwości co do właściwości ministra lub w przypadku, gdy właściwych jest kilku ministrów - minister wyznaczony przez Prezesa Rady Ministrów - jeżeli stan klęski żywiołowej wprowadzono na obszarze więcej niż jednego województwa.

Art. 9.

1. W czasie stanu klęski żywiołowej właściwy miejscowo wójt (burmistrz, prezydent miasta) kieruje działaniami prowadzonymi na obszarze gminy w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia.
2. W zakresie działań, o których mowa w ust. 1, wójt (burmistrz, prezydent miasta) może wydawać polecenia wiążące organom jednostek pomocniczych, kierownikom jednostek organizacyjnych utworzonych przez gminę, kierownikom jednostek ochrony przeciwpożarowej działających na obszarze gminy oraz kierownikom jednostek organizacyjnych czasowo przekazanych przez właściwe organy do jego dyspozycji i skierowanych do wykonywania zadań na obszarze gminy.
3. W zakresie działań, o których mowa w ust. 1, wójt (burmistrz, prezydent miasta) może występować do kierowników innych jednostek organizacyjnych niż określone w ust. 2, działających na obszarze gminy z wnioskami o wykonanie czynności niezbędnych w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia. W razie odmowy wykonania tych czynności lub ich niewłaściwego wykonywania wójt (burmistrz, prezydent miasta) niezwłocznie zawiadamia organ, któremu podlega kierownik lub który sprawuje nadzór nad nim.
4. W zakresie działań, o których mowa w ust. 1, w przypadkach określonych w art. 8 pkt 2-4, wójt (burmistrz, prezydent miasta nie będącego miastem na prawach powiatu) podlega staroście.
5. W razie niezdolności do kierowania lub niewłaściwego kierowania działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia wojewoda z inicjatywy własnej lub na wniosek starosty może zawiesić uprawnienia wójta (burmistrza, prezydenta miasta), określone w ust. 2 i 3, oraz wyznaczyć pełnomocnika do kierowania tymi działaniami. Do pełnomocnika stosuje się odpowiednio przepis ust. 4.
6. W przypadku, o którym mowa w art. 8 pkt 2, wójt (burmistrz, prezydent miasta) albo pełnomocnik, o którym mowa w ust. 5, wykonują czynności kierownicze na właściwym dla siebie obszarze wobec podmiotów, o których mowa w ust. 2.

Art. 10.

1. W czasie stanu klęski żywiołowej właściwy miejscowo starosta kieruje działaniami prowadzonymi na obszarze powiatu w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia.
2. W zakresie działań, o których mowa w ust. 1, starosta może wydawać polecenia wiążące wójtom (burmistrzom, prezydentom miast niebędących miastami na prawach powiatu), kierownikom jednostek organizacyjnych utworzonych przez powiat, kierownikom powiatowych służb, inspekcji i straży, kierownikom jednostek ochrony przeciwpożarowej działających na obszarze powiatu oraz kierownikom jednostek organizacyjnych czasowo przekazanych przez właściwe organy do jego dyspozycji i skierowanych do wykonywania zadań na obszarze powiatu.
3. W zakresie działań, o których mowa w ust. 1, starosta może występować do kierowników innych jednostek organizacyjnych niż określone w ust. 2, działających na obszarze powiatu z wnioskami o wykonanie czynności niezbędnych w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia. W razie odmowy wykonania tych czynności lub ich niewłaściwego wykonywania starosta niezwłocznie zawiadamia organ, któremu podlega kierownik lub który sprawuje nadzór nad nim.
4. W zakresie działań, o których mowa w ust. 1, w przypadkach określonych w art. 8 pkt 3 i 4, starosta podlega wojewodzie.

Załącznik 6

USTAWA
z dnia 18 kwietnia 2002 r.
O STANIE KLĘSKI ŻYWIOŁOWEJ
(Dz.U. 2002 Nr 62 poz. 558)

Rozdział 1
PRZEPISY OGÓLNE

Art. 1.

Ustawa określa tryb wprowadzenia i zniesienia stanu klęski żywiołowej, a także zasady działania organów władzy publicznej oraz zakres ograniczeń wolności i praw człowieka i obywatela w czasie stanu klęski żywiołowej.

Art. 2.

Stan klęski żywiołowej może być wprowadzony dla zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej oraz w celu ich usunięcia.

Art. 3.

1. Ilekroć w ustawie jest mowa o:
   1) klęsce żywiołowej - rozumie się przez to katastrofę naturalną lub awarię techniczną, których skutki zagrażają życiu lub zdrowiu dużej liczby osób, mieniu w wielkich rozmiarach albo środowisku na znacznych obszarach, a pomoc i ochrona mogą być skutecznie podjęte tylko przy zastosowaniu nadzwyczajnych środków, we współdziałaniu różnych organów i instytucji oraz specjalistycznych służb i formacji działających pod jednolitym kierownictwem,
   2) katastrofie naturalnej - rozumie się przez to zdarzenie związane z działaniem sił natury, w szczególności wyładowania atmosferyczne, wstrząsy sejsmiczne, silne wiatry, intensywne opady atmosferyczne, długotrwałe występowanie ekstremalnych temperatur, osuwiska ziemi, pożary, susze, powodzie, zjawiska lodowe na rzekach i morzu oraz jeziorach i zbiornikach wodnych, masowe występowanie szkodników, chorób roślin lub zwierząt albo chorób zakaźnych ludzi albo też działanie innego żywiołu,
   3) awarii technicznej - rozumie się przez to gwałtowne, nieprzewidziane uszkodzenie lub zniszczenie obiektu budowlanego, urządzenia technicznego lub systemu urządzeń technicznych powodujące przerwę w ich używaniu lub utratę ich właściwości.

Opracowano na podstawie: Dz.U. z 2002 r. Nr 62, poz. 558, Nr 74, poz. 676.

2. Katastrofą naturalną lub awarią techniczną może być również zdarzenie wywołane działaniem terrorystycznym.

Art. 4.

1. Stan klęski żywiołowej może być wprowadzony na obszarze, na którym wystąpiła klęska żywiołowa, a także na obszarze, na którym wystąpiły lub mogą wystąpić skutki tej klęski.
2. Stan klęski żywiołowej wprowadza się na czas oznaczony, niezbędny dla zapobieżenia skutkom klęski żywiołowej lub ich usunięcia, nie dłuższy niż 30 dni.

Art. 5.

1. Rada Ministrów, w drodze rozporządzenia, może wprowadzić stan klęski żywiołowej z własnej inicjatywy lub na wniosek właściwego wojewody.
2. W rozporządzeniu, o którym mowa w ust. 1, określa się przyczyny, datę wprowadzenia oraz obszar i czas trwania stanu klęski żywiołowej, a także, w zakresie dopuszczonym niniejszą ustawą, rodzaje niezbędnych ograniczeń wolności i praw człowieka i obywatela.
3. Rozporządzenie, o którym mowa w ust. 1, ogłasza się w Dzienniku Ustaw Rzeczypospolitej Polskiej, a ponadto podaje do publicznej wiadomości, w drodze obwieszczenia właściwego wojewody przez rozplakatowanie w miejscach publicznych, a także w sposób zwyczajowo przyjęty na danym obszarze.
4. Redaktorzy naczelni dzienników oraz nadawcy programów radiowych i telewizyjnych są obowiązani do niezwłocznego, nieodpłatnego podania do publicznej wiadomości rozporządzenia Rady Ministrów o wprowadzeniu stanu klęski żywiołowej, przekazanego im przez wojewodę właściwego ze względu na siedzibę redakcji lub nadawcy.

Art. 6.

1. Stan klęski żywiołowej może zostać przedłużony na czas oznaczony, w drodze rozporządzenia Rady Ministrów, po wyrażeniu przez Sejm zgody na to przedłużenie.
2. Rada Ministrów, w drodze rozporządzenia, znosi stan klęski żywiołowej na całym obszarze jego obowiązywania lub na części tego obszaru przed upływem czasu, na który został wprowadzony, jeżeli ustaną przyczyny jego wprowadzenia.
3. Przepisy art. 5 stosuje się odpowiednio do rozporządzeń, o których mowa w ust. 1 i 2.

Art. 14.

Kierowanie działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia na obszarach i w obiektach jednostek organizacyjnych podległych, podporządkowanych lub nadzorowanych przez Ministra Obrony Narodowej, Ministra Sprawiedliwości, ministra właściwego do spraw zagranicznych oraz ministra właściwego do spraw wewnętrznych, Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu wymaga współdziałania:

1) organu, o którym mowa w art. 8 pkt 1-3, z właściwymi kierownikami jednostek organizacyjnych podległych, podporządkowanych lub nadzorowanych przez Ministra Obrony Narodowej, Ministra Sprawiedliwości, ministra właściwego do spraw zagranicznych oraz ministra właściwego do spraw wewnętrznych, Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu,
2) ministra, o którym mowa w art. 8 pkt 4, z właściwym ministrem, Szefem Agencji Bezpieczeństwa Wewnętrznego lub Szefem Agencji Wywiadu.

Art. 15.

1. Wojewodowie albo pełnomocnicy, o których mowa w art. 11 ust. 4, są obowiązani do współdziałania i wzajemnego przekazywania informacji w zakresie zapobiegania skutkom klęski żywiołowej lub ich usuwania.
2. Obowiązek przewidziany w ust. 1 dotyczy odpowiednio wójtów (burmistrzów, prezydentów miast), starostów albo pełnomocników, o których mowa w art. 9 ust. 5 i art. 10 ust. 5.

Art. 16.

Minister, o którym mowa w art. 8 pkt 4, jest obowiązany do informowania na bieżąco Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów o skutkach klęski żywiołowej i działaniach podejmowanych w celu zapobieżenia tym skutkom lub ich usunięcia.

Art. 17.

1. W zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu są obowiązane uczestniczyć: Państwowa Straż Pożarna i inne jednostki ochrony przeciwpożarowej, Policja, Państwowe Ratownictwo Medyczne i jednostki ochrony zdrowia, Straż Graniczna, Morska Służba Poszukiwania i Ratownictwa oraz inne właściwe w tych sprawach państwowe urzędy, agencje, inspekcje, straże i służby.
2. Podmioty, o których mowa w ust. 1, podlegają kierownictwu organów, o których mowa w art. 8, albo pełnomocników, o których mowa w art. 9 ust. 5, art. 10 ust. 5 i art. 11 ust. 4.

Art. 18.

1. W czasie stanu klęski żywiołowej, jeżeli użycie innych sił i środków jest niemożliwe lub niewystarczające, Minister Obrony Narodowej może przekazać do dyspozycji wojewody, na którego obszarze działania występuje klęska żywiołowa, pododdziały lub oddziały sił zbrojnych Rzeczypospolitej Polskiej wraz ze skierowaniem ich do wykonywania zadań związanych z zapobieżeniem skutkom klęski żywiołowej lub ich usunięciem.
2. W przypadku, o którym mowa w ust. 1, pododdziały i oddziały sił zbrojnych Rzeczypospolitej Polskiej pozostają pod dowództwem przełożonych służbowych i wykonują zadania określone przez wojewodę.
3. Rada Ministrów, w drodze rozporządzenia, określi szczegółowe zasady udziału pododdziałów i oddziałów sił zbrojnych Rzeczypospolitej Polskiej w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu, uwzględniając:
   1) rodzaje działań ratowniczych lub prewencyjnych, w których pododdziały i oddziały sił zbrojnych Rzeczypospolitej Polskiej mogą brać udział,
   2) sposób koordynowania i dowodzenia ich działaniami,
   3) sposób zapewnienia im zabezpieczenia logistycznego.

Art. 19.

Kierujący działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia współpracują ze społecznymi organizacjami ratowniczymi, charytatywnymi, stowarzyszeniami, fundacjami oraz innymi podmiotami działającymi na obszarze ich właściwości, a na wniosek lub za zgodą tych podmiotów koordynują ich działalność.

Rozdział 3

ZAKRES OGRANICZEŃ WOLNOŚCI I PRAW CZŁOWIEKA I OBYWATELA

Art. 20.

Ograniczenia wolności i praw człowieka i obywatela w stanie klęski żywiołowej stosuje się do osób fizycznych zamieszkałych lub czasowo przebywających na obszarze, na którym został wprowadzony stan klęski żywiołowej, oraz odpowiednio do osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej, mających siedzibę lub prowadzących działalność na obszarze, na którym został wprowadzony stan klęski żywiołowej, z zastrzeżeniem art. 24 i art. 25.

Art. 21.

1. Ograniczenia, o których mowa w art. 20, mogą polegać na:
   1) zawieszeniu działalności określonych przedsiębiorców,
   2) nakazie lub zakazie prowadzenia działalności gospodarczej określonego rodzaju,

5. W razie niezdolności do kierowania lub niewłaściwego kierowania działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia, wojewoda może zawiesić uprawnienia starosty określone w ust. 2 i 3, oraz wyznaczyć pełnomocnika do kierowania tymi działaniami. Do pełnomocnika stosuje się odpowiednio przepis ust. 4.
6. W przypadku, o którym mowa w art. 8 pkt 3, wójt (burmistrz, prezydent miasta) albo pełnomocnik, o którym mowa w art. 9 ust. 5, oraz starosta albo pełnomocnik, o którym mowa w ust. 5, wykonują czynności kierownicze na właściwym dla siebie obszarze wobec podmiotów, o których mowa odpowiednio w art. 9 ust. 2 oraz w ust. 2.

Art. 11.

1. W czasie stanu klęski żywiołowej właściwy wojewoda kieruje działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia na obszarze województwa.
2. W zakresie działań, o których mowa w ust. 1, wojewodzie są podporządkowane organy i jednostki organizacyjne administracji rządowej i samorządu województwa działające na obszarze województwa oraz inne siły i środki wydzielone do jego dyspozycji i skierowane do wykonywania tych działań na obszarze województwa, w tym pododdziały i oddziały sił zbrojnych Rzeczypospolitej Polskiej.
3. W zakresie działań, o których mowa w ust. 1, w przypadku określonym w art. 8 pkt 4 wojewoda podlega właściwemu ministrowi.
4. W razie niezdolności do kierowania lub niewłaściwego kierowania działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia minister, o którym mowa w art. 8 pkt 4, może zawiesić uprawnienia wojewody, o których mowa w ust. 1 i 2, oraz wyznaczyć pełnomocnika do kierowania tymi działaniami. Do pełnomocnika stosuje się odpowiednio przepis ust. 3.
5. W przypadku, o którym mowa w art. 8 pkt 4, wójt (burmistrz, prezydent miasta) albo pełnomocnik, o którym mowa w art. 9 ust. 5, starosta albo pełnomocnik, o którym mowa w art. 10 ust. 5, oraz wojewoda albo pełnomocnik, o którym mowa w ust. 4, wykonują czynności kierownicze na właściwym dla siebie obszarze wobec podmiotów, o których mowa odpowiednio w art. 9 ust. 2, art. 10 ust. 2 oraz w ust. 2.

Art. 12.

1. Działania w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia wójt (burmistrz, prezydent miasta), starosta i wojewoda albo pełnomocnicy, o których mowa w art. 9 ust. 5, art. 10 ust. 5 i art. 11 ust. 4 oraz ministrowie, o których mowa w art. 8 pkt 4, wykonują przy pomocy odpowiednio gminnego zespołu reagowania, powiatowego zespołu reagowania kryzysowego, wojewódzkiego zespołu reagowania kryzysowego oraz Rządowego Zespołu Koordynacji Kryzysowej, zwanych dalej .zespołami..
2. Do zadań zespołów należy w szczególności:
   1) monitorowanie występujących klęsk żywiołowych i prognozowanie rozwoju sytuacji,
   2) realizowanie procedur i programów reagowania w czasie stanu klęski żywiołowej,
   3) opracowywanie i aktualizowanie planów reagowania kryzysowego,
   4) planowanie wsparcia organów kierujących działaniami na niższym szczeblu administracji publicznej,
   5) przygotowywanie warunków umożliwiających koordynację pomocy humanitarnej,
   6) realizowanie polityki informacyjnej związanej ze stanem klęski żywiołowej.
3. Skład zespołów określają odpowiednio organy, o których mowa w ust. 1.
4. Funkcjonowanie zespołów finansowane jest odpowiednio z budżetów jednostek samorządu terytorialnego, wojewodów oraz ministra właściwego do spraw wewnętrznych.
5. Rada Ministrów, w drodze rozporządzenia, określi sposób tworzenia zespołów i ich funkcjonowania, uwzględniając w szczególności:
   1) usytuowanie i sposób finansowania zespołów,
   2) warunki techniczne i standardy ich wyposażenia,
   3) tryb pracy zespołów,
   4) sposób dokumentowania działań i prac zespołów.

Art. 13.

1. W zakresie działań prowadzonych w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia minister, o którym mowa w art. 8 pkt 4, może wydawać polecenia wiążące organom administracji rządowej, z wyjątkiem Rady Ministrów, Prezesa Rady Ministrów i wiceprezesów Rady Ministrów, a także wydawać polecenia wiążące organom samorządu terytorialnego.
2. W razie odmowy wykonania polecenia, o którym mowa w ust. 1, lub niewłaściwego wykonywania polecenia przez:
   1) organy administracji rządowej - minister, o którym mowa w art. 8 pkt 4, niezwłocznie zawiadamia Prezesa Rady Ministrów,
   2) organy samorządu terytorialnego - minister, o którym mowa w art. 8 pkt 4, może zawiesić odpowiednie uprawnienia takiego organu oraz wyznaczyć pełnomocnika do wykonywania tych uprawnień, zawiadamiając o tym właściwego wojewodę i Prezesa Rady Ministrów.

w ciąży i kobiety karmiące - w zakresie świadczeń wymienionych w ust. 1 pkt 1-3, 6, 8 i 10, 3) osoby sprawujące opiekę nad dziećmi do lat 8, nad chorymi lub osobami niepełnosprawnymi - w zakresie świadczeń wymienionych w ust. 1 pkt 1-3, 6 i 10.

3. W szczególnie uzasadnionych przypadkach wójt (burmistrz, prezydent miasta), starosta, wojewoda albo pełnomocnik może odstąpić od nałożenia lub zwolnić od obowiązków, o których mowa w ust. 1, również inne osoby i podmioty, ze względu na interes publiczny albo wyjątkowo ważny interes danej osoby lub podmiotu.

Art. 23.

1. Niezbędne ograniczenia wolności i praw człowieka i obywatela, o których mowa w art. 21 i art. 22, w granicach dopuszczonych w rozporządzeniu Rady Ministrów o wprowadzeniu stanu klęski żywiołowej wprowadza, odpowiednio w zakresie kompetencji wynikających z art. 8:
   1) wójt (burmistrz, prezydent miasta) albo pełnomocnik, o którym mowa w art. 9 ust. 5 - w drodze zarządzenia albo decyzji,
   2) starosta albo pełnomocnik, o którym mowa w art. 10 ust. 5 - w drodze zarządzenia albo decyzji,
   3) wojewoda albo pełnomocnik, o którym mowa w art. 11 ust. 4 - w drodze rozporządzenia albo decyzji.
2. Rozporządzenia wojewody lub pełnomocnika i zarządzenia, o których mowa w ust. 1 pkt 1 i 2, podlegają ogłoszeniu przez rozplakatowanie obwieszczeń w miejscach publicznych lub w inny sposób miejscowo przyjęty, a także przez ogłoszenie w lokalnej prasie.
3. W rozporządzeniu wojewody lub pełnomocnika, zarządzeniu lub decyzji należy podać:
   1) podstawę prawną,
   2) określenie zakresu i rodzaju ograniczeń,
   3) określenie obowiązanych podmiotów,
   4) miejsce, dzień i godzinę osobistego stawiennictwa lub realizacji innych ograniczeń,
   5) czas trwania ograniczeń,
   6) pouczenie o odpowiedzialności karnej lub innych skutkach prawnych naruszenia rozporządzenia, zarządzenia lub decyzji.
4. Do decyzji, o których mowa w ust. 1, stosuje się przepisy Kodeksu postępowania administracyjnego z zastrzeżeniem, że:
   1) podlegają one natychmiastowemu wykonaniu z chwilą ich doręczenia lub ogłoszenia,
   2) mogą one być w nagłych wypadkach wydawane ustnie, a następnie niezwłocznie potwierdzane na piśmie,
   3) odwołanie od nich wnosi się w terminie 3 dni od dnia doręczenia lub potwierdzenia na piśmie decyzji wydanej ustnie,
   4) wniesione odwołania podlegają przekazaniu organowi odwoławczemu w terminie 3 dni, a rozpatrzeniu – w terminie 7 dni od dnia doręczenia mu odwołania,
   5) organem wyższego stopnia w sprawach decyzji wydanych przez starostę i wójta (burmistrza, prezydenta miasta) jest wojewoda.
5. Wojewoda może uchylić w całości lub w części zarządzenie lub decyzję wójta (burmistrza, prezydenta miasta), starosty albo pełnomocników, o których mowa w art. 9 ust. 5 i art. 10 ust. 5.
6. Minister właściwy do spraw administracji publicznej może uchylić w całości lub w części rozporządzenie lub decyzję wojewody albo pełnomocnika, o którym mowa w art. 11 ust. 4.

Art. 24.

1. W celu usprawnienia przemieszczania się środków transportowych niezbędnych dla prowadzenia działań ratowniczych mogą być wprowadzone ograniczenia w transporcie drogowym, kolejowym i lotniczym oraz w ruchu jednostek pływających na śródlądowych drogach wodnych, morskich wodach wewnętrznych i morzu terytorialnym.
2. Minister właściwy do spraw transportu w zakresie transportu drogowego, kolejowego, lotniczego i ruchu jednostek pływających na śródlądowych drogach wodnych, a minister właściwy do spraw gospodarki morskiej w zakresie ruchu na morskich wodach wewnętrznych i morzu terytorialnym, w porozumieniu z ministrem właściwym do spraw wewnętrznych i Ministrem Obrony Narodowej, w drodze rozporządzenia, może wprowadzić ograniczenia, o których mowa w ust. 1, oraz określić zakres tych ograniczeń z uwzględnieniem konieczności zapewnienia warunków pozwalających na sprawne zapobieganie lub zwalczanie skutków klęski żywiołowej przy jednoczesnym zminimalizowaniu uciążliwości wynikłych dla innych użytkowników z wprowadzonych ograniczeń.

Art. 25.

1. Dla zapewnienia łączności na potrzeby działań ratowniczych mogą być wprowadzone ograniczenia w wykonywaniu pocztowych usług o charakterze powszechnym lub usług kurierskich.
2. Ograniczenia w pracy urządzeń radiowych nadawczych lub nadawczo-odbiorczych oraz w wykonywaniu usług telekomunikacyjnych określają odrębne przepisy.

3) nakazaniu pracodawcy oddelegowania pracowników do dyspozycji organu kierującego działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia,
4) całkowitej lub częściowej reglamentacji zaopatrzenia w określonego rodzaju artykuły,
5) obowiązku poddania się badaniom lekarskim, leczeniu, szczepieniom ochronnym oraz stosowaniu innych środków profilaktycznych i zabiegów, niezbędnych do zwalczania chorób zakaźnych oraz skutków skażeń chemicznych i promieniotwórczych,
6) obowiązku poddania się kwarantannie,
7) obowiązku stosowania środków ochrony roślin lub innych środków zapobiegawczych niezbędnych do zwalczania organizmów szkodliwych dla ludzi, zwierząt lub roślin,
8) obowiązku stosowania określonych środków zapewniających ochronę środowiska,
9) obowiązku stosowania środków lub zabiegów niezbędnych do zwalczania chorób zakaźnych zwierząt,
10) obowiązku opróżnienia lub zabezpieczenia lokali mieszkalnych bądź innych pomieszczeń,
11) dokonaniu przymusowych rozbiórek i wyburzeń budynków lub innych obiektów budowlanych albo ich części,
12) nakazie ewakuacji w ustalonym czasie z określonych miejsc, obszarów i obiektów,
13) nakazie lub zakazie przebywania w określonych miejscach i obiektach oraz na określonych obszarach,
14) zakazie organizowania lub przeprowadzania imprez masowych,
15) nakazie lub zakazie określonego sposobu przemieszczania się,
16) wykorzystaniu, bez zgody właściciela lub innej osoby uprawnionej, nieruchomości i rzeczy ruchomych,
17) zakazie prowadzenia strajku w odniesieniu do określonych kategorii pracowników lub w określonych dziedzinach,
18) ograniczeniu lub odstąpieniu od określonych zasad bezpieczeństwa i higieny pracy, jednakże nie powodującym bezpośredniego narażenia życia lub zdrowia pracownika,
19) wykonywaniu świadczeń osobistych i rzeczowych określonych w art. 22.

2. Ograniczenia, o których mowa w art. 20, w stosunku do osób zatrudnionych u pracodawcy, wobec którego został wydany nakaz prowadzenia działalności gospodarczej, mogą polegać na:
   1) zmianie systemu, wymiaru i rozkładu czasu pracy, w tym wydłużeniu okresu rozliczeniowego do dwunastu miesięcy, na zasadach określonych w Kodeksie pracy, 2) obowiązku pracy w niedziele, święta i dni wolne od pracy wynikające z rozkładu czasu pracy w pięciodniowym tygodniu pracy, w tym wydłużeniu okresu rozliczeniowego do dwunastu miesięcy, na zasadach określonych w Kodeksie pracy,
   2) powierzeniu pracownikowi wykonywania pracy innego rodzaju niż wynikający z nawiązanego stosunku pracy; w takim przypadku pracownik zachowuje prawo do dotychczasowego wynagrodzenia, obliczonego według zasad obowiązujących przy obliczaniu wynagrodzenia za czas urlopu wypoczynkowego.
3. Ograniczenia, o których mowa w ust. 2, nie mogą być stosowane wobec pracowników młodocianych, osób niepełnosprawnych oraz kobiet w ciąży i karmiących.

Art. 22.

1. Jeżeli siły i środki, którymi dysponuje wójt (burmistrz, prezydent miasta), starosta lub wojewoda albo pełnomocnik, są niewystarczające, można wprowadzić obowiązek świadczeń osobistych i rzeczowych polegających na:
   1) udzielaniu pierwszej pomocy osobom, które uległy nieszczęśliwym wypadkom,
   2) czynnym udziale w działaniu ratowniczym lub wykonywaniu innych zadań wyznaczonych przez kierującego akcją ratowniczą,
   3) wykonywaniu określonych prac,
   4) oddaniu do używania posiadanych nieruchomości lub rzeczy ruchomych,
   5) udostępnieniu pomieszczeń osobom ewakuowanym,
   6) użytkowaniu nieruchomości w określony sposób lub w określonym zakresie,
   7) przyjęciu na przechowanie i pilnowaniu mienia osób poszkodowanych lub ewakuowanych,
   8) zabezpieczeniu zagrożonych zwierząt, a w szczególności dostarczaniu paszy i schronienia,
   9) zabezpieczeniu zagrożonych roślin lub nasion,
   10) pełnieniu wart,
   11) zabezpieczeniu własnych źródeł wody pitnej i środków spożywczych przed ich zanieczyszczeniem, skażeniem lub zakażeniem, a także udostępnianiu ich dla potrzeb osób ewakuowanych lub poszkodowanych, w sposób wskazany przez organ nakładający świadczenie,
   12) zabezpieczeniu zagrożonych dóbr kultury.
2. Od obowiązku świadczeń osobistych zwolnione są: 1) osoby do 16 roku życia i powyżej 60 roku życia – w zakresie świadczeń wymienionych w ust. 1 pkt 2, 3, 6 i 10, 2) osoby chore, niepełnosprawne, kobiety

2. Rozpoznawanie spraw, określonych w ust. 1, następuje w trybie przepisów o postępowaniu w sprawach o wykroczenia w postępowaniu przyśpieszonym.

Art. 28.

1. Niewykonane w całości lub w części do dnia zniesienia stanu klęski żywiołowej lub uchylenia odpowiednich ograniczeń wolności i praw człowieka i obywatela kary za wykroczenia wymierzone na podstawie przepisów ustawy podlegają wykonaniu.
2. Postępowania w sprawach o wykroczenia określone w niniejszej ustawie, wszczęte i niezakończone orzeczeniem kończącym postępowanie do dnia zniesienia stanu klęski żywiołowej lub uchylenia odpowiednich ograniczeń wolności i praw człowieka i obywatela, prowadzi się na podstawie przepisów ustawy, a wymierzone kary podlegają wykonaniu.
3. Po zniesieniu stanu klęski żywiołowej postępowanie w sprawach o wykroczenia określone w niniejszej ustawie prowadzi się na zasadach ogólnych.

Rozdział 5

ZMIANY W PRZEPISACH OBOWIĄZUJĄCYCH I PRZEPIS KOŃCOWY

Art. 29.

W ustawie z dnia 8 marca 1990 r. o samorządzie gminnym (Dz.U. z 2001 r. Nr 142, poz. 1591 i z 2002 r. Nr 23, poz. 220) wprowadza się następujące zmiany:

1) w art. 7 w ust. 1 w pkt 14 po wyrazie „przeciwpowodziowej" dodaje się wyrazy „w tym wyposażenia i utrzymania gminnego magazynu przeciwpowodziowego";
2) po art. 31 dodaje się art. 31a i 31b w brzmieniu: .Art. 31a.
   Wójt lub burmistrz opracowuje plan operacyjny ochrony przed powodzią oraz ogłasza i odwołuje pogotowie i alarm przeciwpowodziowy.
   Art. 31b.
   1. Jeżeli w inny sposób nie można usunąć bezpośredniego niebezpieczeństwa dla życia ludzi lub dla mienia, wójt lub burmistrz może zarządzić ewakuację z obszarów bezpośrednio zagrożonych.
   2. W przypadku wprowadzenia stanu klęski żywiołowej wójt lub burmistrz działa na zasadach określonych w odrębnych przepisach...

Art. 30.

W ustawie z dnia 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz.U. Nr 81, poz. 351, z 1994 r. Nr 27, poz. 96 i Nr 89, poz. 414, z 1996 r. Nr 106, poz. 496, z 1997 r. Nr 111, poz. 725 i Nr 121, poz. 770, z 1998 r. Nr 106, poz. 668 i Nr 162, poz. 1126, z 2000 r. Nr 120, poz. 1268 oraz z 2001 r. Nr 113, poz. 1207) wprowadza się następujące zmiany:

1) w art. 2 pkt 3 otrzymuje brzmienie: „3) innym miejscowym zagrożeniu - rozumie się przez to zdarzenie wynikające z rozwoju cywilizacyjnego i naturalnych praw przyrody nie będące pożarem ani klęską żywiołową, stanowiące zagrożenie dla życia, zdrowia, mienia lub środowiska, któremu zapobieżenie lub którego usunięcie skutków nie wymaga zastosowania nadzwyczajnych środków";
2) w art. 14: a) ust. 4 otrzymuje brzmienie: „4. Wojewoda i starosta wykonują swoje zadania przy pomocy odpowiednio wojewódzkiego i powiatowego zespołu reagowania kryzysowego, działających na podstawie przepisów o stanie klęski żywiołowej", b) skreśla się ust. 6-9.

Art. 31.

W ustawie z dnia 5 czerwca 1998 r. o administracji rządowej w województwie (Dz.U. z 2001 r. Nr 80, poz. 872 i Nr 128, poz. 1407 oraz z 2002 r. Nr 37, poz. 329) w art. 15 dodaje się pkt 4a w brzmieniu: .4a) dokonuje oceny stanu zabezpieczenia przeciwpowodziowego województwa, opracowuje plan operacyjny ochrony przed powodzią oraz ogłasza i odwołuje pogotowie i alarm przeciwpowodziowy,..

Art. 32.

W ustawie z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz.U. z 2001 r. Nr 142, poz. 1590 i z 2002 r. Nr 23, poz. 220) w art. 14 w ust. 1 w pkt 9 po wyrazie .przeciwpowodziowej. dodaje się wyrazy „a w szczególności wyposażenia i utrzymania wojewódzkich magazynów przeciwpowodziowych".

Art. 33.

W ustawie z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz.U. z 2001 r. Nr 142, poz. 1592 i z 2002 r. Nr 23, poz. 220) wprowadza się następujące zmiany:

1) w art. 4 w ust. 1 w pkt 16 po wyrazie „przeciwpowodziowej" dodaje się wyrazy „w tym wyposażenia i utrzymania powiatowego magazynu przeciwpowodziowego";
2) w art. 12 pkt 9d otrzymuje brzmienie: „9d) dokonywanie oceny stanu bezpieczeństwa przeciwpożarowego i zabezpieczenia przeciwpowodziowego powiatu";
3) w art. 34 po ust. 1 dodaje się ust. 1a i 1b w brzmieniu: „1a. Starosta opracowuje plan operacyjny ochrony przed powodzią oraz ogłasza i odwołuje pogotowie i alarm przeciwpowodziowy. 1b. W przypadku wprowadzenia stanu klęski żywiołowej starosta działa na zasadach określonych w odrębnych przepisach".

Art. 34.

Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

3. Minister właściwy do spraw łączności może, w drodze rozporządzenia, wprowadzić ograniczenia, o których mowa w ust. 1, oraz określić zakres tych ograniczeń z uwzględnieniem konieczności zapewnienia warunków pozwalających na sprawne zapobieganie lub zwalczanie skutków klęski żywiołowej przy jednoczesnym zminimalizowaniu uciążliwości wynikłych dla osób i podmiotów korzystających z pocztowych usług o charakterze powszechnym lub usług kurierskich.

Art. 26.

Redaktorzy naczelni dzienników oraz nadawcy programów radiowych i telewizyjnych są obowiązani, na żądanie ministra, o którym mowa w art. 8 pkt 4, wojewodów, starostów, wójtów (burmistrzów, prezydentów miast) albo pełnomocników do nieodpłatnego, niezwłocznego publikowania lub zamieszczania komunikatów tych organów związanych z działaniami w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia.

Rozdział 4

PRZEPISY KARNE

Art. 27.

1. Kto w czasie stanu klęski żywiołowej:
   1) wbrew zakazowi określonemu w art. 21 ust. 1 pkt 1 prowadzi działalność gospodarczą,
   2) wbrew zakazowi określonemu w art. 21 ust. 1 pkt 2 prowadzi działalność gospodarczą określonego rodzaju,
   3) wbrew nakazowi określonemu w art. 21 ust. 1 pkt 2 nie podejmuje działalności gospodarczej określonego rodzaju,
   4) wbrew nakazowi określonemu w art. 21 ust. 1 pkt 3 nie oddeleguje pracowników do dyspozycji organu kierującego działaniami prowadzonymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia,
   5) wbrew nakazowi określonemu w art. 21 ust. 1 pkt 4 narusza zasady reglamentacji zaopatrzenia w określonego rodzaju artykuły,
   6) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 5 i 6 nie poddaje się badaniom lekarskim, leczeniu, szczepieniom ochronnym oraz stosowaniu innych środków profilaktycznych i zabiegów niezbędnych do zwalczania chorób zakaźnych oraz skutków skażeń chemicznych i promieniotwórczych, a także nie poddaje się obowiązkowi kwarantanny,
   7) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 7 nie stosuje środków ochrony roślin lub innych środków zapobiegawczych niezbędnych do zwalczania organizmów szkodliwych dla ludzi, zwierząt lub roślin,
   8) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 8 nie stosuje określonych środków zapewniających ochronę środowiska,
   9) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 9 nie stosuje środków lub zabiegów niezbędnych do zwalczania chorób zakaźnych zwierząt,
   10) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 10 nie opróżnia lub nie zabezpiecza lokalu mieszkalnego lub innych pomieszczeń,
   11) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 11 nie dokonuje przymusowych rozbiórek i wyburzeń budynków lub innych obiektów budowlanych albo ich części,
   12) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 12 nie stosuje się do nakazu ewakuacji w ustalonym czasie z określonych miejsc, obszarów lub obiektów,
   13) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 13 nie stosuje się do nakazu albo zakazu przebywania w określonych miejscach i obiektach oraz na określonych obszarach,
   14) wbrew zakazowi określonemu w art. 21 ust. 1 pkt 14 i 17 narusza wprowadzone ograniczenia organizując lub przeprowadzając imprezę masową albo strajk,
   15) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 15 nie stosuje się do nakazu albo zakazu określonego sposobu przemieszczania się,
   16) wbrew obowiązkowi określonemu w art. 21 ust. 1 pkt 19 nie wykonuje świadczeń osobistych lub rzeczowych albo nie wykonuje ich w pełnym zakresie,
   17) wbrew obowiązkowi określonemu w art. 21 ust. 2 nie stosuje się do wprowadzonych ograniczeń w zakresie prawa pracy,
   18) wbrew obowiązkowi określonemu w art. 24 nie stosuje się do wprowadzonych ograniczeń w transporcie drogowym, kolejowym lub lotniczym albo w ruchu jednostek pływających na śródlądowych drogach wodnych, na morskich wodach wewnętrznych lub morzu terytorialnym,
   19) wbrew obowiązkowi określonemu w art. 25 nie stosuje się do wprowadzonych ograniczeń w pracy urządzeń radiowych nadawczych lub nadawczo-odbiorczych, w wykonywaniu usług telekomunikacyjnych, pocztowych usług o charakterze powszechnym lub usług kurierskich,
   20) wbrew obowiązkowi określonemu w art. 26 nie publikuje lub nie zamieszcza komunikatów i decyzji związanych z działaniami podejmowanymi w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia - podlega karze aresztu albo grzywny.

lub miasta na prawach powiatu i obejmować zasięgiem działania obszar obu sąsiadujących jednostek samorządu terytorialnego.

5. Grupami roboczymi powiatowego zespołu o charakterze czasowym są:
   1) grupa operacji i organizacji działań;
   2) grupa zabezpieczenia logistycznego;
   3) grupa opieki zdrowotnej i pomocy socjalno-bytowej.
6. Szefa powiatowego zespołu i jego zastępców wyznacza starosta lub prezydent miasta na prawach powiatu spośród osób zatrudnionych w starostwie powiatowym, powiatowych jednostkach organizacyjnych lub jednostkach organizacyjnych stanowiących aparat pomocniczy kierowników powiatowych służb, inspekcji i straży, posiadających wykształcenie specjalistyczne w zakresie ratownictwa, ochrony przeciwpożarowej, inżynierii bezpieczeństwa cywilnego lub zarządzania kryzysowego, a także absolwentów wyższych szkół wojskowych.
7. Grupy robocze, o których mowa w ust. 2 i 5, tworzy się spośród osób zatrudnionych w starostwie powiatowym, powiatowych jednostkach organizacyjnych lub jednostkach organizacyjnych stanowiących aparat pomocniczy kierowników powiatowych służb, inspekcji i straży.
8. W skład grup roboczych, o których mowa w ust. 5, mogą wchodzić również specjaliści, eksperci, osoby zaufania społecznego, a także przedstawiciele organów władzy publicznej lub społecznych organizacji ratowniczych.

§ 5.

1. Wojewódzki zespół reagowania kryzysowego, zwany dalej „wojewódzkim zespołem", składa się z szefa, zastępców oraz grup roboczych o charakterze stałym i czasowym.
2. Grupami roboczymi wojewódzkiego zespołu o charakterze stałym są:
   1) grupa bezpieczeństwa powszechnego i porządku publicznego;
   2) grupa planowania cywilnego;
   3) grupa monitorowania, prognoz i analiz.
3. Grupy robocze, o których mowa w ust. 2 pkt 2 i 3, stanowią wojewódzkie centrum zarządzania kryzysowego, będące komórką organizacyjną urzędu wojewódzkiego.
4. Grupami roboczymi wojewódzkiego zespołu o charakterze czasowym są:
   1) grupa operacji;
   2) grupa zabezpieczenia logistycznego;
   3) grupa opieki zdrowotnej i pomocy socjalno-bytowej.
5. Szefa wojewódzkiego zespołu i jego zastępców wyznacza wojewoda spośród działających pod zwierzchnictwem wojewody kierowników zespolonych służb, inspekcji i straży bądź ich zastępców oraz innych osób zatrudnionych w jednostkach organizacyjnych służb, inspekcji i straży wojewódzkich, pracowników urzędu wojewódzkiego, posiadających wykształcenie specjalistyczne w zakresie ratownictwa, ochrony przeciwpożarowej, inżynierii bezpieczeństwa cywilnego lub zarządzania kryzysowego, a także absolwentów wojskowych szkół wyższych.
6. Grupę roboczą, o której mowa w ust. 2 pkt 1, tworzy się spośród członków zarządu województwa wyznaczonych przez marszałka województwa na wniosek wojewody, kierowników zespolonych służb, inspekcji i straży wojewódzkich, organów administracji niezespolonej w województwie oraz kierowników komórek organizacyjnych urzędu wojewódzkiego i urzędu marszałkowskiego.
7. Grupy robocze, o których mowa w ust. 2 pkt 2 i 3 oraz ust. 4, tworzy się spośród pracowników urzędu wojewódzkiego, osób zatrudnionych w jednostkach organizacyjnych służb, inspekcji i straży wojewódzkich oraz przedstawicieli samorządu województwa wyznaczonych przez marszałka województwa na wniosek wojewody.
8. W skład grup roboczych, o których mowa w ust. 4, mogą wchodzić również specjaliści, eksperci, osoby zaufania społecznego, a także przedstawiciele organów administracji publicznej lub społecznych organizacji ratowniczych.

§ 6.

1. Rządowy Zespół Koordynacji Kryzysowej, zwany dalej „rządowym zespołem", składa się z szefa, dwóch zastępców: stałego i czasowego oraz grup roboczych o charakterze stałym i czasowym.
2. Grupami roboczymi rządowego zespołu o charakterze stałym są:
   1) międzyresortowa grupa polityki bezpieczeństwa i planowania cywilnego;
   2) grupa bezpieczeństwa powszechnego i porządku publicznego;
   3) grupa monitorowania, prognoz i analiz.
3. Grupa robocza, o której mowa w ust. 2 pkt 3, stanowi Rządowe Centrum Koordynacji Kryzysowej, składające się z komórek organizacyjnych urzędu zapewniającego obsługę ministra właściwego do spraw wewnętrznych właściwych w sprawach związanych z zapobieganiem skutkom klęsk żywiołowych lub ich usuwaniem, uzupełniane na czas trwania stanu nadzwyczajnego o grupy robocze o charakterze czasowym, wymienione w ust. 4.
4. Grupami roboczymi rządowego zespołu o charakterze czasowym są:

Załącznik nr 7

ROZPORZĄDZENIE RADY MINISTRÓW
z dnia 3 grudnia 2002 r.
W SPRAWIE SPOSOBU TWORZENIA GMINNEGO ZESPOŁU REAGOWANIA, POWIATOWEGO I WOJEWÓDZKIEGO ZESPOŁU REAGOWANIA KRYZYSOWEGO ORAZ RZĄDOWEGO ZESPOŁU KOORDYNACJI KRYZYSOWEJ I ICH FUNKCJONOWANIA
(Dz. U. Nr 215 z 17 grudnia 2002 r., poz. 1818)

Na podstawie art. 12 ust. 5 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. Nr 62, poz. 558 i Nr 74, poz. 676) zarządza się, co następuje:

§ 1.

Rozporządzenie określa:
1) sposób tworzenia gminnego zespołu reagowania, powiatowego i wojewódzkiego zespołu reagowania kryzysowego oraz Rządowego Zespołu Koordynacji Kryzysowej;
2) sposób funkcjonowania zespołów;
3) usytuowanie i sposób ich finansowania;
4) warunki techniczne i standardy ich wyposażenia;
5) tryb pracy zespołów;
6) sposób dokumentowania działań i prac zespołów.

§ 2.

Ilekroć w rozporządzeniu jest mowa o:
1) „powiecie" - rozumie się przez to również miasto na prawach powiatu;
2) „wójcie" - rozumie się przez to również burmistrza (prezydenta miasta).

§ 3.

1. Gminny zespół reagowania, zwany dalej „gminnym zespołem", składa się z szefa, zastępcy oraz grup roboczych o charakterze stałym i czasowym.
2. Grupami roboczymi gminnego zespołu o charakterze stałym są:
   1) grupa planowania cywilnego;
   2) grupa monitorowania, prognoz i analiz.
3. Grupy robocze, o których mowa w ust. 2, stanowią gminne centrum reagowania, będące komórką organizacyjną urzędu gminy. Siedziba gminnego centrum reagowania powinna być odpowiednio oznakowana, a jego lokalizacja podana do publicznej wiadomości w sposób umożliwiający poinformowanie wszystkich mieszkańców gminy.
4. Grupami roboczymi gminnego zespołu o charakterze czasowym są:
   1) grupa operacji i organizacji działań;
   2) grupa zabezpieczenia logistycznego;
   3) grupa opieki zdrowotnej i pomocy socjalno-bytowej.
5. Szefa gminnego zespołu i jego zastępców wyznacza wójt spośród zatrudnionych w urzędzie gminy, gminnych jednostkach organizacyjnych lub w jednostkach pomocniczych, osób posiadających wykształcenie specjalistyczne w zakresie ratownictwa, ochrony przeciwpożarowej, inżynierii bezpieczeństwa cywilnego lub zarządzania kryzysowego, absolwentów wyższych szkół wojskowych, a także spośród funkcjonariuszy pożarnictwa, wyznaczonych do wykonywania zadań poza jednostkami organizacyjnymi Państwowej Straży Pożarnej.
6. Grupy robocze, o których mowa w ust. 2 i 4, tworzy się spośród osób zatrudnionych w urzędzie gminy, gminnych jednostkach organizacyjnych lub jednostkach pomocniczych.
7. W skład grup roboczych, o których mowa w ust. 4, mogą wchodzić również specjaliści, eksperci, osoby zaufania społecznego, a także przedstawiciele organów administracji publicznej lub społecznych organizacji ratowniczych.

§ 4.

1. Powiatowy zespół reagowania kryzysowego, zwany dalej "powiatowym zespołem", składa się z szefa, zastępcy oraz grup roboczych o charakterze stałym i czasowym.
2. Grupami roboczymi powiatowego zespołu o charakterze stałym są:
   1) grupa planowania cywilnego;
   2) grupa monitorowania, prognoz i analiz.
3. Grupy robocze, o których mowa w ust. 2, stanowią powiatowe centrum zarządzania kryzysowego, będące komórką organizacyjną starostwa powiatowego lub komendy powiatowej Państwowej Straży Pożarnej. Przepis § 3 ust. 3 zdanie drugie stosuje się odpowiednio.
4. Na podstawie porozumienia między właściwym starostą a prezydentem miasta na prawach powiatu, centrum zarządzania kryzysowego, o którym mowa w ust. 3, może być ulokowane na terenie powiatu

9. Obsługę kancelaryjno-biurową zespołów zapewniają odpowiednio urząd gminy (miasta), starostwo, urząd wojewódzki i urząd obsługujący ministra właściwego do spraw wewnętrznych.

§ 8.

1. Grupy robocze zespołów o charakterze stałym pracują zgodnie z rozkładem czasu pracy obowiązującym w urzędzie, w którym są usytuowane, z zapewnieniem dobowych dyżurów.
2. W czasie obowiązywania stanu klęski żywiołowej zespoły pracują w składzie grup roboczych o charakterze stałym i czasowym, w urzędzie, w którym są usytuowane, w trybie ciągłym, z zapewnieniem zmianowej pracy osób wchodzących w ich skład.

§ 9.

1. Dokumentami działań i prac zespołów są:
   1) roczne plany pracy;
   2) plany reagowania kryzysowego;
   3) plany ćwiczeń;
   4) protokoły posiedzeń grup roboczych o charakterze stałym i czasowym;
   5) raporty bieżące i okresowe;
   6) karty zdarzeń, w przypadku uruchomienia grup roboczych o charakterze czasowym;
   7) raporty odbudowy;
   8) inne niezbędne dokumenty.
2. Plan reagowania kryzysowego określa zespół przedsięwzięć na wypadek zagrożeń noszących znamiona klęski żywiołowej, a w szczególności:
   1) zadania w zakresie monitorowania zagrożeń;
   2) bilans sił ratowniczych i środków technicznych niezbędnych do usuwania skutków zagrożeń;
   3) procedury uruchamiania działań przewidzianych w planie oraz zasady współdziałania, a także sposoby ograniczania rozmiaru strat i usuwania skutków zagrożeń;
3. Plan reagowania kryzysowego jest uzgadniany z kierownikami jednostek organizacyjnych planowanych do użycia w realizacji przedsięwzięć określonych w planie w zakresie dotyczącym tych jednostek, a następnie zatwierdzany przez organ administracji publicznej wyższego stopnia.
4. Karta zdarzeń zawiera chronologiczny opis zdarzeń i wdrożonych działań oraz decyzji podejmowanych w celu likwidacji zagrożeń, pomocy poszkodowanym i ograniczeniu strat, a w szczególności informacje o:
   1) kolejności alarmowania sił ratowniczych;
   2) podmiocie kierującym działaniami ratowniczymi;
   3) podejmowanych decyzjach, w tym o zadaniach stawianych poszczególnym formacjom ratowniczym i podmiotom ujętym w planie reagowania kryzysowego;
   4) liczbie poszkodowanych i wielkości strat;
   5) sposobie udzielania pomocy i zabezpieczania terenu zdarzenia.
5. Raport odbudowy zawierający opis i analizę skutków zaistniałego zdarzenia oraz propozycje działań mających na celu odbudowę, a w szczególności:
   1) szczegółowy wykaz strat w infrastrukturze oraz w potencjale ratowniczym,
   2) projekt harmonogramu likwidacji strat i odbudowy,
   3) wstępny bilans potrzeb finansowych w zakresie odbudowy - jest przedstawiany właściwemu organowi, kierującemu działaniami w czasie stanu klęski żywiołowej.

§ 10.

1. W celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia zespoły pracują w fazach zapobiegania, przygotowania, reagowania i odbudowy.
2. W fazie zapobiegania zespoły podejmują działania, które redukują lub eliminują prawdopodobieństwo wystąpienia klęski żywiołowej albo w znacznym stopniu ograniczają jej skutki.
3. W fazie przygotowania zespoły podejmują działania planistyczne dotyczące sposobów reagowania na czas wystąpienia klęski żywiołowej, a także działania mające na celu powiększenie zasobów sił i środków niezbędnych do efektywnego reagowania.
4. W fazie reagowania zespoły podejmują działania polegające na dostarczeniu pomocy poszkodowanym, zahamowaniu rozwoju występujących zagrożeń oraz ograniczeniu strat i zniszczeń.
5. W fazie odbudowy zespoły podejmują działania mające na celu przywrócenie zdolności reagowania, odbudowę zapasów służb ratowniczych oraz odtworzenie kluczowej dla funkcjonowania państwa infrastruktury telekomunikacyjnej, energetycznej, paliwowej, transportowej i dostarczania wody.
6. Działania określone w ust. 2 i 3 są realizowane przez grupy robocze o charakterze stałym.
7. Działania określone w ust. 4 i 5 są realizowane przez zespoły w pełnym składzie.
8. Odpowiednio wójt, starosta, wojewoda i minister właściwy do spraw wewnętrznych zarządza co najmniej raz w roku ćwiczenia realizowane przez zespół w pełnym składzie, określając ich cel, główne

1) grupa planowania wsparcia i analizy zasobów;
2) grupa koordynacji działań kryzysowych;
3) grupa koordynacji pomocy humanitarnej;
4) grupa polityki informacyjnej.

5. Szefa rządowego zespołu wyznacza minister właściwy do spraw wewnętrznych spośród sekretarzy i podsekretarzy stanu w urzędzie obsługującym tego ministra.
6. Stałego zastępcę szefa rządowego zespołu wyznacza minister właściwy do spraw wewnętrznych spośród podporządkowanych mu centralnych organów administracji rządowej, wykonujących zadania w dziedzinie zapobiegania klęskom żywiołowym i usuwania ich skutków.
7. W skład grupy roboczej, o której mowa w ust. 2 pkt 1, wchodzą osoby powołane przez ministra właściwego do spraw wewnętrznych na wniosek Ministra Obrony Narodowej oraz ministrów właściwych do spraw: zagranicznych, administracji publicznej, zdrowia, zabezpieczenia społecznego, środowiska, kultury i ochrony dziedzictwa narodowego, oświaty i wychowania, gospodarki wodnej, finansów publicznych, Skarbu Państwa, rolnictwa, gospodarki, gospodarki morskiej, łączności oraz transportu, spośród sekretarzy i podsekretarzy stanu w urzędach obsługujących tych ministrów.
8. W skład grupy roboczej, o której mowa w ust. 2 pkt 2, wchodzą osoby powołane przez ministra właściwego do spraw wewnętrznych na wniosek Szefa Kancelarii Prezesa Rady Ministrów, Szefa Wojskowych Służb Informacyjnych, Szefa Agencji Bezpieczeństwa Wewnętrznego, Prezesa Państwowej Agencji Atomistyki, Głównego Inspektora Sanitarnego, Głównego Inspektora Nadzoru Budowlanego, Generalnego Dyrektora Dróg Krajowych i Autostrad, Głównego Dyrektora Transportu Drogowego, Prezesa Urzędu Regulacji Telekomunikacji i Poczty, Głównego Lekarza Weterynarii, Głównego Geodetę Kraju, Głównego Inspektora Ochrony Środowiska, Głównego Inspektora Ochrony Roślin i Nasiennictwa oraz osoby wyznaczone przez ministra właściwego do spraw wewnętrznych, spośród osób zatrudnionych w urzędzie obsługującym tego ministra, w jednostkach organizacyjnych przez niego nadzorowanych oraz w urzędach obsługujących organy podległe temu ministrowi.
9. W skład grupy roboczej, o której mowa w ust. 2 pkt 3, wchodzą osoby powołane przez ministra właściwego do spraw wewnętrznych spośród osób zatrudnionych lub pełniących służbę w urzędzie obsługującym ministra właściwego do spraw wewnętrznych.
10. Skład grup roboczych może być uzupełniony o osoby wyznaczone przez innych ministrów na wniosek ministra właściwego do spraw wewnętrznych, a także innych specjalistów, ekspertów lub osoby zaufania społecznego.
11. Czasowego zastępcę szefa rządowego zespołu oraz skład grup roboczych, o których mowa w ust. 4, wyznacza minister, o którym mowa w art. 8 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej, spośród osób zatrudnionych w urzędzie obsługującym tego ministra, w jednostkach organizacyjnych przez niego nadzorowanych oraz w urzędach obsługujących organy podległe temu ministrowi.

§ 7.

1. Gminne, powiatowe, wojewódzkie i rządowy zespoły, zwane dalej „zespołami", działają na podstawie planów pracy zatwierdzonych odpowiednio przez wójta, starostę, wojewodę i ministra właściwego do spraw wewnętrznych.
2. Pracami zespołów kierują ich szefowie.
3. Do zadań szefów zespołów należy w szczególności:
   1) przygotowanie rocznego planu pracy zespołu;
   2) opracowanie regulaminu bieżących prac zespołu oraz działań w sytuacjach zagrożeń katastrofą naturalną lub awarią techniczną noszącą znamiona klęski żywiołowej;
   3) ustalanie przedmiotu i terminu posiedzeń;
   4) zawiadamianie o terminach posiedzeń;
   5) przewodniczenie posiedzeniom;
   6) zapraszanie na posiedzenia osób niebędących członkami zespołu;
   7) inicjowanie i organizowanie prac zespołu.
4. Posiedzenia zespołu zwołuje jego szef na polecenie odpowiednio wójta, starosty, wojewody i ministra właściwego do spraw wewnętrznych, jednak nie rzadziej niż raz na kwartał, a także w zależności od potrzeb.
5. W przypadkach wymagających natychmiastowej analizy i oceny zagrożeń oraz koordynacji działań ratowniczych, szef może zarządzić posiedzenie zespołu w trybie natychmiastowym.
6. Posiedzeniami zespołu kieruje szef, a w razie jego nieobecności - zastępca szefa.
7. W przypadku zaistnienia okoliczności uniemożliwiających szefowi zespołu sprawowanie jego funkcji, powierza on kierowanie pracami zespołu zastępcy.
8. W przypadku zaistnienia okoliczności uniemożliwiających sprawowanie obowiązków przez zastępcę, szef może wyznaczyć spośród członków zespołu osobę pełniącą obowiązki zastępcy.

3. Zadania inwestycyjne, niezbędne do utworzenia i funkcjonowania zespołów, o których mowa w ust. 1, oraz zapewnienia ich gotowości do wykonywania zadań w stanach nadzwyczajnych, są finansowane z dotacji celowych z budżetu państwa na finansowanie lub dofinansowanie kosztów inwestycji realizowanych przez jednostki samorządu terytorialnego oraz ze środków programów wieloletnich.

§ 17.

1. Finansowanie zespołów wojewódzkiego i rządowego planuje się w ramach odpowiednich części budżetu państwa.
2. Zadania inwestycyjne, niezbędne do utworzenia i funkcjonowania zespołów, o których mowa w ust. 1, oraz zapewnienia ich gotowości do wykonywania zadań w stanach nadzwyczajnych, są finansowane ze środków przeznaczonych w budżecie państwa na inwestycje państwowych jednostek budżetowych oraz ze środków programów wieloletnich.

§ 18.

Warunki techniczne i standardy wyposażenia gminnych zespołów, określone w § 1-15, powinny zostać zapewnione w terminie 3 lat od dnia wejścia w życie rozporządzenia.

§ 19.

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia (czyli 1 stycznia 2003 r.).

zadania i przebieg. Po przeprowadzonych ćwiczeniach szef zespołu przedstawia odpowiednio wójtowi, staroście, wojewodzie i ministrowi właściwemu do spraw wewnętrznych raport z ćwiczeń.

9. Minister właściwy do spraw wewnętrznych zarządza, co najmniej raz na cztery lata, ogólnokrajowe ćwiczenia zespołów, określając zakres, cel, główne zadania i przebieg tych ćwiczeń.

§ 11.

Warunki techniczne i standardy wyposażenia gminnego, powiatowego, wojewódzkiego i rządowego zespołu, a w szczególności infrastruktura techniczna i wyposażenie, powinny umożliwić efektywne wypełnianie zadań zespołów, z zachowaniem ciągłości ich działania i wymiany informacji podczas pracy oraz możliwości pracy w przypadku braku zasilania zewnętrznego, wystąpienia awarii lub uszkodzenia systemów łączności.

§ 12.

1. Warunki techniczne do pracy zespołów, o których mowa w § 11, zapewniają pomieszczenia:
   1) służby dyżurnej;
   2) operacyjne do pracy i ćwiczeń zespołów;
   3) zaplecza socjalnego, sanitarnego i technicznego.
2. Pomieszczenia i ich wyposażenie powinny zapewniać bezpieczne i higieniczne warunki pracy dyspozytorów w zakresie oświetlenia, wymiany powietrza, zabezpieczenia przed wilgocią, niekorzystnymi warunkami cieplnymi, nasłonecznieniem oraz przed drganiami, hałasem i innymi czynnikami szkodliwymi lub uciążliwymi dla zdrowia, o których mowa w przepisach z zakresu bezpieczeństwa i higieny pracy.

§ 13.

1. Standardowe wyposażenie zespołów zlokalizowane w pomieszczeniach, o których mowa w § 12 ust. 1 pkt 1 i 2, stanowią:
   1) stanowisko dyspozytorskie oraz stanowiska pomocnicze dla służb dyżurnych w liczbie niezbędnej do realizacji zadań;
   2) stanowiska pracy odpowiednio dla wójta, starosty, wojewody i właściwego ministra.
2. Stanowisko dyspozytorskie i stanowiska pomocnicze, o których mowa w ust. 1 pkt 1, są wyposażane standardowo w:
   1) urządzenia łączności przewodowej i bezprzewodowej z podmiotami uwzględnionymi w planie reagowania kryzysowego zapewniające ich alarmowanie, dysponowanie i współdziałanie, a także zapewniające przekazywanie informacji kierującym działaniami w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia;
   2) system teleinformatyczny kompatybilny z systemami funkcjonującymi w każdym z pozostałych zespołów;
   3) specjalistyczne oprzyrządowanie i oprogramowanie systemu, zapewniające możliwości multimedialnej prezentacji danych;
   4) mapy operacyjne standardowe i cyfrowe oraz specjalistyczne oprogramowanie prognostyczno-planistyczne, a także dokumentację i procedury odpowiednio dla gminy, powiatu, województwa i kraju;
   5) awaryjne plany ewakuacji oraz funkcjonowania właściwego zespołu w miejscach zastępczych;
   6) system uruchamiania ostrzegania i alarmowania ludności;
   7) system rejestracji treści rozmów radiowych i telefonicznych oraz ich archiwizacji;
   8) awaryjne zasilanie urządzeń końcowych.

§ 14.

1. Na wypadek niemożności użytkowania powiatowych i wojewódzkich centrów zarządzania kryzysowego oraz Rządowego Centrum Koordynacji Kryzysowej, dla prac zespołów, o których mowa w § 4 ust. 1, § 5 ust. 1 i § 6 ust. 1, zapewnia się pomieszczenia zastępcze.
2. Na wypadek niemożności użytkowania powiatowych i wojewódzkich centrów zarządzania kryzysowego, dla prac zespołów, o których mowa w § 4 ust. 1 i § 5 ust. 1, zapewnia się ponadto awaryjne ruchome centra kierowania.

§ 15.

1. Standard wyposażenia miejsc zastępczych dla prac właściwych zespołów, o których mowa w § 14 ust. 1, odpowiada wymaganiom określonym w § 13.
2. Standard wyposażenia awaryjnych ruchomych centrów kierowania, o których mowa w § 14 ust. 2, odpowiada wymaganiom określonym w § 13 ust. 2 pkt 1-4 i 6-8.

§ 16.

1. Finansowanie zespołów gminnego i powiatowego planuje się w ramach budżetów odpowiednio gmin i powiatów.
2. Bieżące prace zespołów, o których mowa w ust. 1, mogą być finansowane także z dotacji celowych z budżetu państwa na dofinansowanie zadań własnych gmin i powiatów, określonych w ustawie z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej.

Stan obecny:
W związku z koniecznością rozwoju społeczeństwa informacyjnego w Polsce:

- 17.05.1999 r. powołany został, zarządzeniem Prezesa Rady Ministrów, **Międzyresortowy Zespół ds. handlu metodami elektronicznymi** (Zespół wykonał analizę obowiązującego stanu prawnego pod kątem możliwości wykorzystania istniejących regulacji prawnych w transakcjach zawieranych metodami elektronicznymi i wyznaczył kierunki niezbędnych prac legislacyjnych w tym obszarze w dokumencie z „*Program prac legislacyjnych Rządu w zakresie handlu metodami elektronicznymi na lata 2000-2002*", przyjętym przez Radę Ministrów 11.07.2000 r.) - Zespól zakończył pracę 30.06.2000 r. natomiast 30.11.2000 r. Prezes RM powołał zarządzeniem nr 89, w celu kontynuacji prowadzonych działań, **Międzyresortowy Zespół do spraw gospodarki elektronicznej**,
- Ministerstwo Gospodarki przygotowało program „*Zwiększanie innowacyjności gospodarki w Polsce do 2006 roku*" (zatwierdzony w lipcu 2000 r. przez Radę Ministrów), który ma na celu promowanie rozwoju technik informacyjnych, jako jednego z istotnych elementów wpływających na innowacyjność i konkurencyjność gospodarki,
- 28.11.2000 r. Rada Ministrów przyjęła dokument „*Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce*" (zawiera on priorytety dotyczące powszechnego dostępu do informacji, edukacji informatycznej, zmian struktury zatrudnienia, walki z przestępczością informatyczną, gospodarki elektronicznej, informatyzacji zamówień publicznych, administracji, rozwoju rynku teleinformatycznego, zastosowania informatyki w dziedzinie nauki i kultury oraz działania konieczne dla ich osiągnięcia),
- zgodnie z ustaleniami z posiedzenia Rady Ministrów z 28.11.2000 r. oraz z zapisami dokumentu „*ePolska –plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*", Minister Nauki – przewodniczący Komitetu Badań naukowych monitoruje realizację zadań związanych z rozwojem społeczeństwa informacyjnego w Polsce i przedkłada Radzie Ministrów co kwartał raporty w tym zakresie. Wszystkie raporty publikowane są również w Internecie,
- 28.03.2001 r. z powołany został decyzją KIE zespół ds. projektu eEurope+, którego prace koordynuje Minister Nauki, Przewodniczący KBN,
- 23.01.2001 r. Minister Nauki – Przewodniczący Komitetu Badań Naukowych powołał **Forum ds. Społeczeństwa Informacyjnego** - zespół przedstawicieli ministerstw, urzędów centralnych, organizacji pozarządowych oraz samorządowych działających w dziedzinie społeczeństwa informacyjnego, którego zadaniem tego zespołu jest inicjowanie nowych zadań w zakresie społeczeństwa informacyjnego,
- 11.09.2001r. Rada Ministrów przyjęła strategię rozwoju społeczeństwa informacyjnego „*ePolska - Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*". Dokument ten, przygotowany przez byłe Ministerstwo Łączności (obecnie Ministerstwo Infrastruktury) na wzór podjętej przez UE inicjatywy *e*Europe – przedstawia analizę potrzeb w sferze dostępu do informacji, jej zakresu, środków jej przekazywania i udostępniania. Corocznie weryfikowany i aktualizowany plan działań *ePolska* , jest dokumentem o znaczeniu strategicznym,
- Ministerstwo Spraw Wewnętrznych i Administracji prowadzi prace nad zbiorczym planem informatyzacji administracji w Polsce *„Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce – informatyzacja administracji",*
- 21.12.2001 Sejm RP przyjął ustawę o zmianie ustawy o organizacji i trybie pracy Rady Ministrów oraz o zakresie działania poszczególnych ministrów, ustawy o działach administracji rządowej oraz o zmianie niektórych ustaw, na mocy której utworzony został dział administracji rządowej pod nawą 'informatyzacja', obejmujący m.in. sprawy społeczeństwa informacyjnego w Polsce. Odnośne przepisy wejdą w życie z dniem 01.07.2002 r.

Stan docelowy:

- przygotowanie oraz wdrożenie zgodnych z prawem wspólnotowym WE regulacji dotyczących dokumentu i handlu elektronicznego (m.in. Ustawa o świadczeniu usług drogą elektroniczną – przewidywany termin rozpatrzenia przez Radę Ministrów – 16 kwietnia 2002 r., Ustawa o elektronicznych instrumentach płatniczych),
- wdrożenie ustawy z dnia 28 kwietnia 2000 r. o systemie oceny zgodności i akredytacji oraz zmianie niektórych innych ustaw, związane z działaniem jednostki akredytującej w związku z wymogami ustawy o podpisie elektronicznym, w Ministerstwie Gospodarki,
- opracowanie zbiorczego planu rozwoju teleinformatyki i jej zastosowań w administracji rządowej,
- rozwój infrastruktury niezbędnej do wdrażania założeń programów wspierania społeczeństwa informacyjnego;
- działania na rzecz edukacji informatycznej i walki z tzw. informacyjnym wykluczeniem;
- promowanie innowacyjnych zastosowań technik informacyjnych;
- zwiększenie powszechnego dostępu do Internetu,

Załącznik nr 8

DZIAŁANIA NIEZBĘDNE ZWIĄZANE Z ROZWOJEM SPOŁECZEŃSTWA INFORMACYJNEGO W POLSCE

Wyciąg z raportu w sprawie dostosowań instytucjonalnych w Polsce do wymogów członkostwa w Unii Europejskiej. przyjęty przez Komitet Integracji Europejskiej 10 kwietnia 2002 r.

ROZWÓJ SPOŁECZEŃSTWA INFORMACYJNEGO W POLSCE

Podstawa prawna oraz dokumenty programowe dotyczące rozwoju społeczeństwa informacyjnego:

Ustawa z dnia 12 stycznia 1991 r. o Komitecie Badań Naukowych, uchwała Sejmu RP z 14 lipca 2000r. w sprawie budowania podstaw społeczeństwa informacyjnego w Polsce, stanowisko Rady Ministrów z dnia 28 listopada 2000 r. w sprawie ww. uchwały Sejmu RP, „*Cele i kierunki rozwoju społeczeństwa informacyjnego w Polsce"* (dokument przyjęty przez Rade Ministrów 28 listopada 2000 r., opracowany przez Komitet Badań Naukowych i Ministerstwo Łączności), program „*eEurope+2003 - a Co-operative Effort to Implement the Information Society in Europe*" (ogłoszony podczas szczytu UE w Goeteborgu 16.06.2001 r. plan działań sporządzony przez kraje kandydujące przy wsparciu Komisji Europejskiej), „*ePolska –Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006" (*rządowa strategia rozwoju społeczeństwa informacyjnego, która została przyjęta przez Radę Ministrów 11 września 2001r., przygotowana przez byłe Ministerstwo Łączności - od października 2001 r. przez Ministerstwo Infrastruktury).

Instytucjami realizującymi w tym przypadku są: Ministerstwo Infrastruktury (program „*ePolska – Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006"*), Komitet Badań Naukowych (zespół ds. *e*Europe+, monitorowanie realizacji zadań w zakresie rozwoju społeczeństwa informacyjnego w Polsce, współpraca z programem eContent, zadania realizowane w ramach 5 Programu Ramowego oraz prace nad 6 Programem Ramowym), Ministerstwo Gospodarki (handel elektroniczny oraz realizacja P*rogramu prac legislacyjnych Rządu w zakresie handlu metodami elektronicznymi na lata 2000-2002*), Ministerstwo Spraw Wewnętrznych i Administracji (informatyzacja administracji, w tym współpraca z programem IDA II) oraz: Ministerstwo Kultury, Ministerstwo Edukacji Narodowej i Sportu, Ministerstwo Finansów, Główny Urząd Statystyczny, Urząd Regulacji Telekomunikacji, Ministerstwo Sprawiedliwości, Urząd Komitetu Integracji Europejskiej.

Podczas szczytu na Korfu (24-25.06.1994 r.) szefowie państw i rządów Unii Europejskiej przyjęli dokument pt. *Europa a globalne społeczeństwo informacyjne – zalecenia dla Rady Europejskiej*. W listopadzie 1999 r. w Helsinkach odbyła się konferencja nt. rozwoju społeczeństwa informacyjnego i jego znaczenia dla państw członkowskich UE. Zgodnie z przyjęta na tym forum deklaracją Komisji Europejskiej, w grudniu 1999 r. stworzony został program „*e-Europe – an Information Society for A*ll" a w 2000r. - „*e-Europe 2002. Information Society for All"*. Na konferencji ministerialnej w Warszawie w dniach 11-12 maja 2000 r. „*Społeczeństwo informacyjne – przyspieszanie integracji europej*skiej", państwa Europy Środkowej i Wschodniej zobowiązały się do przygotowania, we współpracy z UE, Planu działania pod nazwą *e*Europe+, który byłby odpowiednikiem *e*Europe dla państw kandydujących. *e*Europe+ został przyjęty przez stronę wspólnotową na szczycie w Goeteborgu 15-16 czerwca 2001r.

Polska jest stale reprezentowana we Wspólnym Komitecie Wysokiego Szczebla do spraw społeczeństwa informacyjnego przez Przewodniczącego KBN oraz Ministra Infrastruktury. Ponadto na mocy postanowień KIE z 28 marca 2001r. stworzony został Zespołu ds. eEuropy+, którego zadaniem jest m.in. opracowywanie stanowisk Polski na spotkania Wspólnego Komitetu Wysokiego Szczebla (pod przewodnictwem Ministra Nauki , w skład którego weszli przedstawiciele Ministerstwa Łączności – obecnie Ministerstwa Infrastruktury, Ministerstwa Gospodarki, Głównego Urzędu Statystycznego, Ministerstwa Spraw Wewnętrznych i Administracji, Ministerstwa Finansów, Urzędu Komitetu Integracji Europejskiej, Ministerstwa Zdrowia oraz Ministerstwa Rolnictwa i Rozwoju Wsi).

Od 2000 r. Polska jest pełnoprawnym uczestnikiem Piątego Programu Ramowego Badań, Rozwoju Technicznego i Prezentacji WE. Polscy eksperci biorą udział w pracach Wspólnoty Europejskiej nad Szóstym Programem Ramowym, który ma wejść w życie w 2002 r. Polskie instytucje aktywnie uczestniczą m.in. w Information Society Technologies – podprogramie poświęconym rozwojowi technik informacyjnych i ich zastosowaniom, zaś przedstawiciele Polski biorą również udział w pracach IST Committee oraz jego grupach roboczych (ds. edukacji, zdrowia, transportu oraz bezpieczeństwa i zaufania).

oraz będzie miało istotne znaczenie dla urealnienia jawności życia publicznego oraz funkcjonowania w obrębie wspólnego rynku w momencie akcesji); 2) wzmożenie produkcji treści informacyjnych osadzonych w wielojęzycznym oraz wielokulturowym otoczeniu; 3) zwiększenie dynamiki rynku produkcji treści w postaci cyfrowej;
- Uczestnictwo strony polskiej w spotkaniach komitetu sterującego programu *e*Content,
- Stworzony został instytucjonalny koordynator projektu (zgodnie z oczekiwaniami Komisji Europejskiej), którego jednym z zadań jest rozpowszechnianie dorobku programu *e*Content (punkt działa przy Akademii Górniczo –Hutniczej w Krakowie).

b) w programie IDA II (*Interchange of Data between Administrations)* zawierającego identyfikację wspólnych projektów dotyczących sieci transeuropejskich służących elektronicznej wymianie danych pomiędzy administracjami,
c) *eGovernment*- skierowanym do sektora publicznego (ma on na celu ułatwienie dostępu obywateli do instytucji), *eHealth* (wdrożenie osiągnięć technologii informacyjnych do ochrony zdrowia, ułatwienie pacjentom dostępu do usług medycznych, tworzenie elektronicznych kart pacjenta etc.),
d) uczestnictwo w tworzeniu *European Environment Information and Observation Network* (EIONET) oraz wdrażanie inteligentnych usług transportowych;

Program ePolska 2001-2006 obejmuje działania związane z:

a) rozwojem infrastruktury teleinformatycznej,
b) stworzeniem powszechnego dostępu do tańszego, szybszego i bezpiecznego Internetu (szybki Internet dla naukowców, bezpieczeństwo sieci, wolne oprogramowanie),
c) inwestowaniem w ludzi i umiejętności (edukacja w erze cyfrowej, praca zawodowa w społeczeństwie informacyjnym, powszechny udział w gospodarce opartej na wiedzy, polskie zasoby kultury w sieciach globalnych),
d) stymulowaniem lepszego wykorzystania technologii informacyjnych (gospodarka elektroniczna, sądownictwo i prokuratura w sieci, administracja publiczna on-line, teleinformatyka w policji, ochrona zdrowia on-line, integracja społeczna on-line, inteligentne systemy wspomagania transportu),
e) wprowadzaniem teleinformatyki na obszary wiejskie,
f) rozwojem radiofonii i telewizji cyfrowej.

Telekomunikacja i technologie informacyjne

(Wyciąg)

Komisja Europejska w Raporcie Okresowym'2001 stwierdziła, iż w zakresie dostosowań sektora telekomunikacyjnego dokonał się jedynie umiarkowany postęp w ciągu ostatnich 2 lat. Powstał wprawdzie urząd regulacyjny ds. telekomunikacji, jednak kwestie wdrożeniowe nadal nie są rozwiązane. W kwestii usług pocztowych, rynek zdominowany jest nadal przez Pocztę Polską, która posiada monopol na krajowy obrót, sortowanie, transport i dostawę przesyłek listowych o wadze do 2000 g oraz paczek, jak również na realizację pocztowych przekazów pieniężnych. Odnotowano również niewielki postęp w sferze legislacji - projekt ustawy

Prawo pocztowe nie został przyjęty przez Sejm zeszłej kadencji, pomimo tego, że od lutego 2000 r. trwały nad nim dyskusje. Konieczne jest zmieszczenie się w harmonogramie czasowym dostosowania prawa do dorobku wspólnotowego, co wymagać będzie znacznych wysiłków. Nie został jeszcze ustanowiony niezależny Urząd ds. Regulacji Rynku Pocztowego.

W sektorze telefonii stacjonarnej w dalszym ciągu widać spuściznę po latach względnego niedorozwoju, zwłaszcza na terenach wiejskich – uniwersalny charakter usług wciąż stanowi tam poważne wyzwanie.

Obecnie należy znowelizować ustawę Prawo telekomunikacyjne oraz przyjąć wszystkie akty wykonawcze do tej ustawy, w celu zapewnienia pełnej zgodności z dorobkiem wspólnotowym, zwłaszcza w zakresie zorientowania na oszczędności kosztów, wzajemne połączenia lokalne, dostępność finansowa, uniwersalny charakter i możliwość wyboru operatora oraz możliwość przenoszenia numeru. W dużej mierze sukces reformy sektora telekomunikacyjnego zależeć będzie od dalszego doskonalenia przez URT poprawy swoich zdolności nadzoru i regulacji sektora w sposób wydajny i niezależny.

Stan docelowy:

Kompetencje (z zaznaczeniem czy w pełni realizują wymagania *acquis, jeśli* nie - odnotować).
Obecnie istniejące kompetencje URT w zakresie usług powszechnych zostały przejęte 1 kwietnia 2002 r. przez Urząd Regulacji Telekomunikacji i Poczty i poszerzone o zagadnienia związane usługami pocztowymi.
W sektorze **pocztowym**:

- przyjęcie ustawy Prawo pocztowe, uwzględniającej wspólnotową definicję usług powszechnych oraz wymogi dotyczące ich jakości oraz sposobu świadczenia przez operatora publicznego,
- umożliwienie wszystkim potencjalnym użytkownikom możliwości korzystania z pocztowych usług powszechnych ,
- kontynuacja procesu restrukturyzacji i prywatyzacji PPUP Poczty Polskiej S.A.,

- liberalizacja rynku telekomunikacyjnego, w tym uwolnienie pętli abonenckich,

Zgodnie z dokumentem „*ePolska - Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006*" ma nastąpić przygotowanie społeczeństwa polskiego do szybkich przemian technologicznych, społecznych i gospodarczych związanych z tworzeniem się społeczeństwa informacyjnego, poprzez:

- dostosowanie regulacji prawnych do wymagań szybkiego postępu technologicznego i ery społeczeństwa informacyjnego,
- przygotowanie społeczeństwa polskiego do wyzwań nowego rynku pracy i nowych metod pracy,
- dostosowanie gospodarki narodowej do wymagań globalnej gospodarki,
- stworzenie przejrzystych i przyjaznych obywatelowi struktur administracji publicznej na miarę otwartego społeczeństwa informacyjnego za pomocą narzędzi wykorzystujących technologie informacyjne i komunikacyjne,
- stworzenie warunków dla trwałego i zrównoważonego rozwoju regionalnego z uwzględnieniem nowoczesnych technik społeczeństwa informacyjnego,
- wzrost innowacyjności gospodarki w celu poprawy jej konkurencyjności,
- zapewnienie wsparcia dla gospodarki elektronicznej przez zaplecze naukowe w celu lepszego wykorzystania szans, jakie oferuje model społeczeństwa informacyjnego,
- szeroką promocję kultury polskiej,
- podjęcie działań tworzących warunki do angażowania się samorządów w zwiększaniu liczby punktów dostępu do sieci, oraz Wspieranie inicjatyw rozwoju i budowy sieci amatorskich i prywatnych oraz stworzenie, przyjęcie i skuteczne egzekwowanie przepisów uniemożliwiających blokowanie budowy sieci,
- realizuje program „*PIONIER: Polski Internet Optyczny – Zaawansowane Aplikacje, Usługi i Technologie dla Społeczeństwa Informacyjnego*",

Kompetencje (z zaznaczeniem czy w pełni realizują wymagania *acquis, jeśli* nie odnotować poniżej)

a) udział Polski w 5 Programie Ramowym Badań, Rozwoju Technologicznego i Prezentacji UE (w tym w *Information Society Technologies Programme* – II podprogramie tematycznym 5 Programu) oraz przygotowanie do udziału w 6 Programie Ramowym,
b) kontynuacja prac przez Forum ds. Społeczeństwa Informacyjnego,
c) wdrażanie programu „*eEurope+ - Wspólne działania na rzecz wdrożenia Społeczeństwa Informacyjnego w Europie*",
d) wdrażanie programu *ePolska 2001-2006*,

Kompetencje do uzupełnienia:

a) Polska przedstawi raport dotyczący wdrożenia programu *eEurope+* w 2001, na Konferencji ministerialnej w Ljubljanie na początku czerwca 2002,
b) Program ePolska 2001-2006 będzie natomiast uaktualniony w kwietniu 2002 r.
c) W związku z utworzeniem działu administracji publicznej 'informatyzacja' (odnośne przepisy wchodzą w życie z dniem 01.07.2002 r.), decyzją Prezesa RM kompetencje w tym zakresie będą powierzone Ministrowi Nauki, Przewodniczącemu Komitetu Badań Naukowych. Konieczne będzie zapewnienie mu odpowiedniej obsługi administracyjnej.

Obsada kadrowa

Obecna: trudne do oszacowania ze względu na horyzontalny charakter podejmowanych działań.

Inne uwagi:

W ramach programu eEurope+ Polska uczestniczyc będzie m.in. w następujących programach szczegółowych:

a) w wieloletnim programie *eContent* – programie UE, mającym na celu stymulowanie rozwoju i wdrażania europejskich zasobów cyfrowych w sieciach globalnych oraz promowanie różnorodności językowej w społeczeństwie informacyjnym:
   - wszedł on w życie 18 stycznia 2001 r. w związku z zapotrzebowaniem w ramach inicjatywy *e*Europe, na wypełnienie zadań dotyczących upowszechniania zastosowań Internetu (*Government online: electronic access to public services* i *European digital content for global networks*) oraz priorytetowym traktowaniem przez UE działań na rzecz promocji kultury i dziedzictwa oraz różnorodności językowej, a także potrzebę wsparcia małych i średnich przedsiębiorstw działających w sektorze multimediów i teleinformatyki. Założony budżet programu w okresie 4 lat jego funkcjonowania wynosił będzie 100 mln EUR. DG Społeczeństwo Informacyjne zobowiązana została do przygotowywania dwuletnich planów realizacyjnych (pierwszy z nich obejmuje lata 2001 – 2002). *eContent* realizowany jest w trzech liniach tematycznych: 1) poprawa dostępności oraz rozszerzenie zakresu wykorzystywania informacji sektora publicznego (udział krajów kandydujących w inicjatywach tej linii tematycznej usprawni przyszłą integrację poprzez stworzenie lepszych i spójnych z europejskimi, zasad organizacji wykorzystywania informacji, na przykład rejestrów państwowych, dziedzictwa kulturowego, sektora publicznego w wersji wielojęzycznej,

Załącznik nr 9

ROZPORZĄDZENIE
MINISTRA INFRASTRUKTURY[1]
z dnia 24 stycznia 2003 r.
W SPRAWIE WYKONYWANIA PRZEZ OPERATORÓW ZADAŃ NA RZECZ OBRONNOŚCI, BEZPIECZEŃSTWA PAŃSTWA ORAZ BEZPIECZEŃSTWA I PORZĄDKU PUBLICZNEGO
(Dz. U. z dnia 7 Lutego 2003 R.)

Na podstawie art. 40 ust. 3 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, z 2001 r. Nr 122, poz. 1321 i Nr 154, poz. 1800 i 1802 oraz z 2002 r. Nr 25, poz. 253, Nr 74, poz. 676 i Nr 166, poz. 1360) zarządza się, co następuje:

§ 1.

1. Rozporządzenie określa:
   1) szczegółowe wymagania i sposób wykonywania przez operatorów obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie zapewnienia technicznych i organizacyjnych możliwości wykonywania w sieci telekomunikacyjnej eksploatowanej przez operatora zadań, na rzecz podmiotów, o których mowa w art. 40 ust. 2 ustawy z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne, zwanych dalej "uprawnionymi podmiotami";
   2) przypadki, w których operator może wnioskować o odroczenie wykonania obowiązków, o których mowa w pkt 1;
   3) warunki, jakie muszą być spełnione dla udzielenia odroczenia wykonania obowiązków, o których mowa w pkt 1;
   4) maksymalne terminy odroczeń wykonania obowiązków, o których mowa w pkt 1.
2. Ilekroć w rozporządzeniu jest mowa o "ustawie", rozumie się przez to ustawę z dnia 21 lipca 2000 r. - Prawo telekomunikacyjne.

§ 2.

1. Operator zapewnia uprawnionym podmiotom techniczne i organizacyjne możliwości realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w eksploatowanej przez niego sieci telekomunikacyjnej, zwanej dalej „siecią operatora", poprzez:
   1) przygotowanie technicznych systemów umożliwiających dostęp do treści informacji przesyłanej w sieci operatora oraz do danych posiadanych przez operatora, w tym do danych posiadanych przez innego operatora świadczącego usługę telekomunikacyjną przy wykorzystaniu sieci operatora, związanych ze świadczoną usługą;
   2) przygotowanie sieci operatora dla zapewnienia telekomunikacji dla systemu kierowania obroną państwa;
   3) przygotowanie sieci operatora do dołączania urządzeń telekomunikacyjnych będących w dyspozycji lub w posiadaniu uprawnionych podmiotów;
   4) udostępnianie urządzeń końcowych operatora dla zapewnienia telekomunikacji w sytuacjach szczególnych zagrożeń, o których mowa w art. 64-66 ustawy;
   5) przygotowanie sieci operatora do kierowania połączeń inicjowanych za pomocą numerów alarmowych do właściwych terytorialnie jednostek organizacyjnych służb ustawowo powołanych do niesienia pomocy oraz do preferencyjnej obsługi abonentów i użytkowników, ważnych dla funkcjonowania państwa w sytuacjach szczególnych zagrożeń, o których mowa w art. 64-66 ustawy.
2. Wymagania, o których mowa w ust. 1 pkt 1-3, są zapewniane w sposób ciągły.
3. Wymagania, o których mowa w ust. 1 pkt 2-5, są zapewniane na zasadach i w trybie określonych w przepisach art. 64-66 ustawy lub w umowach zawartych między uprawnionymi podmiotami i operatorami.

§ 3.

Systemy, o których mowa w § 2 ust. 1 pkt 1, zapewniają dostęp do:
1) danych identyfikujących abonentów, użytkowników i zakończenia sieci telekomunikacyjnych oraz danych dotyczących faktu, okoliczności i rodzaju połączenia, prób uzyskania połączenia między określonymi zakończeniami sieci telekomunikacyjnych, danych identyfikujących zakończenia sieci telekomunikacyjnych, między którymi wykonano połączenie, w tym połączenie konferencyjne, oraz lokalizacje tych zakończeń, zwanych dalej „danymi", posiadanych przez operatora;
2) treści informacji przesyłanej w sieci operatora, w tym treści informacji przesyłanej w tej sieci w wyniku świadczenia usługi telekomunikacyjnej przez innego operatora, zwanej dalej „treścią".

---

[1] Minister Infrastruktury kieruje działem administracji rządowej - łączność, na podstawie § 1 ust. 2 pkt 3 rozporządzenia Prezesa Rady Ministrów z dnia 29 marca 2002 r. w sprawie szczegółowego zakresu działania Ministra Infrastruktury (Dz. U. Nr 32, poz. 302 oraz z 2003 r. Nr 19, poz. 165).

- liberalizacja sektora usług pocztowych oraz poprawa jakości świadczonych usług powszechnych,

Kompetencje do uzupełnienia

W sektorze **telekomunikacyjnym**:

- W związku z dyrektywą o usługach powszechnych i prawach użytkownika dotyczącej sieci usług komunikacji elektronicznej, przyjęcie znowelizowanej ustawy Prawo telekomunikacyjne, uwzględniającej wspólnotową definicję usług powszechnych, wymogi dotyczące ich jakości oraz sposobu świadczenia przez operatora publicznego, uregulowania dotyczące finansowani świadczenia usługi powszechnej (np. Fundusz Usług Powszechnych), przenaszalność numerów, obowiązek „must – carry" mający na celu dostarczenie specjalnych programów telewizyjnych i radiowych, uregulowania odnoszące się do obowiązku przeprowadzania szerokich konsultacji środowiskowych dotyczących publicznie dostępnej sieci usług komunikacji elektronicznej, obowiązku zatwierdzania przez organ regulacyjny formy spisu abonentów oraz udostępniania tych spisów abonentom, nałożenie na organy regulacyjne obowiązku monitorowania taryf detalicznych publicznie dostępnej usługi telefonicznej w sieci stacjonarnej przez wyznaczone przedsiębiorstwa, rozszerzenie kontroli cenowej na urządzenia i usługi dodatkowe do zapewnienia podłączenia do publicznej sieci telefonicznej i publicznie dostępnych usług telefonicznych
- umożliwienie wszystkim potencjalnym użytkownikom możliwości korzystania z telekomunikacyjnych usług powszechnych (w przypadku usług telekomunikacyjnych związane jest to przede wszystkim z koniecznością rozwoju sieci telekomunikacyjnej, zwłaszcza na terenach słabo rozwiniętych),
- poprawa jakości świadczonych usług,
- wydanie aktów wykonawczych do ustawy Prawo Telekomunikacyjne w zakresie usług powszechnych:
- Rozporządzenia określającego szczegółowe wymagania dotyczące świadczenia usług powszechnych, w tym wymagania dotyczące ich jakości, dostępności , a także liczby publicznie dostępnych telefonów, w których połączenie jest opłacane automatycznie, w szczególności za pomocą monety, żetonu lub karty telefonicznej albo karty płatniczej, zwanych dalej „aparatami publicznymi"
- Rozporządzenia dotyczącego szczegółowego zakresu obowiązku świadczenia usług powszechnych osobom niepełnosprawnym, uwzględniające specyfikę potrzeb osób o różnych rodzajach niesprawności

§ 11.

Warunkiem uzyskania odroczenia jest:

1) złożenie wraz z wnioskiem, zaopiniowanego przez uprawnione podmioty, harmonogramu osiągania przez operatora pełnej zdolności realizacji zadań przez systemy, o których mowa w § 2 ust. 1 pkt 1;
2) udokumentowanie braku środków finansowych na dokończenie procesu wdrażania systemów, o których mowa w § 2 ust. 1 pkt 1, przy przekroczeniu pierwotnie zaplanowanych kosztów.

§ 12.

Maksymalny termin odroczenia wynosi sześć miesięcy.

§ 13.

1. Dla operatora, który rozpoczął eksploatację sieci telekomunikacyjnej lub rozpoczął świadczenie usług telekomunikacyjnych przy wykorzystaniu sieci innego operatora przed dniem wejścia w życie rozporządzenia, maksymalny termin odroczenia wynosi osiemnaście miesięcy.
2. Operator, który rozpoczął eksploatację sieci telekomunikacyjnej lub rozpoczął świadczenie usług telekomunikacyjnych przy wykorzystaniu sieci innego operatora przed dniem wejścia w życie rozporządzenia, może złożyć wniosek, o którym mowa w § 10 ust. 1, najpóźniej w terminie dwudziestu ośmiu dni od dnia wejścia w życie rozporządzenia.

§ 14.

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

§ 4.

Systemy, o których mowa w § 2 ust. 1 pkt 1, zapewniające dostęp do treści zapewniają również dostęp do danych z nią skojarzonych przesyłanych w sieci operatora:

1) identyfikujących abonentów i użytkowników uczestniczących w połączeniu, ze wskazaniem strony inicjującej połączenie oraz wszystkich uczestników połączenia konferencyjnego, a także ich lokalizację, wraz z kategorią połączenia zgodnie z kryteriami stosowanymi przez operatora;
2) dotyczących daty oraz czasu rozpoczęcia i zakończenia połączenia oraz długości jego trwania;
3) dotyczących niepełnych lub niezrealizowanych połączeń;
4) dotyczących przeniesień, przekierowań, dostępu do poczty głosowej, połączeń zwrotnych, połączeń do zlecania i realizacji usług sieciowych, modyfikacji i włączania funkcji sieciowych, zmiany kodów i numerów.

§ 5.

Systemy, o których mowa w § 2 ust. 1 pkt 1, zapewniają niezwłocznie w ciągu całej doby:

1) przechwytywanie, odbiór, przesyłanie, odczyt, rejestrację i przechowywanie treści oraz danych;
2) dostęp do treści i danych w taki sposób, aby treści i dane nie uległy zakłóceniu lub zniekształceniu, a treści i dane z nimi skojarzone były prezentowane w czasie rzeczywistym;
3) wprowadzanie przez uprawniony podmiot do sieci operatora danych lub wykonywanie innych czynności niezbędnych do uzyskania lub anulowania dostępu do treści i danych;
4) przechwytywanie treści i danych skojarzonych z tą treścią;
5) przekazywanie treści i danych między tymi systemami a elementami sieci telekomunikacyjnych;
6) jednoczesną i niezależną realizację czynności, o których mowa w pkt 3-5, na potrzeby uprawnionych podmiotów przy spełnieniu wymagań, o których mowa w pkt 2;
7) dostęp do danych posiadanych przez operatora, w tym danych posiadanych przez innego operatora świadczącego usługi telekomunikacyjne przy wykorzystaniu sieci operatora z ostatnich 12 miesięcy.

§ 6.

1. Realizacja czynności określonych w § 5 pkt 3 oraz realizacja odczytu treści i danych z nią skojarzonych, a także pobieranie danych, o których mowa w § 3 pkt 1, odbywa się w miejscach uzgodnionych pomiędzy uprawnionym podmiotem i operatorem.
2. Dostęp do treści i danych, o których mowa w § 3 i 4, jest realizowany za pomocą sieci telekomunikacyjnej.

§ 7.

W przypadku szyfrowania treści i danych przez operatora, w tym przez operatora świadczącego usługi przy wykorzystaniu sieci innego operatora, operator udostępnia treści i dane uprawnionym podmiotom w formie niezaszyfrowanej.

§ 8.

1. Systemy, o których mowa w § 2 ust. 1 pkt 1, zapewniają łączne i niezależne udostępnianie uprawnionym podmiotom treści i danych z nimi skojarzonych, z zastrzeżeniem ust. 2, w ilości co najmniej:
   1) 0,15% pojemności każdej centrali wchodzącej w skład sieci operatora;
   2) 0,2% zakończeń sieci operatora.
2. W przypadku równoczesnego i niezależnego udostępniania treści i danych z nimi skojarzonych ilości, o których mowa w ust. 1, wynoszą odpowiednio 0,05% i 0,03%.

§ 9.

Udział pracowników operatora w realizowaniu zadań, o których mowa w § 2 ust. 1, wymaga posiadania przez nich poświadczenia bezpieczeństwa wydanego na zasadach określonych w przepisach o ochronie informacji niejawnych i nie może naruszać ustawowych praw i obowiązków uprawnionego podmiotu realizującego zadanie oraz powinien być ograniczony do niezbędnego minimum.

§ 10.

1. Operator może złożyć wniosek o odroczenie terminu zapewnienia uprawnionemu podmiotowi technicznych i organizacyjnych możliwości realizacji zadań poprzez systemy, o których mowa w § 2 ust. 1 pkt 1, w przypadku udokumentowanych trudności organizacyjno-technicznych, dotyczących rozpoczętego procesu wdrażania tych systemów.
2. Operator może złożyć wniosek, o którym mowa w ust. 1, najpóźniej w terminie:
   1) dwóch miesięcy przed planowanym terminem rozpoczęcia eksploatacji sieci telekomunikacyjnej lub rozpoczęcia świadczenia usług telekomunikacyjnych w przypadku operatora działającego na podstawie zezwolenia telekomunikacyjnego;
   2) dwudziestu ośmiu dni przed planowanym terminem rozpoczęcia eksploatacji sieci telekomunikacyjnej lub rozpoczęcia świadczenia usług telekomunikacyjnych w przypadku operatora działającego na podstawie zgłoszenia działalności telekomunikacyjnej.

§ 7.

Przygotowanie infrastruktury, o którym mowa w § 4 ust. 2 pkt 3, polega na wytypowaniu istniejących lub budowie nowych obiektów budowlanych oraz wykonywaniu planów ich przystosowania i wyposażenia, umożliwiających ich wykorzystanie w razie wewnętrznego lub zewnętrznego zagrożenia bezpieczeństwa narodowego i w czasie wojny.

§ 8.

Stanowiska kierowania obejmują główne stanowiska kierowania i zapasowe stanowiska kierowania.

§ 9.

1. Główne stanowiska kierowania przygotowuje się w stałych siedzibach organów.
2. Stosownie do potrzeb, główne stanowiska kierowania mogą być przygotowywane także w innych, niż stała siedziba organu, obiektach budowlanych będących w trwałym zarządzie tego organu lub planowanych do przydzielenia temu organowi w ramach świadczeń na rzecz obrony, zwanych dalej „zapasowymi miejscami pracy".

§10.

1. Na potrzeby stanowisk kierowania wykorzystuje się obiekty budowlane ogólnego przeznaczenia, zwane dalej „obiektami budowlanymi", oraz obiekty budowlane wyposażone w urządzenia i sprzęt, których działanie jest niezależne od ogólnodostępnej infrastruktury techniczno-użytkowej, zwane dalej „obiektami specjalnymi".
2. W rejonie głównych stanowisk kierowania, dla Prezydenta Rzeczypospolitej Polskiej oraz Prezesa Rady Ministrów przygotowuje się stanowiska kierowania w obiektach budowlanych i obiektach specjalnych.
3. Przydział obiektów specjalnych na potrzeby stanowisk kierowania Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów, ministrów oraz centralnych organów administracji rządowej następuje na podstawie decyzji Prezesa Rady Ministrów.

§ 11.

1. Główne stanowiska kierowania przygotowuje się dla:
   1) Prezydenta Rzeczypospolitej Polskiej;
   2) Prezesa Rady Ministrów;
   3) ministrów, centralnych organów administracji rządowej oraz wojewodów;
   4) kierowników urzędów centralnych nie wchodzących w skład administracji rządowej;
   5) kierowników zespolonych służb, inspekcji i straży działających pod zwierzchnictwem wojewody oraz organów administracji nie zespolonej, ustalonych przez ministrów i wojewodów stosownie do kompetencji;
   6) organów wykonawczych samorządu terytorialnego.
2. Główne stanowiska kierowania przygotowują:
   1) minister właściwy do spraw wewnętrznych dla organów, o których mowa w ust. 1 pkt 1 i 2;
   2) organy, o których mowa w ust. 1 pkt 3-6.
3. Organy, o których mowa w ust. 1 pkt 3 i 4, przygotowują główne stanowiska kierowania:
   1) w swojej stałej siedzibie;
   2) w zapasowym miejscu pracy, którego lokalizację uzgadniają z ministrem właściwym do spraw wewnętrznych.
4. Organy, o których mowa w ust. 1 pkt 5 i 6, przygotowują główne stanowiska kierowania:
   1) w swojej stałej siedzibie;
   2) w zapasowym miejscu pracy, którego lokalizację uzgadniają z właściwym wojewodą.
5. W przypadku gdy organy, o których mowa w ust. 1 pkt 3-6, nie posiadają w trwałym zarządzie obiektów odpowiednich na zapasowe miejsce pracy, składają wnioski o przydział takich obiektów, w ramach świadczeń na rzecz obrony, do właściwego wojewody, starosty, prezydenta miasta, burmistrza lub wójta.

§ 12.

1. Zapasowe stanowiska kierowania przygotowuje się dla:
   1) Prezydenta Rzeczypospolitej Polskiej;
   2) Prezesa Rady Ministrów;
   3) ministrów i centralnych organów administracji rządowej, wskazanych przez Prezesa Rady Ministrów;
   4) wojewodów.
2. Zapasowe stanowiska kierowania przygotowują:
   1) Minister Obrony Narodowej dla organów, o których mowa w ust. 1 pkt 1-3;
   2) wojewodowie.
3. Usytuowanie zapasowego stanowiska kierowania wojewodowie uzgadniają z ministrem właściwym do spraw wewnętrznych i Ministrem Obrony Narodowej.

Załącznik nr 10

ROZPORZĄDZENIE RADY MINISTRÓW
z dnia 27 kwietnia 2004 r.
W SPRAWIE PRZYGOTOWANIA SYSTEMU KIEROWANIA BEZPIECZEŃSTWEM NARODOWYM
(Dz. U. z dnia 1 maja 2004 r.)

Na podstawie art. 6 ust. 2 pkt 2 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2002 r. Nr 21, póz. 205, z późn. zm.[1]) zarządza się, co następuje:

§ 1.

Rozporządzenie określa:
1) organizację i tryb przygotowania systemu kierowania bezpieczeństwem narodowym, w tym obroną państwa, zwanego dalej „systemem kierowania";
2) warunki funkcjonowania organów władzy publicznej na stanowiskach kierowania.

§ 2.

1. W skład systemu kierowania wchodzą organy władzy publicznej i kierownicy jednostek organizacyjnych, zwani dalej „organami", które wykonują zadania związane z kierowaniem bezpieczeństwem narodowym.
2. W skład systemu kierowania wchodzą również organy dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej, w tym Naczelny Dowódca Sił Zbrojnych, z chwilą jego mianowania.
3. Organy uczestniczą w kierowaniu bezpieczeństwem narodowym w granicach kompetencji określonych w odrębnych przepisach, z wykorzystaniem obsługujących ich urzędów oraz niezbędnej infrastruktury.
4. Organy wykonują zadania związane z kierowaniem bezpieczeństwem narodowym, w zależności od skali zagrożenia, z wykorzystaniem stałych siedzib lub stanowisk kierowania.

§ 3.

System kierowania przygotowuje się w celu zapewnienia ciągłości podejmowania decyzji i działań dla utrzymania bezpieczeństwa narodowego, w tym:
1) monitorowania źródeł, rodzajów, kierunków i skali zagrożeń;
2) zapobiegania powstawaniu zagrożeń bezpieczeństwa narodowego na terytorium Rzeczypospolitej Polskiej oraz poza jej granicami;
3) zapobiegania skutkom zagrożeń bezpieczeństwa narodowego, a także ich usuwania;
4) kierowania obroną państwa.

§ 4.

1. Przygotowanie systemu kierowania obejmuje planowanie, organizowanie i realizowanie przedsięwzięć zapewniających organom wykonywanie zadań związanych z kierowaniem bezpieczeństwem narodowym w czasie pokoju w razie wewnętrznego lub zewnętrznego zagrożenia bezpieczeństwa narodowego, w tym w razie wystąpienia działań terrorystycznych lub innych szczególnych zdarzeń, a także w czasie wojny.
2. Przedsięwzięcia, o których mowa w ust. 1, obejmują:
   1) przygotowanie organów i obsługujących ich urzędów do funkcjonowania w systemie kierowania;
   2) wykonywanie planów operacyjnych i programów obronnych;
   3) przygotowanie infrastruktury umożliwiającej funkcjonowanie systemu kierowania.
3. Przedsięwzięcia, o których mowa w ust. 2, realizuje się w czasie pokoju.
4. W przygotowaniu systemu kierowania uwzględnia się również przedsięwzięcia wynikające z umów międzynarodowych, którymi Rzeczpospolita Polska jest związana.

§ 5.

Przygotowanie organów i obsługujących ich urzędów, o którym mowa w § 4 ust. 2 pkt 1, realizuje się przez:
1) prowadzenie polityki kadrowej w zakresie obsady stanowisk służbowych zapewniających przygotowanie oraz sprawne funkcjonowanie systemu kierowania;
2) udział w szkoleniu obronnym prowadzonym na podstawie odrębnych przepisów.

§ 6.

Warunki i tryb wykonywania planów operacyjnych i programów obronnych, o których mowa w § 4 ust. 2 pkt 2, określają odrębne przepisy.

---

[1] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 74, poz. 676, Nr 81, poz. 732, Nr 113, poz. 984 i 985, Nr 156, poz. 1301, Nr 166, poz. 1363, Nr 199, poz. 1673 i Nr 200, poz. 1679 i 1687 oraz z 2003 r. Nr 45, poz. 391, Nr 90, poz. 844, Nr 96, poz. 874, Nr 139, poz. 1326, Nr 179, poz. 1750, Nr 210, poz. 2036 i Nr 223, poz. 2217.

11) szkolenie pracowników zapewniających utrzymanie obiektów specjalnych stanowisk kierowania w gotowości do ich wykorzystania;
12) określenie świadczeń na rzecz obrony w zakresie przygotowania infrastruktury;
13) weryfikację przydziału obiektów budowlanych oraz monitorowanie należytego ich utrzymania przez kolejnych użytkowników.

§ 17.

1. Finansowanie zadań realizowanych w ramach przygotowania stanowisk kierowania należy do organów, które będą na tych stanowiskach funkcjonować, z zastrzeżeniem ust. 2 i 3.
2. Finansowanie zadań związanych z przygotowaniem zapasowych miejsc pracy głównych stanowisk kierowania Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów należy do ministra właściwego do spraw wewnętrznych.
3. Finansowanie zadań związanych z przygotowaniem stanowisk kierowania, o których mowa w § 12 ust. 2 pkt 1, należy do Ministra Obrony Narodowej.

§ 18.

1. Przemieszczenie organów, o których mowa w § 12 ust. 1 pkt 3 i 4, na zapasowe stanowiska kierowania realizuje się na podstawie decyzji Prezesa Rady Ministrów, zgodnie z opracowanymi planami operacyjnymi, o ile odrębne przepisy nie stanowią inaczej.
2. Przemieszczenie organów, o których mowa w § 11 ust. 1 pkt 3 i 4, na zapasowe miejsca pracy realizuje się na podstawie decyzji danego organu, zgodnie z opracowanymi planami operacyjnymi, po uprzednim powiadomieniu Szefa Kancelarii Prezesa Rady Ministrów oraz ministra właściwego do spraw wewnętrznych.
3. Przemieszczenie organów, o których mowa w § 11 ust. 1 pkt 5 i 6, na zapasowe miejsca pracy realizuje się na podstawie decyzji danego organu, zgodnie z opracowanymi planami operacyjnymi.

§ 19.

W ramach przygotowywania systemu kierowania Minister Obrony Narodowej:
1) przygotowuje projekty *zadań* dla organów administracji rządowej związanych z przygotowaniem systemu kierowania;
2) koordynuje wykonywanie zadań związanych z przygotowaniem systemu kierowania;
3) uzgadnia lokalizację nowych obiektów specjalnych przeznaczonych na stanowiska kierowania, stosownie do wniosków zgłoszonych przez zainteresowane organy;
4) w rejonie zapasowych stanowisk kierowania:
   a) przygotowuje stanowiska kierowania w zakresie uzgodnionym z organami, o których mowa w § 12 ust. 1 pkt 1-3,
   b) sprawuje nadzór nad maskowaniem przedsięwzięć związanych z przygotowaniem zapasowych stanowisk kierowania,
   c) zapewnia bezpośrednią ochronę i obronę rejonu, a w uzgodnieniu z Szefem Biura Ochrony Rządu, bezpośrednią ochronę określonych osób,
   d) zapewnia, we współdziałaniu z ministrem właściwym do spraw wewnętrznych oraz właściwym wojewodą, bezpieczeństwo i porządek publiczny, ochronę przeciwpożarową, prowadzenie akcji ratunkowo-ewakuacyjnych oraz ostrzeganie i alarmowanie,
   e) przygotowuje, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych oraz ministrem właściwym do spraw łączności i Szefem Agencji Bezpieczeństwa Wewnętrznego, plan organizacji systemu łączności, w tym łączności specjalnej,
   f) zapewnia warunki utrzymania obiektów specjalnych, a także ich obsługi technicznej w razie wewnętrznego lub zewnętrznego zagrożenia bezpieczeństwa narodowego i w czasie wojny.

§ 20.

W ramach przygotowywania systemu kierowania minister właściwy do spraw wewnętrznych:
1) opracowuje, w uzgodnieniu z Ministrem Obrony Narodowej, koncepcję przygotowania i utrzymania obiektów specjalnych;
2) przygotowuje, w uzgodnieniu z Ministrem Obrony Narodowej, plan przemieszczenia organów, o których mowa w § 12 ust. 1 pkt 1-3, na zapasowe stanowiska kierowania;
3) w rejonie głównych stanowisk kierowania:
   a) przygotowuje stanowiska kierowania Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów, w zakresie uzgodnionym odpowiednio z Szefem Biura Bezpieczeństwa Narodowego i z Szefem Kancelarii Prezesa Rady Ministrów,
   b) przygotowuje obiekty specjalne stanowisk kierowania Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów,
   c) planuje i organizuje przemieszczenie Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów na zapasowe miejsca pracy,

4. Wojewodowie, w ramach zapasowych stanowisk kierowania, zapewniają miejsca pracy marszałkowi województwa lub komisarzowi rządowemu powołanemu na podstawie odrębnych przepisów, a także innym organom niezbędnym w kierowaniu obroną województwa.
5. Ministrowie i centralne organy administracji rządowej, inni niż określeni w ust. 1 pkt 3, oraz kierownicy urzędów centralnych nie wchodzących w skład administracji rządowej, mogą - stosownie do swoich potrzeb - przygotowywać zapasowe stanowiska kierowania, których lokalizację uzgadniają z właściwym wojewodą.

§ 13.

1. Stanowiska kierowania Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów oraz ministrów i centralnych organów administracji rządowej, wskazanych przez Prezesa Rady Ministrów, tworzą Centralne Stanowisko Kierowania Obroną Państwa.
2. Granice rejonu głównych stanowisk kierowania organów, o których mowa w ust. 1, ustala Prezes Rady Ministrów, na wniosek ministra właściwego do spraw wewnętrznych uzgodniony z Ministrem Obrony Narodowej.

§ 14.

1. Zapasowe stanowiska kierowania organów, o których mowa w § 12 ust. 1 pkt 1-3, przygotowuje się w rejonach, które w pierwszym okresie prowadzenia obrony państwa będą najmniej narażone na działanie środków walki, zwanych dalej „rejonami zapasowych stanowisk kierowania".
2. Granice rejonów zapasowych stanowisk kierowania organów, o których mowa w § 12 ust. 1 pkt 1-3, ustala Prezes Rady Ministrów, na wniosek Ministra Obrony Narodowej uzgodniony z ministrem właściwym do spraw wewnętrznych.

§ 15.

Organy przygotowujące stanowiska kierowania, z zastrzeżeniem § 19 pkt 4 lit. a i § 20 pkt 3 lit. a, są obowiązane do:

1) przygotowania obiektów przeznaczonych na stanowiska kierowania, w tym przydzielonych w ramach świadczeń na rzecz obrony, zgodnie z wymogami określonymi w § 16;
2) przygotowania regulaminów i instrukcji pracy na stanowiskach kierowania;
3) ujęcia w planach operacyjnych zamierzeń związanych z przemieszczeniem i funkcjonowaniem na stanowiskach kierowania.

§ 16.

Przygotowanie stanowiska kierowania obejmuje:

1) opracowanie dokumentacji związanej z przemieszczeniem i zapewnieniem warunków funkcjonowania organu na stanowisku kierowania;
2) utrzymywanie stanu technicznego oraz modernizację infrastruktury przez jej użytkowników w czasie pokoju;
3) ustalenie zasad i trybu obiegu informacji dotyczącej gotowości organu do podjęcia zadań i ich realizacji oraz zorganizowanie specjalnych, w tym utajnionych, systemów teleinformatycznych;
4) wyposażenie w urządzenia łączności zapewniające możliwość niezakłóconej pracy organu;
5) wyposażenie w urządzenia filtrowentylacyjne, źródła energii elektrycznej i cieplnej oraz ujęcia wody, których działanie jest niezależne od ogólnodostępnej infrastruktury techniczno-użytkowej;
6) wyposażenie w urządzenia techniczne i sanitarne oraz sprzęt biurowy i kwaterunkowy niezbędny do pracy i odpoczynku;
7) uodpornienie na oddziaływanie środków rozpoznania i rażenia przeciwnika, głównie przez maskowanie oraz budowę i modernizację ukryć i schronów;
8) zorganizowanie:
   a) żywienia i zaopatrywania w artykuły codziennego użytku,
   b) zabezpieczenia medycznego,
   c) transportu oraz obsługi pojazdów i urządzeń technicznych,
   d) zaopatrywania w paliwa i materiały eksploatacyjne,
   e) osłony kontrwywiadowczej,
   f) punktów zabiegów specjalnych;
9) zorganizowanie systemu powiadamiania i alarmowania o zagrożeniu z powietrza oraz skażeniach i zakażeniach;
10) przygotowanie środków do:
   a) rozwinięcia i odtwarzania systemu łączności oraz utrzymania bezpieczeństwa teleinformatycznego,
   b) ochrony i obrony stanowisk kierowania, w tym przed rozpoznaniem i obezwładnianiem radioelektronicznym,
   c) prowadzenia akcji ratowniczych,
   d) przemieszczenia na zapasowe miejsca pracy i zapasowe stanowiska kierowania;

Załącznik nr 11

DZ.U.04.180.1855
ROZPORZĄDZENIE RADY MINISTRÓW
z dnia 3 sierpnia 2004 r.
W SPRAWIE PRZYGOTOWANIA I WYKORZYSTANIA SYSTEMÓW ŁĄCZNOŚCI NA POTRZEBY OBRONNE PAŃSTWA
(Dz. U. z dnia 18 sierpnia 2004 r.)

Na podstawie art. 6 ust. 2 pkt 7 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 2002 r. Nr 21, poz. 205, z późn. zm[1]. zarządza się, co następuje:

§ 1.

Rozporządzenie określa:
1) warunki i sposób przygotowania i wykorzystania systemów łączności na potrzeby obronne państwa;
2) właściwość organów władzy publicznej w sprawach, o których mowa w pkt 1.

§ 2.

Użyte w rozporządzeniu określenia oznaczają:
1) obronne systemy łączności - systemy łączności przygotowane do wykorzystania na potrzeby obronne;
2) dedykowane sieci telekomunikacyjne - sieci telekomunikacyjne wydzielone lub wydzierżawione z infrastruktury operatorów telekomunikacyjnych lub wybudowane wyłącznie na potrzeby użytkowników specjalnych, przeznaczone do zapewnienia telekomunikacji w razie zagrożenia bezpieczeństwa państwa;
3) inwestycja postulowana - inwestycję realizowaną, na wniosek organu administracji rządowej, przez ministra właściwego do spraw łączności, w zakresie przygotowania obronnych systemów łączności;
4) preferencyjna obsługa - przedsięwzięcia organizacyjno-techniczne umożliwiające priorytetowe zapewnienie telekomunikacji lub poczty użytkownikom specjalnym, w tym w warunkach zakłóceń funkcjonowania systemów łączności;
5) resortowe sieci telekomunikacyjne - sieci telekomunikacyjne eksploatowane przez organy władzy publicznej na własne potrzeby;
6) system łączności specjalnej - system łączności zabezpieczony przed nieuprawnionym dostępem do przekazywanej w nim informacji przez zastosowanie urządzeń i narzędzi kryptograficznych;
7) użytkownik specjalny - organ władzy publicznej, Siły Zbrojne Rzeczypospolitej Polskiej lub przedsiębiorcę o szczególnym znaczeniu gospodarczo-obronnym, o którym mowa w art. 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. Nr 122, poz. 1320 oraz z 2002 r. Nr 188, poz. 1571).

§ 3.

Obronne systemy łączności powinny cechować się w szczególności:
1) niezawodnością;
2) odpornością na zakłócenia;
3) zdolnością zapewnienia użytkownikom specjalnym bezpiecznego przekazywania informacji;
4) zdolnością zachowania ciągłości łączności podczas zmian miejsc pracy, w ramach stanowisk kierowania;
5) zdolnością do elastycznej rekonfiguracji systemu;
6) zdolnością do preferencyjnej obsługi użytkowników specjalnych.

§ 4.

Przygotowanie i wykorzystanie obronnych systemów łączności obejmuje planowanie, organizowanie i realizację przedsięwzięć umożliwiających kierowanie państwem w warunkach zagrożenia bezpieczeństwa państwa i w czasie wojny lub dowodzenie Siłami Zbrojnymi Rzeczypospolitej Polskiej.

§5.

1. Przygotowanie obronnych systemów łączności realizuje się w szczególności przez:
   1) precyzowanie potrzeb w zakresie łączności;
   2) analizę możliwości przedsiębiorców telekomunikacyjnych i operatorów pocztowych w zakresie ich wykorzystania na potrzeby obronne państwa;
   3) planowanie wykorzystania istniejących systemów łączności na potrzeby obronne państwa;
   4) wytypowanie osób odpowiedzialnych za planowanie, wdrażanie, zarządzanie i eksploatację obronnych systemów łączności;
   5) utworzenie bazy danych o przedsiębiorcach telekomunikacyjnych i operatorach pocztowych, niezbędnej do przygotowania i wykorzystania obronnych systemów łączności;

---

[1] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 74, poz. 676, Nr 81, poz. 732, Nr 113, poz. 984 i 985, Nr 156, poz. 1301, Nr 166, poz. 1363, Nr 199, poz. 1673 i Nr 200, poz. 1679 i 1687, z 2003 r. Nr 45, poz. 391, Nr 90, poz. 844, Nr 96, poz. 874, Nr 139, poz. 1326, Nr 179, poz. 1750, Nr 210, poz. 2036 i Nr 223, poz. 2217 oraz z 2004 r. Nr 116, poz. 1203.

d) zapewnia ochronę i obronę stanowisk kierowania Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów,
e) zapewnia bezpośrednią ochronę określonych osób,
f) planuje i organizuje, w uzgodnieniu z ministrem właściwym do spraw łączności, specjalne systemy teleinformatyczne na potrzeby systemu kierowania oraz zapewnia ich funkcjonowanie,
g) zapewnia utrzymanie obiektów specjalnych przeznaczonych dla Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów, ministrów oraz centralnych organów administracji rządowej w gotowości do wykorzystania, a także ich obsługę techniczną w razie wewnętrznego lub zewnętrznego zagrożenia bezpieczeństwa narodowego i w czasie wojny,
h) zapewnia ochronę oraz bezpieczeństwo, porządek publiczny i ochronę przeciwpożarową,
i) zapewnia funkcjonowanie systemu ostrzegania i alarmowania oraz prowadzenie akcji ratunkowo-ewakuacyjnych.

§ 21.

W ramach przygotowywania systemu kierowania minister właściwy do spraw łączności:
1) w uzgodnieniu z Ministrem Obrony Narodowej, ministrem właściwym do spraw wewnętrznych, ministrem właściwym do spraw zagranicznych i Szefem Agencji Bezpieczeństwa Wewnętrznego przygotowuje:
   a) koncepcję organizacji systemu łączności, w tym współdziałania z systemami łączności państw sojuszniczych,
   b) wymagania techniczno-eksploatacyjne dla urządzeń łączności wykorzystywanych na potrzeby systemu kierowania, a także standardy wyposażenia stanowisk kierowania w urządzenia łączności oraz nadzoruje ich wdrażanie poprzez Prezesa Urzędu Regulacji Telekomunikacji i Poczty;
2) zapewnia, w uzgodnieniu z Prezesem Urzędu Regulacji Telekomunikacji i Poczty, na wniosek organów, o których mowa w § 11 ust. 1, połączenie wewnętrznej sieci telekomunikacyjnej stanowisk kierowania z sieciami przedsiębiorców telekomunikacyjnych;
3) opracowuje koncepcję wykonywania i odbioru robót w zakresie łączności oraz wyłania wykonawców dokumentacji projektowej i robót w rejonach stanowisk kierowania, a także sprawuje nadzór nad ich wykonywaniem poprzez Prezesa Urzędu Regulacji Telekomunikacji i Poczty.

§ 22.

W ramach przygotowywania systemu kierowania minister właściwy do spraw zdrowia przygotowuje, w uzgodnieniu z Ministrem Obrony Narodowej i ministrem właściwym do spraw wewnętrznych, plan zabezpieczenia świadczeń zdrowotnych na potrzeby Prezydenta Rzeczypospolitej Polskiej, Prezesa Rady Ministrów, ministrów oraz centralnych organów administracji rządowej i jednostek organizacyjnych zabezpieczających ich funkcjonowanie w rejonach głównych i zapasowych stanowisk kierowania.

§ 23.

W ramach przygotowywania systemu kierowania minister właściwy do spraw budownictwa, gospodarki przestrzennej i mieszkaniowej:
1) przygotowuje, na podstawie koncepcji, o której mowa w § 20 pkt 1, warunki jakim powinny odpowiadać nowo budowane obiektyspecjalne i inne obiekty adaptowane na potrzeby stanowisk kierowania;
2) przygotowuje warunki wykonywania i odbioru robót budowlano-montażowych oraz wykonywania rozruchów mechaniczno-technologicznych;
3) planuje, w uzgodnieniu z Ministrem Obrony Narodowej i ministrem właściwym do spraw wewnętrznych, normy należności środków materiałowych dla organów funkcjonujących na stanowiskach kierowania, w tym gromadzenia i utrzymywania rezerwy specjalnej tych środków;
4) przygotowuje, stosownie do wniosków złożonych przez zainteresowane organy, programy modernizacji i budowy obiektów specjalnych oraz przedstawia je do zatwierdzenia Radzie Ministrów.

§ 24.

W ramach przygotowywania systemu kierowania Szef Agencji Bezpieczeństwa Wewnętrznego:
1) zapewnia ochronę kontrwywiadowczą oraz rozpoznanie radioelektroniczne rejonów i obiektów stanowisk kierowania organów określonych w § 11 ust. 1 pkt 1-3;
2) zapewnia bezpieczeństwo systemów i sieci teleinformatycznych niezbędnych do wytwarzania, przetwarzania, przechowywania i przekazywania informacji niejawnych.

§ 25.

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

c) precyzuje wymagania eksploatacyjne dla urządzeń łączności wykorzystywanych na potrzeby obronnego systemu łączności oraz nadzoruje ich wdrażanie przez Prezesa Urzędu Regulacji Telekomunikacji i Poczty,
d) opracowuje plany i realizuje inwestycje postulowane;

2) Minister Obrony Narodowej zapewnia:
a) wskazywanie potrzeb Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie telekomunikacji i poczty,
b) opracowywanie warunków wykonywania działalności telekomunikacyjnej i pocztowej, w czasie zagrożenia bezpieczeństwa państwa i w czasie wojny, przez komórki i jednostki organizacyjne resortu obrony narodowej oraz przez jednostki sił zbrojnych państw sojuszniczych przebywające czasowo na terytorium Rzeczypospolitej Polskiej na podstawie umów, których Rzeczpospolita Polska jest stroną;

3) minister właściwy do spraw wewnętrznych zapewnia opracowywanie, w uzgodnieniu z ministrem właściwym do spraw łączności, Ministrem Obrony Narodowej, Szefem Agencji Bezpieczeństwa Wewnętrznego, wykazu organów administracji rządowej uprawnionych do preferencyjnej obsługi oraz przekazanie tego wykazu przedsiębiorcom telekomunikacyjnym i operatorom pocztowym za pośrednictwem Prezesa Urzędu Regulacji Telekomunikacji i Poczty;

4) Szef Agencji Bezpieczeństwa Wewnętrznego oraz Szef Wojskowych Służb Informacyjnych, każdy w zakresie swojej właściwości, zapewnia bezpieczeństwo systemów łączności specjalnej;

5) Prezes Urzędu Regulacji Telekomunikacji i Poczty zapewnia realizacją przedsięwzięć, o których mowa w § 5 ust. 1 pkt 2 i 5 oraz ust. 2 pkt 2, oraz kontrolę realizacji zadań na rzecz obronności, wykonywanych przez przedsiębiorców telekomunikacyjnych i operatorów pocztowych, w zakresie łączności;

6) wojewoda zapewnia:
a) opracowywanie potrzeb w zakresie łączności jednostek organizacyjnych podległych i nadzorowanych, przedsiębiorców, dla których jest organem założycielskim, oraz przedsiębiorców niebędących jednostkami organizacyjnymi podległymi lub nadzorowanymi przez ministrów,
b) planowanie, organizowanie i realizację przedsięwzięć związanych z przygotowaniem systemów łączności stanowisk kierowania podmiotów, o których mowa w lit. a,
c) opracowywanie, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, wykazu podmiotów, o których mowa w lit. a, uprawnionych do preferencyjnej obsługi oraz przekazywanie go przedsiębiorcom telekomunikacyjnym i operatorom pocztowym za pośrednictwem Prezesa Urzędu Regulacji Telekomunikacji i Poczty.

2. Przedsięwzięcia, o których mowa w ust. 1 pkt 1 lit. a, c i d oraz w § 5 ust. 1 pkt 3, 5 i 6, ust. 2 pkt 1-3 i ust. 3, realizowane są w uzgodnieniu z Ministrem Obrony Narodowej i ministrem właściwym do spraw wewnętrznych.

§ 12.

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

6) precyzowanie standardów wyposażenia stanowisk kierowania;
7) wykonywanie inwestycji;
8) wykonywanie inwestycji postulowanych.

2. Przygotowanie obronnych systemów łączności w zakresie telekomunikacji realizuje się w szczególności przez:
   1) opracowywanie zasad współpracy sieci przedsiębiorców telekomunikacyjnych z resortowymi sieciami telekomunikacyjnymi;
   2) dostosowywanie obiektów i infrastruktury telekomunikacyjnej przedsiębiorców telekomunikacyjnych do współpracy z ruchomymi urządzeniami telekomunikacyjnymi zgodnie z potrzebami określanymi w szczególności przez Ministra Obrony Narodowej lub ministra właściwego do spraw wewnętrznych;
   3) wskazywanie potrzeb w zakresie rozbudowy infrastruktury telekomunikacyjnej przedsiębiorców telekomunikacyjnych w ramach inwestycji postulowanych;
   4) zapewnianie bezpieczeństwa systemów łączności specjalnej.
3. Przygotowanie obronnych systemów łączności w zakresie poczty realizuje się w szczególności przez precyzowanie potrzeb w zakresie współdziałania operatorów pocztowych z wojskową pocztą polową, z pocztą specjalną podległą ministrowi właściwemu do spraw wewnętrznych oraz z pocztą kurierską podległą ministrowi właściwemu do spraw zagranicznych.

§ 6.

Obronne systemy łączności przygotowuje się z wykorzystaniem w szczególności:
1) resortowych sieci telekomunikacyjnych;
2) sieci telekomunikacyjnych przedsiębiorców telekomunikacyjnych;
3) dedykowanych sieci telekomunikacyjnych;
4) infrastruktury operatorów pocztowych;
5) wojskowej poczty polowej, poczty specjalnej podległej ministrowi właściwemu do spraw wewnętrznych oraz poczty kurierskiej podległej ministrowi właściwemu do spraw zagranicznych.

§ 7.

Przygotowanie obronnych systemów łączności dokonuje się w czasie pokoju, przy uwzględnieniu konieczności ich rozwinięcia, rozbudowy i rekonfiguracji w czasie zagrożenia bezpieczeństwa państwa i w czasie wojny.

§ 8.

Sieci wewnętrzne stanowiska kierowania wykonuje organ władzy publicznej, który przygotowuje i utrzymuje dane stanowisko.

§ 9.

Organy władzy publicznej przy planowaniu, budowie, rozbudowie, eksploatacji lub łączeniu systemów łączności uwzględniają potrzeby wynikające z zapewnienia bezpieczeństwa państwa.

§ 10.

1. Obronne systemy łączności wykorzystywane są na potrzeby:
   1) systemu kierowania bezpieczeństwem narodowym;
   2) zapewnienia funkcjonowania państwa w razie zagrożenia bezpieczeństwa i w czasie wojny;
   3) dowodzenia Siłami Zbrojnymi Rzeczypospolitej Polskiej;
   4) współpracy z systemami łączności państw sojuszniczych;
   5) utrzymywania w stałej gotowości jednolitych systemów obserwacji, pomiarów, analiz, prognozowania i powiadamiania, o których mowa w art. 6 ust. 1 pkt 6 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej.
2. Obronne systemy łączności mogą być wykorzystywane także w czasie pokoju, w tym w razie wystąpienia działań terrorystycznych lub innych szczególnych zdarzeń.

§ 11.

1. W ramach przygotowania i wykorzystania obronnych systemów łączności organy władzy publicznej, według swojej właściwości, zaspokajają potrzeby dotyczące funkcjonowania obronnych systemów łączności w szczególności na stanowiskach kierowania, realizując przedsięwzięcia, o których mowa w § 5 ust. 1 pkt 1, 4 i 7, a ponadto:
   1) minister właściwy do spraw łączności zapewnia, na wniosek organów administracji rządowej, połączenie sieci, o których mowa w § 8, z sieciami telekomunikacyjnymi przedsiębiorców telekomunikacyjnych, a także realizuje przedsięwzięcia, o których mowa w § 5 ust. 1 pkt 3 i 6, ust. 2 pkt 1 i 3, ust. 3 oraz:
      a) koordynuje przygotowanie i wykorzystanie systemów łączności na potrzeby obronne państwa,
      b) powołuje ekspertów w zakresie zarządzania kryzysowego, planowania cywilnego i współpracy cywilno-wojskowej w dziale administracji rządowej - łączność,

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 58639
II
Akademii