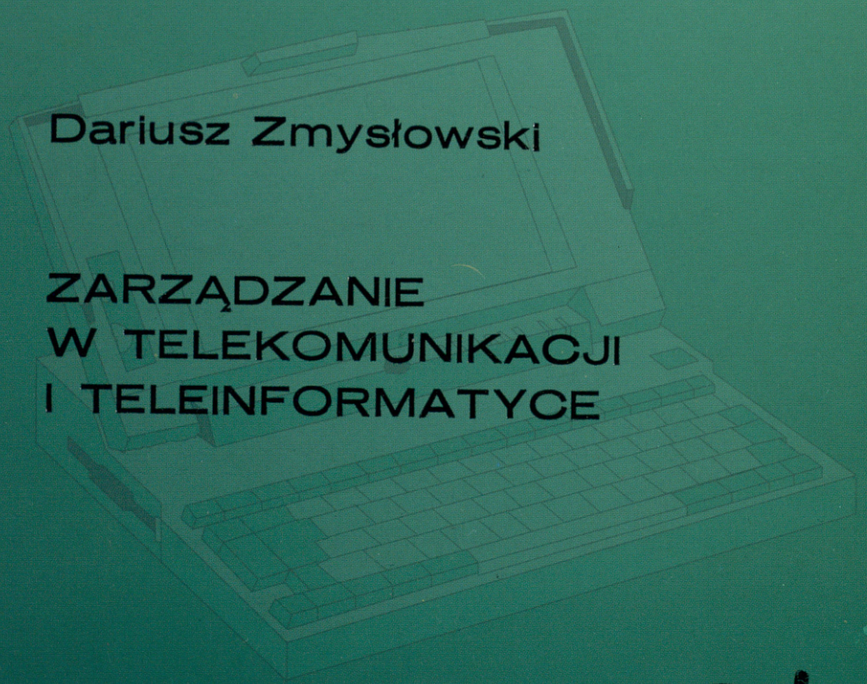
AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
AKADEMII OBRONY NARODOWEJ

AON 5657/04



Dariusz Zmysłowski

ZARZĄDZANIE W TELEKOMUNIKACJI I TELEINFORMATYCE

WARSZAWA

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ WOJSK LĄDOWYCH
INSTYTUT ZARZĄDZANIA I DOWODZENIA

AON 5657/04

Dariusz Zmysłowski

ZARZĄDZANIE
W TELEKOMUNIKACJI I TELEINFORMATYCE

WARSZAWA 2004

Spis treści

Spis treści

Spis ilustracji

Spis Tabel

Wykaz ważniejszych oznaczeń

ACSE	*ang. Association Contorol Service Element*
API	*ang. Application Programming Interface lub Application Program Interface.– Interfejs programów użytkowych.*
AppleTalk	*ang. Protokół komunikacyjny firmy Apple Computer*
APPN	*ang. Advanced Peer-to-Peer Networking*
ARP	*ang. Adress Resolution Protocol*
ARPA	*ang. Pierwsza sieć pakietowa. Oferuje usługi datagramowe, przesyłające pakety zmiennymi trasami w sieci*
ASCII	*ang. American Standard Code for Information Interchange*
ASN.1	*ang. Abstract Syntax Notation One*
ATM	*ang. Asynchronus Transfer Mode*
CCITT	*ang. Consultative Committee for International Telegraph and Telefone – Komitet Miedzynarodowej Unii Telekomunikacyjne*
CMIP	*ang. Common Management Information Protocol*
CMIS	*ang. Common Management Information Service*
CMOT	*ang. CMIP over TCP/IP*
CORBA	*ang. Common Object Request Broken Architecture*
CPU	*ang. Central Unit Procesor*
CRC	*ang. Cyclic Redundancy Code*
DCF	*ang. Data Communications Function*
DCN	*ang. Data Communication Network*
DES	*ang. Data Encryption Standard*
DIAL	*ang. Dial-In Access to LAN*
DME	*ang. Distributed Management Environment*
DMI	*ang. Desktop Management Interface*
DMI	*ang. Definition of management Information*
DSL	*ang. Data-link Switching*
DSM	*ang. Distribured State Machine*
ELAN	*ang. Emulated LAN*
FDDI	*ang. Fiber Distributed Data Interface*
GIS	*ang. Geographical Information Systems*
GUI	*ang. Graphics User Interface*
IAB	*ang. Internet Activities Board*
ICF	*ang. Information Conversion Function*
ICF	*ang. Information Conversion Function*
ICMP	*ang. Internet Control Message Protocol*
ICMP	*ang. Internet Control Message Protocol*
IDRP	*ang. Interdomain Routing Protocol*
IETF	*ang. Internet Enginneering Task Force*
IP	*ang. Internet Protocol*
IPX	*ang. Internetwork Packet Exchange*
ISDN	*ang. Integrated Service Digital Network*
ISO	*ang. International Oraganization for Standarization*
IT	*ang. Informatic Technology*
ITU	*ang. International Telecommunications Union*
LAN	*ang. Local Area Network*
LCN	*ang. Local Communication Network*
LED	*ang. Light Emitting Diode*
MAC	*ang. Media Access Control*

MAF	*ang. Management Application Function*
MCF	*ang. Message Communications Function*
MD	*ang. Media Device*
MD5	*ang. Message Digest 5 – algorytm autentyfikacji*
MIB	*ang. Management Information Base*
MIF	*ang. Management Information Format*
MIS	*ang. Management Information Server*
NE	*ang. Network Element*
NFS	*ang. Network File System*
NMA	*ang. Network Management Agent*
NMF	*ang. Network Management Forum*
NMS	*ang. Network Management System*
ODBC	*ang. Open DataBase Connectivity*
OSF	*ang. Operations Systems Function block*
OSF	*ang. Open Software Foundation*
OSI	*ang. Open Systems Interconnection*
OSPF	*ang. Open Shortest Path First Protocol*
OSS	*ang. Operations Support System)*
PC	*ang. Personal Computer*
PVC	*ang. Permanent Virtual Circuits*
RAS	*ang. Remote Access Software*
RCL	*ang. Request Control Language*
RFC	*ang. Request for Comments (dokument)*
RMON	*ang. Remote MONitoring*
ROSE	*ang. Remote Operation Service Element).*
RPC	*ang. Remote Procedure Call*
RTM	*ang. Mechanizm pułapek, rozszerzający możliwości SNMP.*
SLIP	*ang. Serial Line IP*
SMS	*ang. Systems Management Server*
SMS	*ang. Short Message Service*
SNA	*ang. System Network Architekture*
SNMP, SNMPv1, SNMPv2	*ang. Simple Network Management Protocol*
SPX	*ang. Sequenced Packet Exchange*
SQL	*ang. Structured Query Language*
TCP/IP	*ang. Ttansmission Control Protocol/Internet Protocol*
TFTP	*ang. Trivial File Transfer Protocol*
TMN	*ang. Telekomunication Management Network*
UDP	*ang. User datagram Protocol*
VLAN	*ang. Virtual LAN*
VPN	*ang. Virtual Private Network*
VPN	*ang. Virtual Private Network*
WAN	*ang. Wide Area Network*
WS	*ang. Work Station*

Wprowadzenie

Najważniejszym faktem, który trzeba sobie uświadomić jest to, że obecnie sieci telekomunikacyjne są dość złożonymi, rozległymi strukturami sprzętowo – programowymi, które w zależności od warunków i realizowanych zadań mają różną i bardzo zmienną w czasie strukturę logiczną. Jest tak dlatego, że sieci są systemami heterogenicznymi, na które składają się różne, często znacznie odmienne architektury logiczne.

Powszechne i praktycznie wykorzystywane są kanały i sieci wirtualne. Informacje przesyłane w sieciach teleinformatycznych mają postać ciągów binarnych, zgrupowanych w zależności od technologii transportowej w pakiety, ramki lub komórki. W związku z przedstawionymi faktami szczególnego znaczenia nabrało sterowanie ruchem w sieciach teleinformatycznych, z którym nierozłącznie wiążą się zagadnienia optymalizacji przepływów w sieciach w relacjach dwubiegunowych.

Kryteriami optymalizacyjnymi w zależności od świadczonych przez sieć usług są:

- minimalizacja czasu w przypadku obsługi usługi transmisji głosu np. Voice over IP, Voice over Frame Relay, Voice over ATM,
- minimalizacja kosztów transmisji – szczególnie ważna w sytuacjach korzystania z zasobów teletransmisyjnych różnych operatorów, stosujących różne taryfy,
- maksymalizacja przepływu – istotna przy obsłudze telekonferencji, wideokonferencji oraz usługi VoD – wideo na żądanie,
- inne zależne od wymagań stawianych danej realizacji.

Należy zatem zauważyć, że we współczesnych sieciach teleinformatycznych, niezależnie od ich rozległości terytorialnej (SAN, LAN, MAN, WAN, GAN) kluczowe znaczenie dla ich działania, a co za tym idzie efektywności mają reguły przydziału dostępu do kanału transmisyjnego oraz zasady sterowania ruchem i rezerwacji pasma transmisyjnego.

Wymagania na zarządzanie tymi sieciami można podzielić na pięć obszarów funkcjonalnych, z których każdy stanowi źródło dla jednego lub więcej standardów obejmujących jedną lub więcej funkcji.
Obszarami tymi są:

- zarządzanie i kontrola uszkodzeń – obejmuje zagadnienia dotyczące identyfikowania, diagnozowania oraz szybkiego likwidowania powstających w systemie problemów oraz monitorowanie statusów i alarmów;
- zarządzanie i kontrola konfiguracji – zapewnia możliwość obserwacji i wpływu na konfigurację systemu i składających się na niego urządzeń z centralnego punktu kontrolnego;
- zarządzanie i kontrola rozliczeń – umożliwia dostarczenie operatorowi systemu, informacji o wykorzystaniu systemu oraz zapewnia rozliczenie z użytkownikami;
- zarządzanie i kontrola wydajności (sprawności) – umożliwia optymalizację wydajności systemu poprzez gromadzenie i analizę danych o sprawności urządzeń;
- zarządzanie bezpieczeństwem; i ochronę przed nieautoryzowanym dostępem i oddziaływaniem.

1. Proces eksploatacji systemów i sieci telekomunikacyjnych

Eksploatacja techniczna jest rozumiana jako całokształt współdziałania człowieka z systemem i obejmuje procesy zarządzania i utrzymania.

Zarządzanie systemu telekomunikacyjnego ma za zadanie maksymalizację zysku jaki daje jego eksploatacja, w okresie centralnego sterowania gospodarką mówiliśmy o maksymalizacji zaspokojenia potrzeb społecznych, są to pojęcia podobne jednak tylko do pewnego stopnia.

Utrzymanie techniczne systemu ma za zadanie zapewnienie parametrów użytkowych systemu co najmniej równych wymaganiom, w całym okresie eksploatacji.

Zagadnienia utrzymania i zarządzania są ściśle powiązane z niezawodnością systemu oraz niezawodnością wszystkich jego elementów.

Funkcje eksploatacyjne obejmują podsystemy:

- wspomagania operatora,
- lokalizację uszkodzeń (diagnostykę),
- zabezpieczenia rozprzestrzeniania się skutków uszkodzeń,
- nadzór nad sprzętem i oprogramowaniem systemu telekomunikacyjnego,
- nadzór nad jakością załatwiania ruchu telekomunikacyjnego.

Środki eksploatacji systemu telekomunikacyjnego są zlokalizowane w poszczególnych obiektach (lokalne) różnych stopni hierarchii obowiązującej w telekomunikacji oraz w specjalnych centrach eksploatacyjnych.

1.1. Eksploatacja a zarządzanie systemem telekomunikacyjnym

Potrzeby racjonalizacji zarządzania systemami telekomunikacyjnymi wynikają między innymi z faktu dużej liczby abonentów z sensie globalnym (kilkaset milionów abonentów), budowy central o bardzo dużych pojemnościach (nawet do kilkuset tysięcy abonentów) oraz z budowy systemów transmisyjnych o bardzo dużych krotnościach. Jednocześnie rozwój urządzeń telekomunikacyjnych oraz rozwój informatyki stwarza realne możliwości budowy specjalnych systemów zarządzania centralnego telekomunikacją obejmujących znaczne obszary geograficzne. Od kilkunastu lat obserwujemy tendencje do decentralizacji a nawet rozpraszania systemów komutacyjnych natomiast systemy zarządzania są raczej centralizowane i znajdują się na szczycie hierarchii w sieci.

Rysunek 1 Zarządzanie i utrzymanie w hierarchii systemu telekomunikacyjnego

Centra zarządzania i utrzymania systemu telekomunikacyjnego zlokalizowane są na poziomie stref numeracyjnych dla ruchu lokalnego, dla ruchu międzymiastowego i międzynarodowego na poziomie centrali międzynarodowej. Ośrodki te powinny być miejscem pracy inżynierów ruchu, reprezentowanych przez dyżurnych dyspozytorów, odpowiedzialnych za określone zadania.

Podstawowe czynności operatora systemu telekomunikacyjnego związane z zarządzaniem to:

- modyfikacje funkcjonalne,
- administrowanie abonenckimi zespołami przyłączeniowymi,
- kierowanie ruchem międzycentralowym
- operacje taryfikacyjne,
- obserwacje i pomiary ruchu telekomunikacyjnego,
- zarządanie łączami międzycentralowymi
- zabiegi mające na celu ograniczenie liczby zgłoszeń niekończących się rozmową,
- archiwizacja wszystkich czynności operatorskich.

1.1.1 Modyfikacje funkcjonalne

Modyfikacje funkcjonalne mają zadanie dostosowanie systemu do aktualnych potrzeb i w nowoczesnym systemie polegają na:

- zmianach zawartości pamięci przeliczeń,
- modyfikacjach oprogramowania związanych ze zmianami w sieci wielocentralowej,
- modyfikacjach oprogramowania związanych z rozbudową centrali bądź sieci,

- modyfikacjach oprogramowania związanych z wprowadzaniem nowych wersji.

Tylko w przypadku bardzo małych central abonenckich możliwe jest ich wyłączenie z ruchu dla wprowadzenia modyfikacji, mówimy wtedy o modyfikacji w trybie "off-line". W pozostałych centralach modyfikacje powinny być wprowadzane bez wyłączania ich z ruchu, w trybie "on-line". Jednak nie zawsze jest to możliwe, zwłaszcza w przypadku poważnych zmian, dlatego zwykle poszczególne administracje dopuszczają możliwość krótkotrwałych wyłączeń w czasie małego ruchu np. w godzinach nocnych, dla wprowadzenie nowej wersji oprogramowania. Polskie wymagania dopuszczają przerwy w pracy centrali w celu modyfikacji (planowe wyłączenia) krótsze od 10 min.

Niezwykle ważnym zagadnieniem ze względu na ciągłość pracy systemu jest zabezpieczenie przed wprowadzaniem błędów w modyfikacjach. Teoretycznie istnieją dwie zasadnicze metody zabezpieczenia.

- Pierwsza **korekcyjna** - polegająca na tym, że system sam podejmuje akcję zmierzającą do przywrócenia sprawności funkcjonalnej w razie wystąpienia błędów w modyfikacji.
- Druga **prewencyjna** - polega na tym, że system nie dopuszcza do przeprowadzenia błędnej modyfikacji.

Trzeba jednak obie metody są tylko w takim stopniu skuteczne w jakim projektant jest w stanie przewidzieć wprowadzane błędy. W praktyce metoda korekcyjna jeszcze nie jest stosowana. Metoda prewencyjna jest stosowana powszechnie jednak trzeba stwierdzić, że jej działanie jest również dość dalekie od doskonałości.

Większe modyfikacje są opracowywane w specjalistycznych pracowniach projektowania oprogramowania zlokalizowanych zwykle bezpośrednio u producenta. pracownie te są wyposażone w makiety central przeznaczonych do testowania opracowanego oprogramowania. Ponieważ małe zmiany są wprowadzane bezpośrednio w centrali, producent może nie znać aktualnej konfiguracji, dlatego algorytm wprowadzania większych modyfikacji funkcjonalnych rozpoczyna się od zczytania aktualnej wersji oprogramowania, przeniesienia jej do pracowni projektowej dokonania modyfikacji, przeprowadzeniu wyczerpującego testowania i ponownego zapisu w pamięci centrali. Algorytm ten kończy się wprowadzeniem do nowej wersji oprogramowania zmian, które zostały wprowadzone do centrali w czasie opracowywania oprogramowania.

Niektórzy producenci oferują nowe wersje oprogramowania (bardziej efektywne, z mniejszą liczbą błędów) co 6 miesięcy. Programy te często zwłaszcza do małych centrów komutacji np. koncentratorów są ładowane zdalnie w godzinach bardzo małego ruchu np. w nocy.

Niezależnie od zapobiegania błędnym modyfikacjom w każdym systemie istnieją zabezpieczenia przed dostępem do oprogramowania osób niepowołanych. Na przykład definiuje się trzy poziomy dostępu:

- pierwszy związany z dostępem do systemu, jest stworzony przez zastosowanie identyfikatorów użytkowników i haseł dostępu,
- drugi poziom to ograniczenie listy komend dla każdego użytkownika,
- trzeci poziom to zadeklarowanie dostępu do określonych elementów sieciowych lub też obszarów sieci.

1.1.2 Administrowanie urządzeniami abonenckimi

W zakres administrowania urządzeniami abonenckimi wchodzą:

- przyporządkowanie łączom abonenckim zespołów przyłączeniowych,
- przyporządkowanie abonentom określonych uprawnień.

W nowoczesnych centralach o sterowaniu programowanym wyposażonym w pamięć przeliczeń, numer katalogowy oraz fizyczny numer zespołu przyłączeniowego mogą być różne. Przyporządkowanie ich jest zawarte w pamięci przeliczeń. W czasie życia centrali, (minimum 30 lat), przyporządkowania te ulegają wielokrotnym zmianom, spowodowanym zmianami strukturalnymi sieci oraz ruchem abonentów. Ponadto zmiana zawartości pamięci przeliczeń wykorzystywana jest przy wprowadzania aktualnych uprawnień abonentów. Większość usług dodatkowych takich jak przenoszenie wywołań czy ograniczenie dostępu jest udostępnianych abonentom po ich zaabonowaniu, co od strony technicznej polega na prowadzeniu odpowiednich danych do pamięci przeliczeń. Te modyfikacje dokonywane są przez operatora systemu (pracownika TP S.A.) Również realizacja niektórych usług np. wybieranie skrócone wymagają dostępu uprawnionych abonentów do pamięci przeliczeń.

1.1.3 Kierowanie ruchem międzycentralowym

Kierowanie ruchem międzycentralowym, gdy ruch telekomunikacyjny wzrasta powyżej możliwości przepustowej w określonych relacjach, ogólna sprawność załatwiania ruchu obniża się, co jest odbierane negatywnie przez abonentów a ponadto powoduje obniżenie zysków operatora.

Wzrost ruchu może być chwilowy i wynikać np. z nadzwyczajnych sytuacji społecznych, politycznych lub innych, ale może również może wynikać ze stałych tendencji rozwojowych np rozwój określonych dzielnic, miast itp.

Łatwo można wyspecyfikować sytuacje wywołujące zaburzenia w sieci telekomunikacyjnej:

- uszkodzenia systemów teletransmisyjnych,

- uszkodzenia systemów komutacyjnych,
- planowane wyłączenia urządzeń teletransmisyjnych,
- nienormalny ruch telefoniczny wywołany np. przez:
  - święta narodowe lub religijne,
  - wielkie imprezy sportowe,
  - kryzysy polityczne,
  - katastrofy itp.
- trudności z zaspokojeniem bieżących potrzeb ruchowych.

Kierowanie ruchem międzycentralowym powinno zapewnić środki minimalizacji obniżenia sprawności obsługi. Te środki to procedury kierowania ruchu międzycentralowego. Kierowanie ruchu międzycentralowego polega na wyznaczaniu odpowiednich dróg kolejnego wyboru. Drogi te są również zapisane w pamięci przeliczeń. W sytuacji trwałych tendencji ruchowych występuje konieczność zmian zapisów w tablicach kierowania ruchu, a nawet wnioskowania o przeprowadzenie określonych inwestycji sieciowych bądź komutacyjnych. Kierowanie ruchem może polegać na:

- bieżącej zmianie zawartości tablic kierowania ruchu,
- blokowaniu określonej części wywołań w określonym kierunku (według wskaźnika międzymiastowego lub nawet prefiksu),
- zezwolenie na ruch o intensywności np. jednego połączenia na sekundę w określonym kierunku,
- blokowanie dróg alternatywnych dla wywołań kierowanych do określonego węzła docelowego,
- blokowanie wywołań przelewanych z danej wiązki, a kierowanych do określonego węzła przeznaczenia,
- określanie wielkości ruchu z danej wiązki pierwszego wyboru, który może być kierowany na drogę alternatywną.

W systemach zarządzania stosowane są dwa podejścia:

- ręczne kierowanie ruchu międzycentralowego,
- półautomatyczne kierowanie ruchu międzycentralowego.

Ręczne kierowanie ruchem wymaga podejmowania na bieżąco decyzji przez operatora - dyspozytora. Natomiast w półautomatycznym sposobie kierowania ruchem operator dyspozytor może przygotować przewidywane warianty kierowania i przypadkach obniżenia sprawności załatwiania ruchu wybiera właściwy.

Zarządzanie ruchem międzycentralowym daje podstawowe korzyści:

- ograniczenie przeciążenia zapobiega jego rozprzestrzenianiu się,
- wzrost przychodów operatora, wynikający ze wzrostu liczby załatwionych zgłoszeń,
- lepsza obsługa abonentów,
- stymulacje ruchu abonenckiego,
- wzrastająca akceptacja abonentów dla nowych usług
- bardziej wiarygodne informacje wyjściowe do planowania sieci i innych inwestycji telekomunikacyjnych,
- wzrost świadomości operatora o statusie i stanie systemu.

Z kierowaniem ruchem związane jest zagadnienie ochrony systemu przed przeciążeniem. Ruch telekomunikacyjny ma tę właściwość, że zgłoszenia nie załatwione, a szczególnie załatwione niewłaściwie np. z powodu przeciążenia wracają do systemu powodując jego dalsze przeciążenie. Dlatego system telekomunikacyjny powinien mieć wbudowany mechanizm ograniczający to zjawisko.

1.1.4 Operacje taryfikacyjne

W początkowym okresie rozwoju telefonii abonenci uiszczali opłatę za korzystanie z telefonu w formie zryczałtowanej, w postaci abonamentu.

W związku z dużą wartością świadczonych usług zachodzi potrzeba uwiarygodnienia rachunku telefonicznego. Już w latach sześćdziesiątych wprowadzono w Stanach Zjednoczonych pełny zapis informacji o przeprowadzanych rozmowach (billing), w Europie zasada ta została wprowadzona znacznie później.

Obecnie stosowane są równolegle dwie zasady taryfikacji (zaliczania) rozmów telefonicznych:

-za pomocą okresowych impulsów,

-z zastosowaniem billingowych rejestrów programowych.

Pierwsza metoda jest stosowana przy współpracy z aparatami wrzutowymi, z abonentami wyposażonymi w aparaty telefoniczne z licznikami kontrolnymi czy z centrali abonenckimi, które prowadzą wewnętrzny system rozliczeń między abonentami. Metoda ta polega na przesyłaniu do abonenta okresowych impulsów o częstotliwości 16 kHz. (na świecie stosowane są również częstotliwości 50 Hz i 12 kHz). Centrale telefoniczne mają określone częstotliwości graniczne impulsów.

Druga polega najczęściej na oderwaniu procesu taryfikacji od procesu i sprzętu komutacji. Dane o każdym połączeniu są rejestrowane w procesie komutacji w postaci tzw. rekordów zaliczeniowych.

Na ogół rekord zaliczeniowy zawiera następujące dane:

-numer krajowy abonenta A,

-kategorię abonenta A,

-numer abonenta B,

-datę realizacji połączenia; rok, miesiąc i dzień,

-czas zgłoszenia się abonenta B: godzina, minuty i sekundy,

-czas trwania rozmowy w sekundach.

Co określony czas dane z rejestrów billingowych są przepisywane do zewnętrznej pamięci masowej np. taśmowej. Taśma magnetyczna z zapisanymi rekordami zaliczeniowymi jest przenoszona do ośrodka prowadzącego taryfikację, gdzie na podstawie zapisanych rekordów zostaje określona wysokość opłaty. Program traryfikacyjny ustala wysokość opłaty przy uwzględnieniu następujących czynników:

-kategorii abonenta A,

-dnia tygodnia,

-godziny dnia,

-typu połączenia,

-pełnego numeru abonenta B (wskaźnik kraju i strefy).

W wielu miejscach sieci pojawia się problem taryfikacji rozmów dla celów rozliczeń między operatorami. Problem ten jest analogiczny do problemu taryfikacji abonenckiej.

1.1.5 Obserwacje i pomiary ruchu telekomunikacyjnego (monitorowanie ruchu)

System monitorowania ruchu powinien być integralną częścią centrali, dane dostarczone przez niego są podstawą do podejmowania decyzji o kierowaniu ruchu. System monitorowania ruchu dostarcza informacji o parametrach eksploatacyjnych centrali, o poziomie świadczonych usług, stopniu obciążenia poszczególnych urządzeń komutacyjnych. Proces monitorowania ruchu możemy podzielić zwykle na trzy fazy:

- **zbierania danych** (śledzenie) - dane dotyczące obciążeń oraz zdarzeń poszczególnych zespołów centrali gromadzone są na bieżąco w rozproszonej bazie danych np związanej z określonym zespołem,
- **rejestrowanie** - stosownie do życzenia operatora dane te są przepisywane do zewnętrznych pamięci masowych, ze względów praktycznych (ogromne ilości danych) operator określa w sposób rejestracje danych w sposób selektywny, również częstotliwość rejestracji jest określona przez operatora (np. co 5 min),

- **analiza** - zarejestrowane dane są podstawą do opracowania okresowych raportów, pozwalających na wnioskowanie o stanie centrali, np. rozkład wywołań, przeciążenia, wykorzystanie łączy w określonych kierunkach itp.

Dwie pierwsze fazy muszą być z definicji realizowane wewnątrz systemu, natomiast faza trzecia może być realizowana poza systemem.

Pomiary realizowane przez system możemy podzielić na pomiary:

- pomiary czasu trwania określonych stanów,
- zdarzeń oraz
- pomiary ruchu.

Pomiary czasu trwania określonych stanów odnoszą się np. do nadmiernych opóźnień przy załatwianiu zgłoszeń, czasu trwania stanów blokady czy czasów zajętości poszczególnych zespołów.

Pomiary zdarzeń obejmują zliczanie wywołań w poszczególnych kategoriach tj. wywołania przychodzące, wychodzące, tranzytowe, wywołania zwykłe, PABX, do służb specjalnych itp. Ponadto mogą obejmować liczbę zgłoszeń załatwionych, liczby wszystkich nieprawidłowości,

Pomiary ruchu obejmują pomiary obciążeń poszczególnych łączy, kierunków i zespołów.

Wyniki pomiarów zapisywane są w pamięci masowej i opracowywane w sposób programowy (trzecia faza), wewnątrz systemu lub poza nim, wyprowadzane w postaci raportów ruchowych na wyznaczonym do tego celu terminalu, np. okresowych obejmujących godzinę największego ruchu, nadzwyczajnych wyprowadzanych w sytuacjach spadku sprawności usługowej, czy na żądanie personelu .

1.1.6 Zabiegi mające na celu ograniczenie liczby zgłoszeń niekończących się rozmową

Zgłoszenia nie kończące się rozmową obciążają zespoły centrali ruchem, za który abonenci nie płacą, ponadto zgłoszenia nie zakończone rozmową powodują, że subiektywna ocena jakości pracy centrali jest zaniżona. Całkowicie ruchu jałowego nie można uniknąć gdyż leży on w naturze ruchu telekomunikacyjnego (abonent może być zajęty lub nieobecny), ale należy go w maksymalnym stopniu ograniczyć. W znacznym stopniu ruch jałowy można

ograniczyć przez szersze wprowadzenie komunikatów słownych dołączanych do wszystkich łączy niewykorzystywanych, do łączy abonenckich uszkodzonych, wyłączonych czasowo itp. Jeżeli abonent A po wybraniu numeru usłyszy w miarę dokładną informację o przyczynach niemożliwości zrealizowania połączenia, nie będzie ponawiał kilkakrotnie a nawet kilkunastokrotnie prób uzyskania połączenia.

Ponadto wprowadzenie niektórych typów usług np. możliwości "zamawiania" połączenia z abonentem zajętym, poczta głosowa może w znacznym stopniu ograniczyć ruch jałowy. Jeżeli abonentowi bardzo zależy na uzyskaniu połączeniu z abonentem stale zajętym, to będzie wolał uzyskać je na pewno bezpośrednio po jego zwolnieniu za dodatkową opłatą niż wielokrotnie ponawiać próby uzyskania połączenia. Dla operatora systemu zysk jest podwójny a nawet potrójny, uzyskuje dodatkowe przychody, maleje ruch jałowy i co jest nie bez znaczenia poprawia się obraz operatora w odczuciu abonentów.

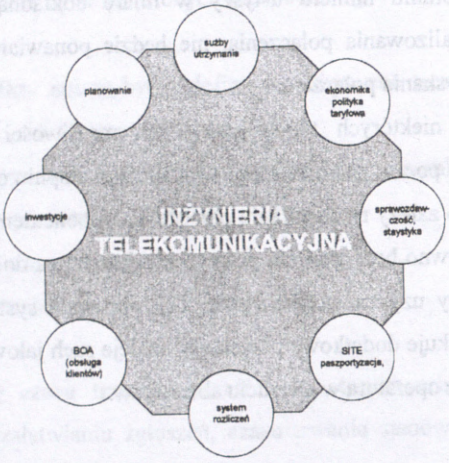
1.1.7 Archiwizacja czynności operatorskich

Zwykle do określonych czynności utrzymaniowych ma dostęp więcej niż jeden pracownik, wynika to z potrzeb organizacyjnych operatora jak również z oczywistego faktu, że posiadający wyższą kategorię uprawnień może wykonać czynności z zakresu niższych uprawnień. W rezultacie określona czynność może mieć wielu "autorów", co w przypadku wprowadzenia błędu do systemu może powodować trudności w ustaleniu "sprawcy" strat spowodowanych tym błędem. Dlatego prowadzona jest pełna archiwizacja wszystkich czynności operatorskich obejmująca zwykle:

- datę operacji,
- godzinę operacji,
- czynność operatorską,
- kod osoby wykonującej czynność.

Niektóre administracje telekomunikacyjne wprowadzają surowe kary za wprowadzenie poważnych błędów operatorskich łącznie ze zwolnieniem z pracy.

Systemy zarządzania realizują zadania z zakresu inżynierii telekomunikacyjnej.



Rysunek 2 Obszary inżynierii telekomunikacyjnej

2. Charakterystyka zadań, struktur i cech systemów zarządzania i utrzymania sieci

2.1. Uwagi wstępne

Zarządzanie telekomunikacją działalność związana z:

- planowaniem,
- organizowaniem,
- sterowaniem,
- kontrolowaniem

zasobów sieci i pracy personelu obsługującego, która ma na celu optymalne wykorzystanie zasobów systemu telekomunikacyjnego, czyli świadczenie usług możliwie najwyższej jakości, ponosząc przy tym możliwie najniższe koszty.

W oparciu o dokumenty standaryzacyjne definiujące zarządzanie w telekomunikacji można przedstawić następujące określenia tego pojęcia:

1. *Definicja wg. ISO (OSI) norma ISO 7498-4*

   Środki sterowania, koordynowania i monitorowania zasobów umożliwiające realizację łączności w środowisku OSI.

2. *Definicja wg. ITU-T (E.410)*

   Funkcje nadzorowania sieci i podejmowanie, gdy jest to niezbędne, działań sterujących ruchem telekomunikacyjnym.

3. *Definicja wg. ITU-T (M.3010)*

   Planowanie, dostarczanie, instalowanie, utrzymanie, eksploatacja i administrowanie sieciami i usługami

4. *Definicja wg. Programu RACE (CSF A150)*

   Zbiór funkcji zaprojektowanych w celu osiągnięcia maksymalnych korzyści z eksploatacji sieci i usług telekomunikacyjnych.

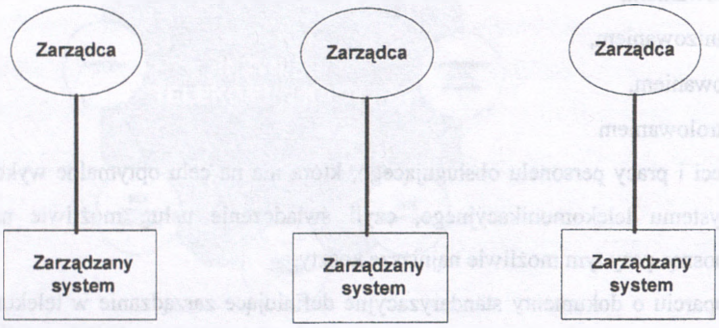
   Zarządzanie siecią obejmuje administrowanie abonentami i siecią oraz zarządzanie jakością obsługi (włączając w to rekonfigurację systemu)

Wyróżnia się następujące strategie zarządzania w telekomunikacji i teleinformatyce:

- zarządzanie pionowe,
- zarządzanie scentralizowane,
- zarzadzanie hierarchiczne,
- zarządzanie zdecentralozowane,
- zarządzanie kooperacyjne.

Zarządzanie pionowe cechuje:

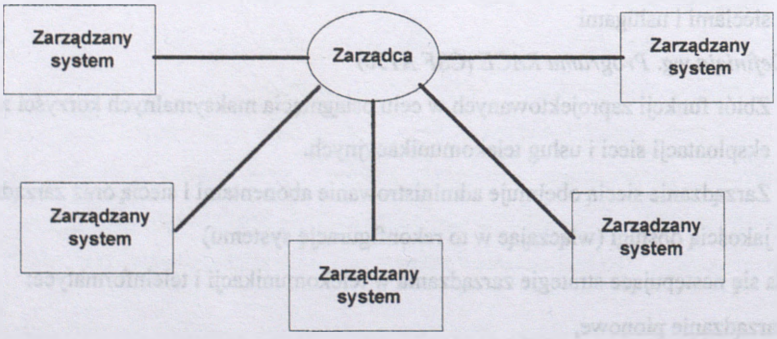
- przestarzałość,
- łatwość realizacyjna,
- trudność w rozwijaniu,
- brak perspektywy globalnej.



Rysunek 3 Zarządzanie pionowe

Zarządzanie scentralizowane cechuje:

- minimalizacja personelu
- skoncentrowanie wiedzy (ekspertyzy),
- uzyskanie perspektywy globalnej,
- możliwość realizacji wyższych (niż elementowa),warstw zarządzania,
- wymaganie przesyłania standardowych informacji.

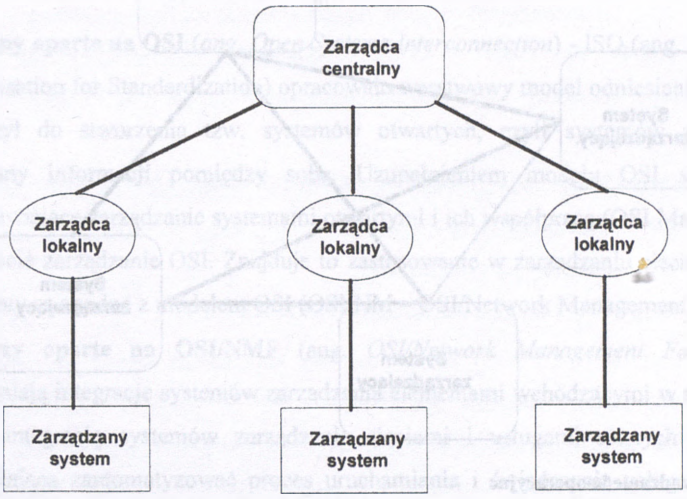


Rysunek 4 Zarządzanie scentralizowane

Zarządzanie hierarchiczne cechuje:

- powszechność aktualnego zastosowania,
- dziedziczenie cech modelu „pionowego",

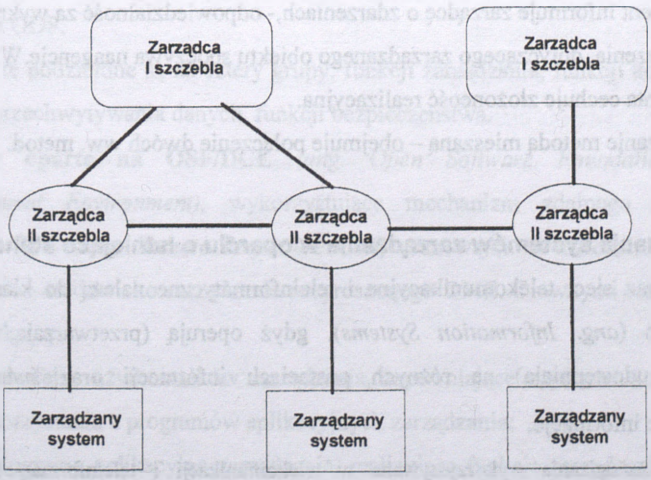
- umożliwianie realizacji globalnej perspektywy zarządzania,
- możliwość realizacji wyższych (niż elementowa) warstw zarządzania,
- wymaganie przesyłania standardowych informacji.



Rysunek 5 Zarządzanie hierarchiczne

Zarządzanie zdecentralizowane cechuje:

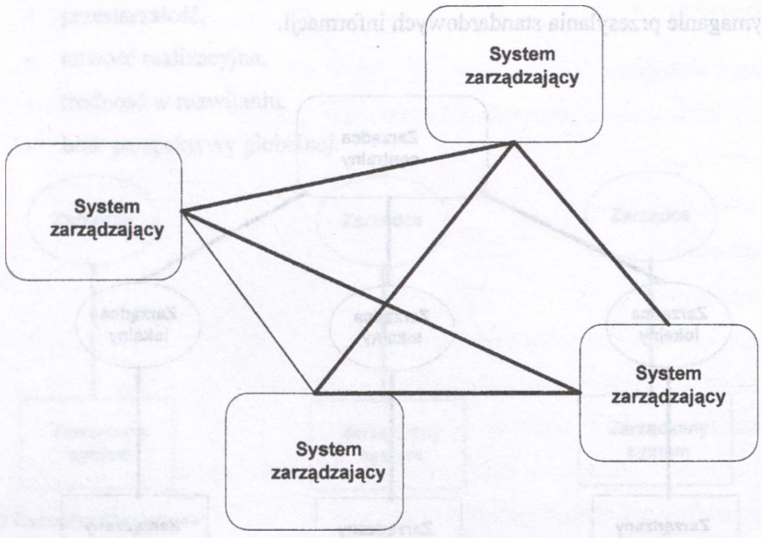
- dzielenie odpowiedzialności,
- brak punktu centralnego,
- potencjalnia odporność na uszkodzenia



Rysunek 6 Zarządzanie zdecentralizowane

Zarządzanie kooperacyjne cechuje:

- możliwość samozarządzania,
- rozproszenie odpowiedzialności.



Rysunek 7 Zarządzanie kooperacyjne

Wyróżnia się następujące mechanizmy zbierania informacji w systemach zarządzania

1. Zarządzanie przez przepytywanie, które przebiega w następujący sposób:
   - - zarządca wysyła zapytania do agentów (przepytywanie)- odpowiedzialność za wykrycie zdarzenia dotyczącego zarządzanego obiektu spoczywa na zarządcy.W tym przypadku agenta cechuje duża prostota realizacyjna.
2. Zarządzanie przez zgłaszanie zdarzeń, które przebiega w następujący sposób:
   - - agent informuje zarządcę o zdarzeniach,- odpowiedzialność za wykrycie zdarzenia, dotyczącego zarządzanego obiektu spoczywa naagencie.W tym przypadku agenta cechuje złożoneość realizacyjna.
3. Zarządzanie metodą mieszaną – obejmuje połączenie dwóch ww. metod.

2.2. Klasyfikacja systemów zarządzania w oparciu o istniejące standardy

Systemy oraz sieci telekomunikacyjne i teleinformatyczne należą do klasy systemów informacyjnych (*ang. Information Systems*), gdyż operują (przetwarzają, wymieniają, przechowują, udostępniają) na różnych postaciach informacji oraz świadczą usługi wykorzystujące informacje.

Systemy zarządzania wykorzystywane w telekomunikacji i teleinformatyce również są systemami informacyjnymi (operują na informacjach związanych z zarządzanymi zasobami, użytkownikami i usługami), ponadto można je zakwalifikować do klasy systemów wspomagania

decyzyjnego (*ang. Decision Support Systems).*

Aktualnie istniejące i opracowywane systemu zarządzania systemami i sieciami telekomunikacyjnymi i teleinformatycznymi oraz usługami, które one oferują realizowane są w oparciu o następujące technologie:

- **Systemy oparte na OSI** (*ang, Open Systems Interconnection*) - ISO (ang. International Organisation for Standardization) opracowało warstwowy model odniesienia OSI, który posłużył do stworzenia tzw. systemów otwartych, czyli systemów zdolnych do wymiany informacji pomiędzy sobą. Uzupełnieniem modelu OSI są standardy umożliwiające zarządzanie systemami otwartymi i ich współpracą (OSI Management) – w skrócie zarządzanie OSI. Znajduje to zastosowanie w zarządzaniu sieciami, których elementy są zgodne z modelem OSI (OSI/NM – OSI/Network Management).
- **Systemy oparte na OSI/NMF** (ang. *OSI/Network Management Forum*), które zapewniają integrację systemów zarządzania elementami wchodzącymi w skład sieci, a także integrację systemów zarządzania sieciami i usługami różnych operatorów, pozwalająca zautomatyzować proces uruchamiania i świadczenia usług. Oznacza to szybszy i pełniejszy dostęp do informacji o elementach zarządzanej sieci, a tym samym możliwości pełniejszego wykorzystania zasobów sieci, obniżenia kosztów eksploatacji i zapewnienia dostępu do sieci.
- **Systemy oparte o ODP** *(ang. Open Distributed Processing).*
  Standard opracowany przez ISO i ITU i ujęty w dokumentach ISO 10746, ITU – X.900 jest opisem funkcji realizowanych w oparciu o przetwarzanie rozproszone przez system zgodny z ODP.
  Funkcje te podzielone są na cztery grupy: funkcji zarządzania, funkcji koordynowania, funkcji przechwytywania danych, funkcji bezpieczeństwa.
- **Systemy oparte na OSF/DCE** *(ang. Open Software Foundation/Distributed Management Environment),* wykorzystujące mechanizm zdalnego wywoływania procedur RPC (*ang. Remote Procedure Call*) oraz wątki. W dziedzinie zarządzania opracowano środowisko zarządzania rozproszonego DME. Głównymi elementami tego środowiska są:
  - interfejsy użytkowników zarządzania, zapewniające użytkownikom możliwość korzystania z programów aplikacyjnych zarządzania;
  - programy aplikacyjne zarządzania, realizujące funkcje zarządzania i mogą być uruchamiane w środowisku DCE;
  - usługi dostępu do zarządzanych obiektów;
  - programy narzędziowe wspomagające projektowanie;

- GUI – graficzne interfejsy użytkownika.

W DME mogą być stosowane protokoły SNMP, CMIP, a także zdalne wywoływanie procedur RPC, zdefiniowane dla środowiska DCE.

- **Systemy oparte na TMN - ITU (International Telecommunication Union)** wykorzystuje standardy ISO, ale wydawane przez niego zalecenia dotyczą m.in. innymi:
  - architektury sieci zarządzania telekomunikacją TMN (Telecommunications Management Network)
  - styków między jej składnikami;
  - oraz usługi i funkcje zarządzania telekomunikacją.

  W systemach opartych na TMN wykorzystuje się model informacji MIM (Management Information Model), protokół CMIP oraz funkcje zarządzania systemami ISO, SMF.
  Klasyfikacja zarządzania w odniesieniu do sieci telekomunikacyjnych, wiąże się z modelem warstwowym zarządzania telekomunikacją, w którym zarządzanie siecią traktowane jest jako jedna z warstw. Zarządzanie w tym modelu można zdefiniować jako tworzenie warunków, w których elementy tworzące sieć mogą świadczyć usługi na rzecz użytkowników tej sieci.
  W podejściu tym wyróżnia się warstwy:
  - zarządzania elementami sieci;
  - zarządzania siecią;
  - zarządzania usługami;
  - zarządzania biznesowego;
- **Systemy oparte na TINA (Telecommunications Information Networking Architecture),** pozwala na elastyczny dostęp do usług telekomunikacyjnych oraz zarządzanie tymi usługami i świadczącą je siecią telekomunikacyjną TINA oparta jest na otwartym standardzie ODP i stanowi próbę integracji telekomunikacji i informatyki.
  Cechy TINA to:
  - modelowanie informacji oparte na notacji GDMO i modelu związków zgodnie z X.725;
  - przetwarzanie rozproszonych programów aplikacyjnych w postaci obiektów obliczeniowych współpracujących przez interfejs operacyjny (przez który mogą

być wydawane polecenia wykonania operacji i przesyłane wyniki operacji) lub strumieniowy (przez który przesyłany jest jedynie strumień danych);

- realizowanie modeli rzeczywistych systemów na podstawie modeli obliczeniowych;
- podział funkcji zarządzania między obszary funkcjonalne;
- oparty na modelu OSI zarządca-agent;
- oparty o architekturę funkcjonalną TMN.

W związku z ww. podziałem tym wytwórcy oprogramowania systemów zarządzania opracowali własne platformy, które cechuje wzajemne przenikanie omówionych wcześniej architektur.

Należą do nich:

OpenView otwarty system zarządzania stworzony przez firmę HP. Podstawą systemu jest szkielet zarządzania, definiuje on środowisko pracy aplikacji zarządzających. Szkielet zarządzania jest implementacją architektury Open View Management Architecture na podstawie której tworzone są zorientowane obiektowo aplikacje zarządzania siecią. Architektura ta jest zgodna z modelem OSI i ma następujące właściwości:

- protokół komunikacyjny TCP/IP;
- protokół zarządzania SNMP;
- protokoły CMIP dla sieci heterogenicznych;
- zgodność z technologią DME.

ONA - (Open Network Architecture), model architektury stworzony przez IBM. Oparty jest na rozwiązaniu otwartej architektury sieciowej, która stanowi szkielet ogólnej architektury zarządzania sieci.

2.3. Funkcje zarządzania systemami otwartymi OSI

Funkcje zarządzania systemami zdefiniowano w standardzie dotyczącym zarządzania OSI (ISO 10164, ITU – X.730 i kolejne). Dotyczą one zarządzania systemami komputerowymi i teleinformatycznymi. Funkcje zarządzania systemami zamieszczono poniżej:

- funkcja zarządzania obiektami – zarządzanie obiektami dotyczy tworzenia i usuwania obiektów, czyli zasobów sieci, modyfikowania wartości ich atrybutów, wydawania obiektom poleceń wykonywania akcji oraz przesyłania przez obiekty meldunków;

- funkcja zarządzania stanem – zarządzanie stanem polega na monitorowaniu i modyfikowaniu bieżącego stanu obiektów i przesyłaniu meldunków dotyczących jego zmian;
- funkcja zarządzania związkiem – zarządzanie związkiem, służy określeniu związków między obiektami oraz ich wzajemnego wpływu;
- funkcja zgłaszania alarmów – zgłaszanie alarmów służy do przesyłania meldunków o niepoprawnym funkcjonowaniu meldunków o niepoprawnym funkcjonowaniu obiektów;
- funkcja zarządzania zgłoszeniami zdarzeń – zarządzanie zgłoszeniami zdarzeń polega na nadzorowaniu procesu rozsyłania zgłoszeń zdarzeń do ich adresatów;
- funkcja nadzorowania dzienników – nadzorowanie dzienników określa jak prowadzić dzienniki w których przechowuje się informacje o zdarzeniach i o operacjach przeprowadzanych na zarządzanych obiektach;
- funkcja zgłaszania alarmów bezpieczeństwa – zgłaszanie alarmów bezpieczeństwa służy do przesyłania alarmów dotyczących bezpieczeństwa obiektów;
- funkcja śladów kontrolnych bezpieczeństwa – polega na przechowywaniu informacji opisujących funkcjonowanie mechanizmów zapewniających bezpieczeństwo obiektów;
- funkcja kontroli dostępu – kontrola dostępu określa zasady dostępu do obiektów oraz zasady nadzorowania, czy meldunki są przesyłane do upoważnionych odbiorców;
- funkcja zbierania danych rozliczeniowych – polega na zbieraniu informacji koniecznych do obliczania kosztów korzystania z zasobów sieci;
- funkcja monitorowania obciążenia – monitorowanie obciążenia polega na dokonywaniu pomiarów parametrów związanych z obciążeniem zarządzanych zasobów;
- funkcja zarządzania testami – zarządzanie testami określa zasady przeprowadzania testów diagnostycznych;
- funkcja podsumowań – podsumowanie polega na zbieraniu danych i przedstawianiu wyników obliczeń statystycznych;
- funkcja tworzenia harmonogramów – tworzenie harmonogramów umożliwia planowanie działań dotyczących zarządzania;

Systemy otwarte definiowane są przez firmy, konsorcja firm, instytucje rządowe oraz międzynarodowe organizacje standaryzacji. Kontrolują one specyfikacje, lecz przy jej definiowaniu współpracują z różnymi firmami i użytkownikami.

Wymagania rynku powodują przesunięcie w kierunku całkowitej otwartości i większej akceptacji istniejących standardów. Protokoły stos protokołów TCP/IP jest na pewno bardziej

popularny niż OSI (Open Systems Interconnections), ponieważ są podstawowymi produktami stosowanymi w Internecie, ponadto wiele firm zapewnia obsługę TCP/IP, a tylko niektóre OSI.

Narzędzia zarządzania powinny według OSI spełniać następujące wymagania użytkowników dotyczące:

- działania, które zarządcom sieci komputerowych umożliwią: planowanie, organizację, nadzór, sterowanie i rozliczenie za używanie usług współdziałania systemów;
- zdolności do reakcji na zmniejszające się wymagania;
- udogodnień do zapewnienia przewidywanego zachowania komunikacyjnego;
- udogodnień gwarantujących ochronę informacji oraz legalizację źródeł i miejsc przeznaczenia przesyłanych danych

Otwarty system zarządzania wykorzystuje podejścia architektury platformy, w którym platforma zaprojektowana jest tak, aby obsłużyć wszystkie funkcje wymagane przez system zarządzania siecią. Te funkcje to: interfejsy protokołu komunikacyjnego, definicje danych i inne możliwości zawiązane z zarządzaniem.

Obecnie wymagania rynku kierowane są w stronę produktów zapewniających jednolity zintegrowany, bądź rozproszony system zarządzania sieciami teleinformatycznymi, systemami i usługami IT. Wykorzystując architekturę rozproszoną, środowisko zarządzania staje się bardziej skalowalne, gdyż w miarę rozrostu sieci można bez przeszkód dodawać nowe elementy aplikacji zarządzania siecią. Architektura rozproszona pozwala również na natychmiastowe przejęcie funkcji jednego lub kilku serwerów bądź klientów, przez inny, co zwiększa niezawodność zarządzania.

Dostępnych jest wiele produktów służących do zarządzania w systemach otwartych, produkty te mają budowę warstwową. Fundamentem jest system operacyjny. Systemy operacyjne stosowane w stacjach zarządzania to systemy typu unixowego: UNIX SCO, Solaris, AIX, oraz systemy: Windows 9x, Windows NT.
Następnie jest platforma do zarządzania.

Platformy zarządzające – są wyspecjalizowanymi narzędziami programowymi do śledzenia i zarządzania systemami teleinformatycznymi, informatycznymi. Wykorzystują jeden z protokołów zarządzania siecią SNMP lub CMIP celem zebrania informacji dotyczących konfiguracji urządzeń zainstalowanych w sieci, a tym samym ustalenia

konfiguracji sieci, przeciążeń segmentów sieciowych bądź przystosowania tych urządzeń do pracy. Platformy można podzielić na dwie kategorie: oparte na systemach unixowych i na Windows. Wybór odpowiedniej platformy zarządzającej jest zależny od oprogramowania systemowego, infrastrukturą sieci, ilością urządzeń oraz sposobem obsługi stanów awaryjnych.

Pakiety zarządzania systemami otwartymi powinny mieć następujące główne cechy:

- **monitorowanie systemu** - agent uruchamia programy monitorujące, które za pośrednictwem mechanizmu systemu oraz zmiennych MIB i protokołu zarządzającego sprawdzają parametry systemu. Powinno być zapewnione okresowe sprawdzanie przekroczenia poziomów krytycznych dla ważnych parametrów systemowych. Ponadto system zarządzania automatycznie reaguje na zajście określonych warunków i powiadamia operatorów centralnej stacji zarządzania.
- **monitorowanie aplikacji** – dostępne powinny być specjalizowane moduły zawierające bazę wiedzy na temat danej aplikacji. Moduły zintegrowane są z agentami, korzystają ze struktury komunikacji, bezpieczeństwa i obsługi zdarzeń. Moduły monitorują nie tylko aplikację pod kątem jej popranej pracy, wydajności, ale również mają wbudowane mechanizmy naprawcze dla zarządzanych aplikacji.
- **badanie dostępności** - centralna stacja zarządzania przepytuje systemy, gdzie działają agenci, sprawdzając, czy agenci są nadal dostępni.
- **bezpieczną komunikację manager – agent**: zapewniającą bezpieczną komunikację między systemem zarządzanym a stacją zarządzania.
- **skalowalność** – system powinien pracować w największych jak i małych środowiskach. Umożliwiać stworzenie hierarchicznej struktury zarządzania, delegację uprawnień i stworzenie centrów kompetencyjnych umożliwiając tym samym możliwie najszybsze i najbardziej efektywne rozwiązywanie problemów, a także działanie proaktywne (zapobieganie problemom w przyszłości).
- bazować na pięciu funkcjach zarządzania według ISO;

Ponadto pakiety zarządzania środowiskami otwartymi powinny, umożliwiać wykrywanie wszystkich zasobów zainstalowanych i pracujących w sieci oraz zarządzanie nimi, a ponadto powinny zapewnić:

- wygodny i efektywny interfejs użytkownika;

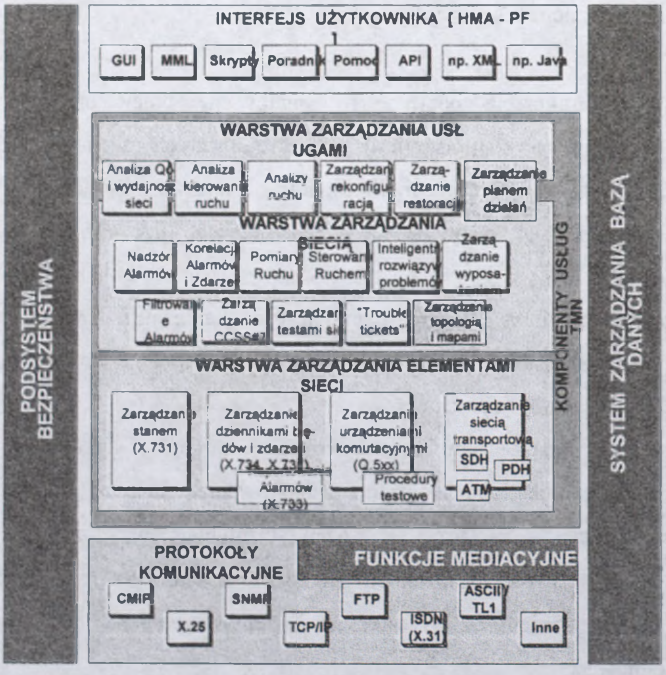
- przepływ informacji zarządzających w czasie rzeczywistym;
- możliwość zmiany konfiguracji i zakresu usług np. na żądanie operatora;
- bezpieczeństwo danych i kontrolowany dostęp do urządzeń i aplikacji zarządzających;
- pełny zestaw narzędzi programowych do analizy stanu zarządzanych elementów, testowania i planowania rozwoju sieci i jej elementów;
- możliwość współpracy z „centralami" innych systemów pracujących według innych protokołów;
- możliwość budowy rozszerzeń programowych i sprzętowych do obsługi sprzętu nietypowego;

Funkcje które powinien realizować otwarty system zarządzania są następujące:

- podstawowe: przesyłanie informacji, pamiętanie informacji, wyszukiwanie informacji, przetwarzanie informacji, ochrona informacji.
- aplikacyjne:
  - zarządzanie konfiguracją pozwala na inicjowanie pracy urządzeń oraz na wspomaganiu pracy administratora w zakresie uruchamiania poszczególnych urządzeń, tworzenie wymaganej konfiguracji systemu, rozbudowy i redukcji, definiowania warunków początkowych dla urządzeń jak również instalowania programów;
  - przygotowanie do funkcjonowania obejmujące działania niezbędne do zapewnienia stanu gotowości systemu do pracy między innymi poprzez kontrolowanie stanu urządzeń oraz wybranych parametrów;
  - sterowanie pozwalające korygować określone parametry urządzeń. Wynikiem realizacji takich funkcji może być np. zablokowanie możliwości użycia urządzeń wadliwie pracujących, przełączanie urządzeń lub zmiana rozpływu ruchu;
- zarządzanie lokalizacją uszkodzeń powinno umożliwiać realizację zadań związanych z wykryciem, wyizolowaniem i skorygowaniem niepoprawnego funkcjonowania systemu. Powinno obejmować:
  - nadzór nad alarmami;
  - testowanie poprawności funkcjonowania wskazanych urządzeń abonenckich (urządzeń sieciowych, central abonenckich itp.);
  - lokalizacje uszkodzeń pozwalającą ustalić źródła stwierdzonych niezdatności;
  - eliminację z systemu elementów uszkodzonych;

- Zarządzanie eksploatacją dotyczy zadań związanych z rejestracją, analizą i zobrazowaniem danych o zachowaniu się systemu lub jego części oraz oceny efektywności jego działania. Są to następujące zadania:
  - śledzenie funkcjonowania poprzez pomiary wielkości zadanych parametrów;
  - nadzór ruchu odnoszący się do zbierania danych o wielkości ruchu generowanego przez abonentów, monitorowanie jakości świadczonych usług poprzez zbieranie i rejestrację danych niezbędnych do wyznaczania wartości wskaźników jakości;
- zarządzanie rozliczeniami – powinno obejmować administrowanie abonentami oraz administrowanie zasobami (również zasobami dzierżawionymi). Umożliwia to rozliczenia pomiędzy użytkownikami systemu oraz operatorami współpracujących podsystemów
- zarządzanie bezpieczeństwem może pozwalają zapewnić ochronę zasobów sieci oraz przesyłanych w niej danych.

Inne podejście reprezentuje TeleManagement Torum



Rysunek 8 Funkcje systemu zarządzania według TeleManagement Forum

Coraz częściej systemy zarządzania wykonywane są w architekturze rozproszonej. Rozproszony otwarty system zarządzania musi realizować następujące funkcje:

- zarządzanie konfiguracjami sprzętu;
- zarządzanie dystrybucją, aktualizacją i licencjonowaniem sprzętu;

- związane z nadzorem sprzętu;

System zarządzania musi zapewniać mechanizmy gromadzenia informacji o stanie sieci oraz przekazywanie ich zarządcom w postaci raportów.

Rozproszone otwarte systemy zarządzania wykorzystują platformę sieciową do decentralizacji funkcji związanych z zarządzaniem. Administratorzy mogą wywoływać system zarządzania z dowolnego miejsca. W całej sieci działają moduły agentów, zbierające informacje i przekazujące je do systemu. Zarządcy mają dzięki temu dostęp do informacji w czasie rzeczywistym.

Dzięki temu upraszcza się proces usuwania usterek, a także profilaktyka eksploatacyjna. Istnieje też możliwość zarządzania proaktywnego, definiowania alarmów ostrzegających przed wystąpieniem przewidywanych problemów.

Niektóre współczesne otwarte systemy zarządzania oparte są na DME (Distributed Management Environment), jest to struktura łącząca funkcje zarządzania systemem i siecią w środowiskach heterogenicznych, przy zachowaniu zgodności z istniejącymi rozwiązaniami.

2.4. Wymagania funkcjonalne

Typowe wymagania na funkcje zarządzania siecią jakie powinny spełniać współczesne pakiety zarządzania systemami otwartymi:

- kontrola dostępu do zasobów sieciowych: śledzi i raportuje wszelką komunikację w sieci, co pozwala na wykrycie niepowołanych dostępów do węzłów sieci oraz kontrola dostępu do platform zarządzających poprzez zastosowanie profili użytkowników: supervisior, administrator sieci, administrator o możliwościach administracyjnych;
- zarządzanie wydajnością sieci: gromadzi i raportuje aktualne dane na temat sposobu wykorzystania sieci. Informacje te są podstawą do planowania optymalizacji architektury i wykorzystania zasobów sieciowych,
- konfiguracja;
- identyfikacja i diagnostyka wszystkich uszkodzeń;
- monitorowanie i sterowanie zasobami;
- zarządzanie w sytuacjach awaryjnych: pozwala na wykrycie i izolację problemów oraz pomoc w ich usunięciu;
- filtrowanie alarmów;

- automatyczne generowanie raportów: ułatwia analizę na czas ogromnej ilości danych przesyłanych w sieci. Odpowiednia aplikacja powinna mieć możliwość współpracy z technikami WWW co pozwala na automatyczne generowanie raportów np. na serwerze WWW. Dzięki tej możliwości administrator systemu może analizować interesujące go dane za pośrednictwem Internetu. Raporty generowane są jako krótkie, poglądowe, bądź dokładne bardzo szczegółowe;

Dodatkowo:

- System zarządzania powinien generować dokładny obraz konfiguracji i statusu sieci, bez względu na to, czy sieć znajduje się w jednym miejscu, czy też jest rozproszona na różnych kontynentach.
- Wykrywane powinny być wszystkie urządzenia, nawet te, które w danej chwili nie są włączone.
- Administrator sieci powinien uzyskiwać prawdziwy i aktualny obraz swego środowiska sieciowego.
- Elementy sieciowe i połączenia pomiędzy nimi, wyświetlane są w postaci mapy połączeń. Obraz sieci może być wyświetlany hierarchicznie (kontekstowe schodzenie do poziomu urządzeń i linków). Pierwszy obraz wyświetlany na ekranie jako ogólny przegląd stanu sieci. Wybierając fragmenty do powiększania w celu znalezienia warstwy, w której powstały jakieś problemy, wyszukuje się urządzenie w celu wyizolowania go.
- Powinien mieć możliwość wykrywania urządzeń zainstalowanych w sieci pochodzących od różnych dostawców np. przy użyciu rozszerzeń MIB innych firm.
- W oparciu o krytyczne punkty ustalone przez administratora sieci powinna istnieć możliwość ustawiania wartości progowych i wyświetlania pojawiających się alarmów.
- Powinna istnieć możliwość definiowania wydarzenia pojawiającego się w sieci, np. przez wyzwolenie alarmów lub podejmowanie jakiegoś działania w razie przekroczenia określonych wartości progowych generowanych przez statystykę (na przykład, odnośnie stopy błędów lub przepustowości).
- Systemy zarządzania powinny mieć możliwość stosowania technik korelacji zdarzeń, która daje możliwość szybkiego ustalenia źródła problemów w sieci. Technologia korelacji zdarzeń pozwala na wyeliminowanie dużej liczby fałszywych zdarzeń i podkreślenie najważniejszych, będących prawdziwymi przyczynami niewłaściwej pracy sieci. Czołowi producenci sprzętu sieciowego dostarczają własne obwody korelacji zdarzeń właściwe dla produkowanego przez nich sprzętu.

- Powinien umożliwiać pomiar i śledzenie wielu wielkości i informacji na każdym urządzeniu współdziałającym z protokołem zarządzania.
- System powinien mieć szereg mechanizmów śledzenia i sporządzania wykresów, wraz z możliwością badania wartości innych niż zapewnionych przez producenta, co umożliwi dostosowanie systemu zarządzającego do potrzeb i upodobań administratora.
- Umożliwiać eksport danych dotyczących topologii sieci, wydajności i zdarzeń do zewnętrznych systemów dla potrzeb analizy i śledzenia trendów – "data warehousing";
- Użytkownik powinien mieć możliwość dodawania nowych, własnych pozycji do menu, wybierając odpowiadające mu zmienne z bazy danych o zarządzaniu (MIB). W ten sposób tworzy własne aplikacje, które stają się częścią standardowego menu.
- Automatyczne zarządzanie pozwala użytkownikom systemu zarządzania na monitorowanie zasobów bez konieczności inicjacji specyficznych zadań. Umożliwia to dostrojenie do specyficznego stylu pracy. Funkcje te są uruchamiane dla zdefiniowanych zdarzeń w odniesieniu do elementów dodawanych do bazy danych zarządzanych urządzeń, graficzny edytor lub np. polecenie wygenerowane przez bibliotekę API.
- Wizualizacja danych w formie wielowymiarowego wykresu zapamiętane lub dynamicznie pozyskiwane dane. Dwu- i trzy-wymiarowe wykresy mogą być bazą do identyfikowania statystycznych trendów ewentualnych problemów pojawiających się w sieci. Formaty wykresów są w pełni definiowalne, a dane wyświetlane na jednym wykresie mogą pochodzić zarówno z pliku jak i bezpośrednio z sieci.
- Zgodność z popularnymi standardami przemysłowymi, przede wszystkim z popularnymi protokołami zarządzania SNMP i CMIP oraz protokołami do utrzymania komunikacji w sieci (TCP, UDP, IP, IPX, DECnet, ARPA i inymi). Pozwala to na pracę w różnorodnych sieciach z różnymi systemami operacyjnymi.

2.5. Architektura sprzętowa systemu zarządzania

Równocześnie z rozwojem prac normalizacyjnych dotyczących systemów zarządzania sieciami telekomunikacyjnymi, ukształtowała się struktura sprzętowa, przystosowana do spełniania zadań bieżącego monitorowania lub zarządzania elementami sieci. Schemat konfiguracji przedstawiono na rys.9.

Architekturę sprzętową tworzą następujące elementy:

Serwer komunikacyjny, który ma za zadanie:

- Kontrolować połączenia z siecią (sieciami) DCN,
- Komunikować się z nadzorowanymi elementami sieci, systemami TMN innych operatorów telekomunikacyjnych lub dostawców usług telekomunikacyjnych,
- Zapewnić translację komunikatów pochodzących z różnych źródeł do wspólnego formatu, konwersję stosowanych protokołów i modeli architektury oraz funkcje urządzenia mediacyjnego.
- Spełniać rolę zabezpieczenia przed niepowołanym dostępem (FireWall) z zewnątrz,
- Zapewnić mechanizmy kryptograficznej ochrony danych.

Serwer plików / bazy danych, który ma za zadanie:

- Przechowywać gromadzone dane dotyczące zarządzanych elementów i udostępniać je aplikacjom,
- Przechowywać kopię istotnych plików serwera komunikacyjnego,
- Dostarczać mechanizmów systemu zarządzania bazą danych dla aplikacji-klientów,
- Zapewniać bezpieczeństwo danych (w tym archiwizację).

Serwery aplikacji, które mają za zadanie:

- Udostępniać aplikacje zarządzania stacjom roboczym,
- Wykonywać automatycznie niektóre aplikacje zarządzania (np. obsługa ekranów projekcyjnych, zadania cykliczne itp.),
- Zapewnić autoryzację użytkowników.

Stacje robocze, wykonujące funkcje zarządzania – stacje graficzne lub mikrokomputery.

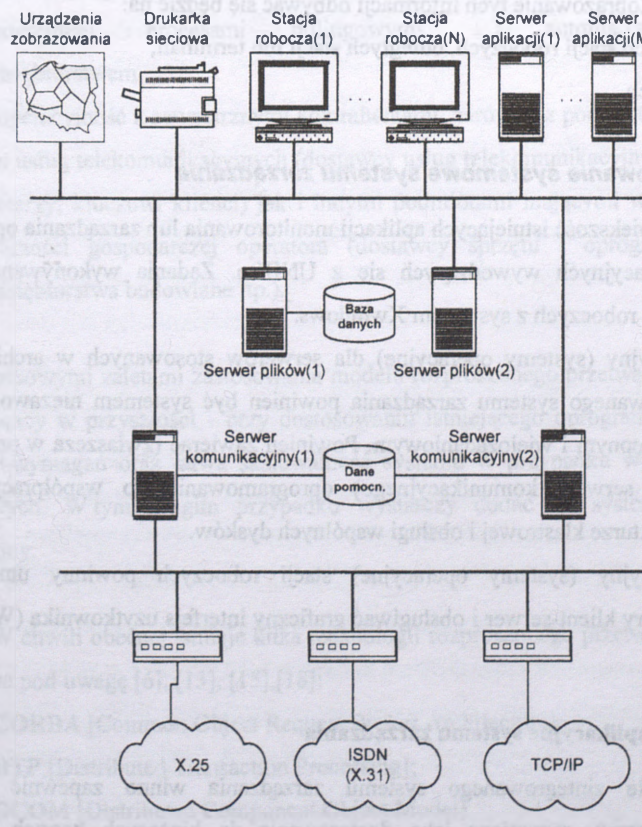
Sieć lokalna – szybka sieć TCP/IP (o przepływności 100 Mb/s), zbudowana w oparciu o kable STP kat. 5 rozszerzonej lub wyższej.

Konfiguracja sprzętowo-programowa powinna umożliwić włączenie dodatkowych urządzeń, służących do prezentacji danych, takich jak ekrany tylnoprojekcyjne, rzutniki projekcyjne, monitory wielkoformatowe itp.

Serwer komunikacyjny i serwer plików powinny być zbudowane w oparciu o konfigurację wielokomputerową. Ilość serwerów aplikacji jest uzależniona od ilości realizowanych funkcji i wymaganej mocy obliczeniowej.

Struktura ta jest z jednej strony wyspecjalizowana do realizacji określonych zadań, z drugiej zaś strony jest podatna na rozbudowę – zarówno ilościową (zwiększona ilość danych może zostać obsłużona przez większą wydajność serwera komunikacyjnego – np. rozbudowa klastra, oraz większą wydajność serwera plików – rozbudowa klastra, rozbudowa macierzy dyskowej) jak i jakościową (nowe funkcje, które nie były przewidziane w fazie projektowania systemu mogą zostać zrealizowane przez dodatkowe serwery aplikacji włączane do systemu w momencie ich zaaplikowania).

Należy przewidzieć, że sieć DCN będzie zrealizowana w oparciu o łącza własne. Ze względów niezawodnościowych należy przewidzieć również rezerwową sieć transmisji danych w oparciu o sieć fizyczną należącą do innego operatora. Celowe jest wykorzystanie do tego celu sieci pakietowej X.25 lub Frame Relay. Niezależnie od sieci DCN może być wykorzystywana sieć oparta o stos protokołów TCP/IP - Internet lub intranet. Takie rozwiązanie zapewni współpracę z innymi systemami lub aplikacjami oraz da możliwość dołączenia odległych terminali do modułu inżynierii.



Rysunek 9 Architektura sprzętowa systemu zarządzania

Zasadniczym elementem służącym do zbierania informacji od nadzorowanych urządzeń będzie serwer komunikacyjny. Serwer komunikacyjny będzie współpracował z siecią lokalną Ethernet (100 Mb/s) poprzez karty sieciowe oraz z siecią DCN wykorzystując karty lub wolnostojące urządzenia dostępowe ISDN i X.25.

Służby dyspozytorskie operatora będą wykorzystywały do wypracowania decyzji operacyjnych informacje prezentowane w formie graficznej.
Urządzeniami zobrazowania będą:

- wideościana,
- monitory graficzne stacji roboczych.

Do celów szczegółowych analiz dyspozytorzy, służby kontrolne, służby planowania i inne służby analityczne przedsiębiorstwa będą wykorzystywały zestawienia tabelaryczne i raporty tekstowe. Zobrazowanie tych informacji odbywać się będzie na:

- monitorach stacji roboczych, odległych stacji lub terminali,
- wydrukach.

2.5.1 Oprogramowanie systemowe systemu zarządzania

Zdecydowana większość istniejących aplikacji monitorowania lub zarządzania oparta jest na systemach operacyjnych wywodzących się z UNIX-a. Zadania wykonywane są na graficznych stacjach roboczych z systemem Xwindows.

System operacyjny (systemy operacyjne) dla serwerów stosowanych w architekturze sprzętowej zintegrowanego systemu zarządzania powinien być systemem niezawodnym w działaniu, wielodostępnym i wielozadaniowym. Powinien zawierać (zwłaszcza w przypadku serwera plików i serwera komunikacyjnego) oprogramowanie do współpracy wielu komputerów w strukturze klastrowej i obsługi wspólnych dysków.

System operacyjny (systemy operacyjne) stacji roboczych powinny umożliwiać realizację architektury klient-serwer i obsługiwać graficzny interfejs użytkownika (Windows, X/Windows, Motif).

Oprogramowanie aplikacyjne systemu zarządzania

Oprogramowanie zintegrowanego systemu zarządzania winno zapewnić wysoką funkcjonalność systemu, rozumianą jako dostosowanie do bieżących potrzeb i zadań

operatora telekomunikacyjnego oraz posiadać możliwość przyszłej rozbudowy systemu o kolejne bloki funkcjonalne.

Równocześnie system należy traktować jako jeden z elementów wspomagania zarządzania operatora telekomunikacyjnego, dlatego musi on umieć wymieniać informacje - poprzez stosowne interfejsy lub unifikację technologii - z innymi systemami wspomagającymi jego działanie oraz z systemami potencjalnych zewnętrznych dostawców usług telekomunikacyjnych. W związku z tym w fazie projektowania poszczególnych aplikacji systemu należy uwzględnić szereg przesłanek i dokonać wyboru stosownych technik i technologii. Poniżej zostaną skrótowo opisane najważniejsze kluczowe zagadnienia, które należy przeanalizować przed przystąpieniem do projektowania aplikacji.

Rozproszone przetwarzanie

Przetwarzanie rozproszone pozwala na stworzenie "wspólnej infrastruktury informacyjnej", rozpatrywanej w dwóch aspektach:

- integracja aplikacji, pozwalająca na wzajemną wymianę danych oraz interakcję pomiędzy procesami inżynierii telekomunikacyjnej i innymi procesami (np. planowaniem, zaopatrzeniem, procesami billingowymi, ...) automatyzacji zarządzania przedsiębiorstwem.
- interoperacyjność z zewnętrznymi kontrahentami, zarówno z podmiotami działającymi na rynku usług telekomunikacyjnych (dostawcy usług telekomunikacyjnych, współpracujący operatorzy, kluczowi klienci) jak i innymi podmiotami mającymi wpływ na całokształt działalności gospodarczej operatora (dostawcy sprzętu i oprogramowania, serwis, przedsiębiorstwa budowlane itp.).

Dodatkowymi zaletami zastosowania modelu rozproszonego przetwarzania jest niewielki nakład pracy w przyszłości - przy dostosowaniu istniejącego oprogramowania do nowych funkcji i wymagań oraz łatwa skalowalność systemu w przypadku wyczerpania zasobów sprzętowych. W tym drugim przypadku wystarczy dodać do systemu kolejny serwer aplikacyjny.

W chwili obecnej istnieje kilka technologii rozproszonego przetwarzania, które mogą być brane pod uwagę [6], [13], [15],[18]:

- **CORBA** [Common Object Request Broker Architecture];
- **DTP** [Distributed Transaction Processing];
- **DCOM** [Distributed Component Object Model]
- **DCE** [Distributed Computing Environment]

Przy wyborze technologii rozproszonego przetwarzania należy również wziąć pod uwagę możliwość integracji tworzonych aplikacji z technologiami inter/intranetowymi – w takim przypadku należy rozpatrywać jedynie technologie DCOM i CORBA (zwłaszcza w połączeniu z JAVA). Ta druga wydaje się być bardziej uniwersalna i rozwojowa [18].

Obiektowość

Obecne tendencje w analizie, projektowaniu i programowaniu, skłaniają do wyboru metod zorientowanych obiektowo. Technologie zorientowane obiektowo pozwalają w prosty sposób wielokrotnie wykorzystywać zdefiniowane obiekty, rozszerzać cechy istniejących obiektów i nadawać im nową funkcjonalność. Obiektowe podejście do projektowania upraszcza znacznie projektowanie aplikacji - zwłaszcza aplikacji wykorzystujących mechanizmy rozproszonego przetwarzania (modele DCOM i CORBA).

Przenośność oprogramowania

W programowaniu obiektowym powszechnie wykorzystywany jest język C++. Kompilatory tego języka zaimplementowane są na wszystkich systemach operacyjnych. C++ tworzy szybki i efektywny kod maszynowy. Alternatywnym rozwiązaniem jest język Java. W przypadku Javy przenośność oprogramowania odbywa się nie na poziomie kodu źródłowego (jak w przypadku C++) lecz na poziomie półkompilatu.

Modułowa struktura aplikacji

W trakcie projektowania i programowania aplikacji należy zapewnić modułową ich strukturę, pozwalającą na późniejszą łatwą rozbudowę systemu o nowe elementy funkcjonalne (np. nowe protokoły i usługi, nowe urządzenia mediacyjne itp.).

Dostęp do informacji

Jednym z głównych czynników, branych pod uwagę w trakcie projektowania systemu, powinien być łatwy i tani sposób wymiany informacji z otoczeniem w formie elektronicznej. Obecnie jednym z prostszych do zrealizowania sposobów udostępniania informacji jest wykorzystanie technologii inter/intranetowych. Implementacja protokołów HTTP i FTP umożliwi wykorzystanie standardowych narzędzi do pozyskiwania informacji (przeglądarki internetowe, klienci FTP). Takie rozwiązanie umożliwi pozyskiwanie dla celów zarządzania przedsiębiorstwem informacji różnego typu i z wielu systemów (również zewnętrznych) za pomocą jednego narzędzia.

Oprogramowanie systemu zarządzania bazą danych

Ekonomicznie uzasadnionym wyborem wydaje się być system zarządzania relacyjną bazą danych, strojoną pod kątem przechowywania obiektów. Przykładem takiego środowiska są najnowsze bazy danych ORACLE. Ponadto zaimplementowany uniwersalny język zapytań

SQL pozwoli na współpracę z istniejącymi starszymi systemami wspomagania zarządzania przedsiębiorstwem poprzez standardowe mechanizmy ODBC.

Dodatkowym argumentem, przemawiającym za wykorzystaniem relacyjnej bazy danych, są dopracowane, kompletne i spójne narzędzia CASE do projektowania i programowania baz danych, wykorzystujące znane metodyki projektowania, skracające do niezbędnego minimum czas potrzebny do utworzenia i udokumentowania bazy danych, z drugiej zaś strony gwarantujące jej formalną poprawność i spójność danych.

Platforma zarządzania [13],[15]

W minionych latach zdefiniowano szereg standardów i protokołów zarządzania sieciami. We wczesnych latach siedemdziesiątych dostawcy sprzętu telekomunikacyjnego zaczęli implementować język MML do komunikacji operatora z urządzeniami telekomunikacyjnymi. W 1984 roku Bellcore stworzyła standard języka MML do zarządzania elementami sieci, zwany TL1 (Transaction Language 1). Organizacje takie jak ITU-T (poprzednio CCITT), ISO oraz IEC opracowały pod koniec lat osiemdziesiątych - i nadal rozwijają - model zarządzania przeznaczony do zarządzania sieciami telekomunikacyjnymi, oparty na zdefiniowanym protokole CMIP, wykorzystującym obiektowy model GDMO. Niezależnie powstał standard zarządzania sieciami teleinformatycznymi SNMP. Protokół SNMP jest przeznaczony do zarządzania prostymi sieciami na zasadzie przepytywania, wykorzystuje statyczny model zarządzanej sieci – nie oferuje dynamicznego zarządzania obiektami – zatem nie nadaje się jako protokół zarządzania złożonymi sieciami telekomunikacyjnymi. Niemniej jednak protokół SNMP powinien być zaimplementowany w systemie dla zarządzania istniejącymi sieciami wykorzystującymi stos protokołów TCP/IP.

Obecnie – po ogłoszeniu specyfikacji architektury CORBA – trwają rozważania na temat włączenia tej architektury do modelu zarządzania sieciami telekomunikacyjnymi i teleinformatycznymi równolegle do stosowanych protokołów SNMP i CMIP. Powodem takiego stanu rzeczy jest konieczność bardziej globalnego spojrzenia na działalność telekomunikacyjną operatora – dotychczasowe protokoły zapewniają zarządzanie na poziomie elementów sieci i sieci (TL-1 tylko na poziomie elementów), pomijając zupełnie warstwy zarządzania usługami i zarządzania biznesowego przedsiębiorstwem.

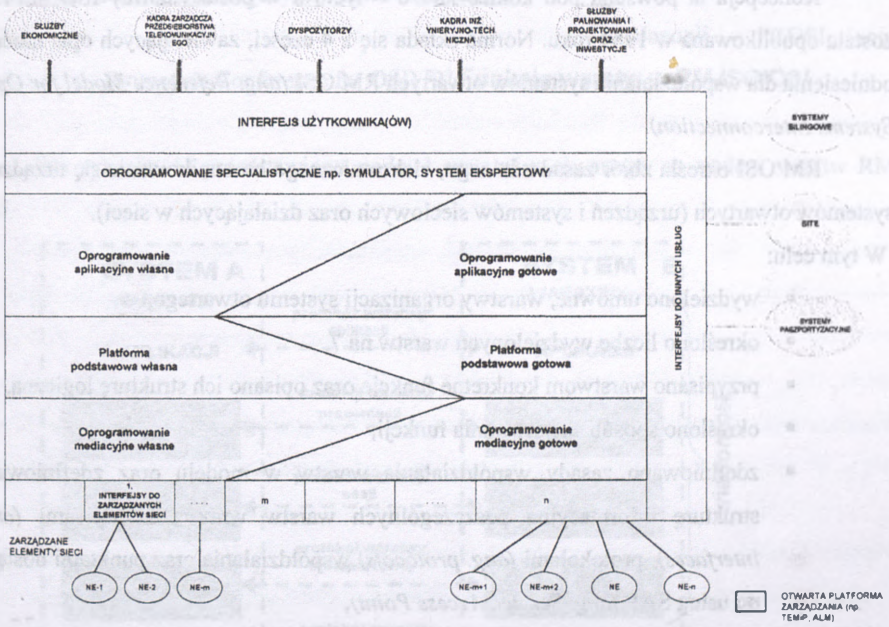
- SNMP i CMIP jest użyteczny do zarządzania wykorzystując architekturę klient-serwer (master/slave) do nadzorowania i sterowania pracą zasobów. Alternatywne technologie (CORBA, DCOM, DCE) proponują interakcje peer-to-peer.

- SNMP i CMIP są właściwe do zastosowań, gdzie wymagana jest interakcja z poszczególnymi elementami sieci. Zarządzanie usługami jest interakcją typu business-to-business/peer-to-peer i z założenia wykorzystuje zalety rozproszonego przetwarzania (elementy potrzebne do wykonania usługi są rozproszone). Oczywiście interakcje są również modelowane jako master/slave.
- GDMO/CMIP widzi poszczególne elementy sieci (atomowo) – CORBA widzi obiekty bardziej abstrakcyjnie – w zależności od żądanego poziomu szczegółowości.
- CMIP i rozszerzenia SNMP są zbyt „ciężkie" do interakcji peer-to-peer, bardziej kosztowne w implementacji i nie nadążają za światowymi trendami tworzenia generalnych, globalnych aplikacji IT. Dostępność doświadczonych programistów CMIP/GDMO jest ograniczona a czas nauki jest zdecydowanie dłuższy niż modelu CORBA i języka takiego jak np. JAVA.

Dostępne na rynku rozwiązania zarządzania sieciami stanowią realizację koncepcji otwartych rozwiązań IT. Wszystkie rozwiązania opierają się na pewnym zestawie rozwiązań protokołów, funkcji i usług, stanowiącym platformę do budowania aplikacji zarządzania. Podstawowe funkcje dostępne w platformach poszczególnych producentów stanowią rodzaj biblioteki prymitywów, z których buduje się komponenty usług zarządzania, z tych zaś bloki funkcjonalne, realizujące określone złożone zadania. W skład platformy wchodzą również interfejsy: graficzny interfejs do komunikacji z użytkownikiem oraz interfejs API do budowy kolejnych elementów systemu zarządzania, protokoły komunikacyjne, mechanizmy interakcji klient/serwer i zarządca/agent, usługi wymiany plików (FTP, FTAM) itp. Producenci oferują również wiele aplikacji zarządzania poziomu zarządzania elementami, zarządzania siecią i ostatnio coraz więcej aplikacji poziomu zarządzania usługami. Pojęcie „platformy" nie oznacza zamkniętego produktu – jest to modularna architektura, pozwalająca na wybór potrzebnych komponentów z oferty. Trudno jest w wielu przypadkach określić, czy komponent jest elementem podstawowej platformy, czy może już aplikacją zbudowaną w oparciu o tą platformę; na przykład najbardziej podstawowe funkcje: zarządzanie stanem obiektu czy też administracja dziennikami (logami) błędów i zdarzeń. Tak więc jako platformę należy przyjąć zestaw bibliotek i aplikacji wybranych z oferty producenta.

Czas potrzebny na zbudowanie „od zera" systemu dla potrzeb zarządzania sieciami należy szacować na kilka a nawet kilkanaście lat. Przy tak szybkim postępie technologii, jaki obserwujemy dzisiaj, może się okazać, że zbudowany system w momencie oddawania do eksploatacji nie jest adekwatny do potrzeb i oczekiwań operatora. W związku z tym słusznym rozwiązaniem jest użycie gotowej platformy i skonstruowanie jedynie niektórych,

specyficznych aplikacji. W ten sposób cykl budowy systemu można ograniczyć do pojedynczych lat, a w niektórych sytuacjach – nawet do miesięcy. Z drugiej strony wytworzenia oprogramowania przez krajowych producentów oprogramowania jeszcze w dalszym ciągu jest niższy niż zakup gotowych rozwiązań zachodnich. Dlatego w fazie oceny i wyboru rozwiązania należy znaleźć rozsądny kompromis pomiędzy czasem wytworzenia oprogramowania a jego sumarycznym kosztem (koszt zakupu elementów platformy, koszt wytworzenia oprogramowania, koszty późniejszych adaptacji systemu).



Rysunek 10 Struktura logiczna oprogramowania systemu zarządzania

3. Charakterystyka zarządzania w ujęciu modelu odniesienia ISO/OSI

Międzynarodowa Organizacja Standaryzacyjna (*ang. International Organisation for Standarizations)*, uwzględniając doświadczenia wynikające z prób współpracy systemów informacyjnych różnych producentów, opracowała spójną metodologicznie koncepcję współdziałania systemów informacyjnych, stanowiącą podstawę do projektowania systemów otwartych, czyli zdolnych do wymiany informacji między sobą.

Koncepcja ta powstała pod koniec lat 70 – tych, a w postaci normy ISO – 7489, została opublikowana w 1984 roku. Norma składa się z 4 części, zawierających opis modelu odniesienia dla współdziałania systemów otwartych RM OSI *(ang. Reference Model for Open Systems Interconnection).*

RM OSI określa zbiór zasad zdalnego, elektronicznego komunikowania się urządzeń/ systemów otwartych (urządzeń i systemów sieciowych oraz działających w sieci).

W tym celu:

- wydzielono umowne, warstwy organizacji systemu otwartego,
- określono liczbę wydzielonych warstw na 7,
- przypisano warstwom konkretne funkcje oraz opisano ich strukturę logiczną,
- określono sposób aktywowania funkcji,
- zdefiniowano zasady współdziałania warstw w modelu oraz zdefiniowano strukturę informacyjną poszczególnych warstw wraz z interfejsami *(ang. interfaces),* protokołami *(ang. protocols)* współdziałania oraz punktami dostępu do usług SAP *(ang. Service Access Point)*,

Model nie określa natomiast fizycznej budowy poszczególnych warstw, a koncentruje się na sposobach ich współpracy.

Warstwy sieci stanowią niezależne całości i chociaż nie potrafią wykonywać żadnych widocznych zadań w odosobnieniu od pozostałych warstw, to z programistycznego punktu widzenia są one odrębnymi poziomami.

Komunikacja pomiędzy systemami otwartymi odbywa się na poziomie odpowiadających sobie warstw. Dla każdej warstwy powinien zostać stworzony własny protokół komunikacyjny w rzeczywistej sieci komunikacja odbywa wyłącznie się na poziomie warstwy fizycznej.

Pomiędzy pozostałymi warstwami istnieje komunikacja wirtualna. Opracowany przez ISO model RM OSI został przyjęty bez zmian przez Komitet Konsultacyjny ds. Międzynarodowej Telefonii i Telegrafii CCITT (ang. Consultative Committee for

International Telephone and Telegraph), obecnie Międzynarodową Unię Telekomunikacyjną ITU – T *(ang. International Telecommunications Union – Telecommunications Sector)*, stanowiąc podstawy koncepcji współdziałania systemów otwartych na obszar systemów telekomunikacyjnych.

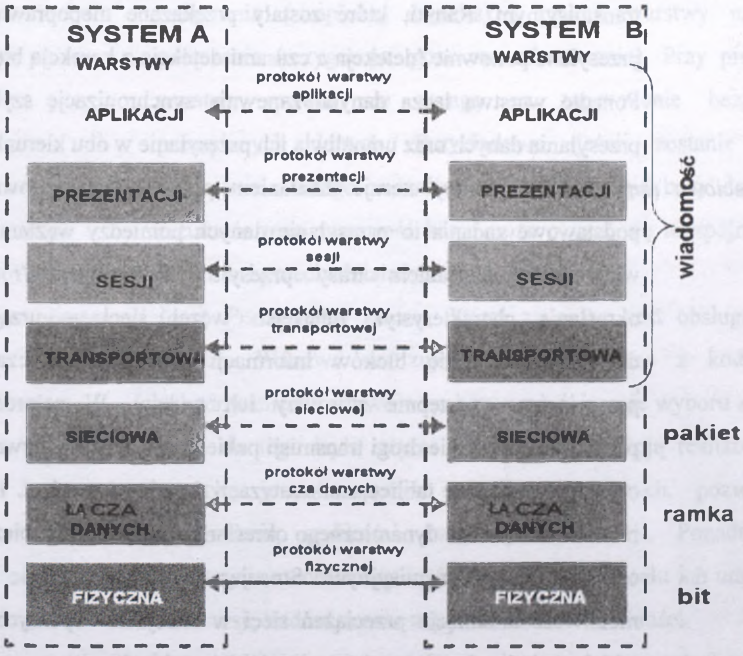
Wynikiem tych prac było opracowanie normy X.200 i wydanie jej w tzw. „Czerwonej Księdze (ang. Red Book) w 1994 r. oraz w „Niebieskiej Księdze" (ang. Blue Book) w 1988 r [2],[3], [6].

Zastosowaniem RM OSI oraz wykorzystaniem standardów wypełniających ten model zajmują się również inne międzynarodowe organizacje:

- w Japonii - PCOSI (ang. Promotion Conference for OSI) [2].

Funkcje warstw w RM ISO/OSI

Na rysunku 11.przedstawiono podział systemów otwartego na siedem warstw RM OSI.



Rysunek 11 Warstwy w modelu odniesienia ISO/OSI

W RM ISO/OSI wprowadzono następujący podział funkcjonalny poszczególnych warstw:

Warstwa fizyczna (ang. Physical Link Layer) odpowiada za transmisję sygnałów w sieci. Realizuje konwersje bitów informacji na sygnały elektryczne, które

będą przesyłane w kanale transmisyjnym z uwzględnieniem maksymalizacji niezawodności przesyłu.

W warstwie fizycznej określa się parametry amplitudowe i czasowe przesyłanego sygnału, fizyczny kształt i rozmiar łączy, znaczenie ich poszczególnych interfejsów (mechanicznych i elektrycznych) oraz wartości napięć na nich występujących, sposoby nawiązywania połączenia i jego rozłączania po zakończeniu transmisji.

Warstwa łącza danych (ang. Data Link Layer) realizuje odbiór i konwersję strumienia bitów pochodzących z urządzeń transmisyjnych w taki sposób, aby nie zawierały one błędów. Warstwa ta postrzega dane jako grupy bitów zwane ramkami. Warstwa łącza danych tworzy i rozpoznaje granice ramki. Ramka tworzona jest przez dołączenie do jej początku i końca grupy specjalnych bitów. Kolejnym zadaniem warstwy jest eliminacja zakłóceń, powstałych w trakcie transmisji informacji w kanale transmisyjnym. Ramki, które zostały przekazane niepoprawnie, są przesyłane ponownie (detekcja a czasami detekcja z korekcją błędów). Ponadto warstwa łącza danych zapewnia synchronizację szybkości przesyłania danych oraz umożliwia ich przesyłanie w obu kierunkach.

Warstwa sieciowa (ang. Network Layer) steruje działaniem podsieci transportowej. Jej podstawowe zadania to przesyłanie danych pomiędzy węzłami sieci wraz z wyznaczaniem trasy przesyłu (marszrutyzacja/routing), określanie charakterystyk interfejsu węzeł sieci – urządzenie dostępowe, łączenie bloków informacji w ramki na czas ich przesyłania a następnie stosowny ich podział. W najprostszym przypadku określanie drogi transmisji pakietu informacji odbywa się w oparciu o statyczne tablice marszrutyzacji (routingu) w sieci. Istnieje również możliwość dynamicznego określania trasy na bazie bieżących obciążeń łączy transmisyjnych. Stosując drugie rozwiązanie mamy możliwość uniknięcia przeciążeń sieci w relacjach wspólnych czyli takich, na których pokrywają się drogi wielu pakietów.

Warstwa transportowa (ang. Transport Layer) obsługuje dane przyjmowane z warstwy sesji. Obejmuje ona opcjonalne dzielenie danych na mniejsze jednostki, przekazywanie zblokowanych danych warstwie sieciowej, otwieranie połączenia stosownego typu i prędkości, realizacja przesyłania danych, zamykanie połączenia. Ponadto mechanizmy wbudowane w warstwę

transportową pozwalają rozdzielać logicznie szybkie kanały transmisyjne pomiędzy kilka połączeń sieciowych. Możliwe jest także udostępnianie jednego połączenia kilku warstwom sieciowym, co może obniżyć koszty eksploatacji sieci. Celem postawionym przy projektowaniu warstwy transportowej jest zapewnienie pełnej jej niezależności od zmian konstrukcyjnych sprzętu.

Warstwa sesji (ang. Session Layer) realizuje określenie parametrów sprzężenia użytkowników. Po nawiązaniu stosownego połączenia warstwa sesji pełni szereg funkcji zarządzających, związanych m. in. z taryfikacją usług w sieci. W celu otwarcia połączenia pomiędzy systemami (sesji transmisyjnej) poza podaniem stosownych adresów warstwa sprawdza, czy obie warstwy (nadawcy i odbiorcy) mogą otworzyć połączenie. Następnie obie komunikujące się strony muszą wybrać opcje obowiązujące w czasie trwania sesji. Dotyczy to na przykład rodzaju połączenia (simpleks, dupleks) i reakcji warstwy na zerwanie połączenia (rezygnacja, ponowne odtworzenie). Przy projektowaniu warstwy zwraca się uwagę na zapewnienie bezpieczeństwa przesyłanych danych. Przykładowo, jeżeli zostanie przerwane połączenie, którego zadaniem była aktualizacja bazy danych, to w rezultacie tego zawartość bazy może okazać się niespójna. Warstwa sesji musi przeciwdziałać takim sytuacjom.

Warstwa prezentacji (ang. Presentation Layer), której zadaniem jest obsługa formatów danych. Warstwa realizuje funkcje związane z kodowaniem i dekodowaniem zestawów znaków oraz dokonuje wyboru algorytmów, które do tego będą użyte. Przykładową funkcją realizowaną przez warstwę jest kompresja przesyłanych danych, pozwalająca na zwiększenie szybkości transmisji informacji. Ponadto warstwa udostępnia mechanizmy kodowania danych w celu ich utajniania oraz konwersję kodów w celu zapewnienia ich mobilności.

Warstwa aplikacji (ang. Aplicattion Layer) zapewnia programom użytkowym usługi komunikacyjne. Określa formaty wymienianych danych i opisuje reakcje systemu na podstawowe operacje komunikacyjne. Warstwa stara się stworzyć wrażenie przezroczystości sieci. Jest to szczególnie ważne w przypadku obsługi rozproszonych baz danych, w których użytkownik nie powinien wiedzieć, gdzie zlokalizowane są

wykorzystywane przez niego dane lub gdzie realizowany jest jego proces obliczeniowy.

3.2 Zarządzanie w środowisku systemów otwartych

W ramach X.200 wykorzystuje się specyficzny język określający opisywane przez zalecenie funkcje, procesy oraz elementy fizyczne, służące do ich realizacji [2], [3], [4], [35]. Poniżej przedstawiono definicję wybranych pojęć.

- *System rzeczywisty(ang. Real System)* - zbiór zawierający jeden lub więcej komputerów, związane z nimi oprogramowanie, urządzenia zewnętrzne, terminale, operatorzy, procesy fizyczne, środki transferu informacji itd., które stanowią autonomiczną całość zdolną do przetwarzania i/lub przesyłania informacji.
- *System rzeczywisty otwarty (ang. Real Open System)* - system rzeczywisty, który spełnia wymagania standardów OSI w zakresie komunikacji z innymi systemami rzeczywistymi.*System otwarty (ang. Open System)* - reprezentacja w modelu odniesienia tych aspektów systemu rzeczywistego otwartego, które odnoszą się do OSI.
- *Proces aplikacyjny AP (ang. Application Process)* - element w systemie rzeczywistym otwartym, który realizuje przetwarzanie informacji dla konkretnego zastosowania.*Segment (ang. Entity)* warstwy modelu OSI – aktywna jednostka danej warstwy, która realizuje funkcje (usługi) przypisane tej warstwie. Segmentem może być na przykład procedura programu lub układ elektroniczny.
- *Segment aplikacyjny AS (ang. Application Entityt)* - aktywny element warstwy aplikacji, który realizuje wybrany zestaw usług komunikacyjnych OSI dla potrzeb danego procesu aplikacyjnego. Segment aplikacyjny AE realizuje wybrany zestaw usług komunikacyjnych OSI dla potrzeb danego *procesu aplikacyjnego,* którego jest częścią.
- Proces aplikacyjny *AP* (ang. *Application Process)* przedstawia te zasoby systemu otwartego, które obsługują wybrane zastosowanie tego systemu, na, przykład zarządzanie siecią. Na proces aplikacyjny składają się programy aplikacyjne odpowiedzialne za przetwarzanie danych (informacji), znajdujące się poza *środowiskiem OSI* (ang. *OSI Environment),* i segmenty aplikacyjne znajdujące się w warstwie aplikacji.

- Aplikacyjny element usługowy ASE *(ang. Application Service Element)* - część segmentu aplikacyjnego, która świadczy wyspecjalizowane usługi dla potrzeb procesu aplikacyjnego.

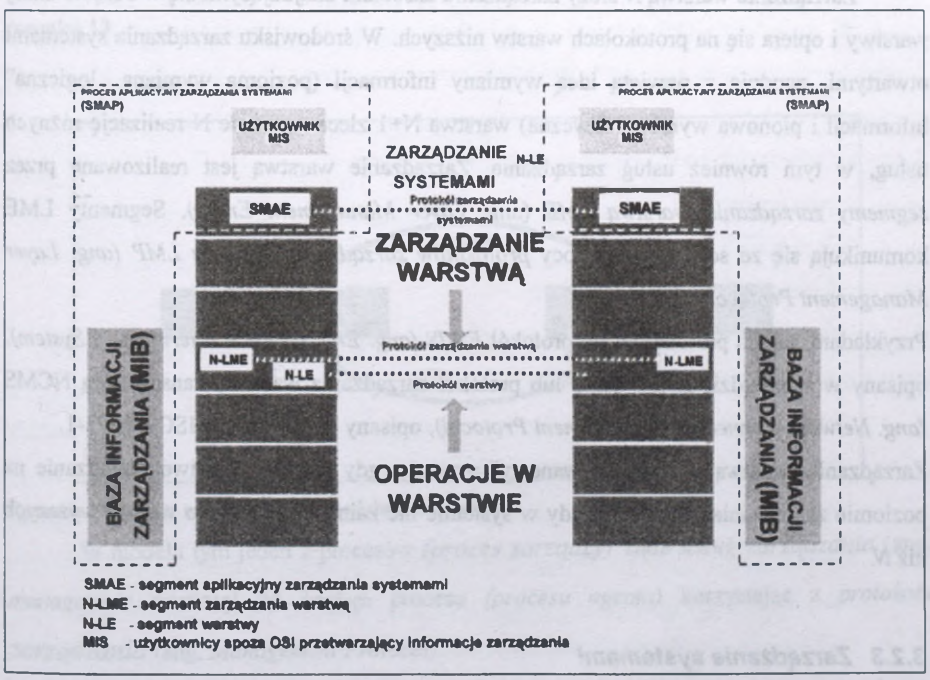
Informacja zarządzania, która jest znana w danym systemie otwartym, jest przechowywana w *bazie informacji zarządzania MIB* (ang. *Management Information Base)* i opisuje *zarządzane obiekty* MO (ang. *Managed Objects),* które są modelami zarządzanych zasobów.

Jeśli procesy zarządzania funkcjonują w różnych systemach otwartych, to komunikują się korzystając z połączenia OSI i odpowiedniego *protokołu zarządzania MP (ang. Management Protocol).*

Komunikacja ta może być prowadzona na trzech *poziomach zarządzania*:

- na poziomie *operacji w warstwie N* (ang. *N-layer Operations),*
- na poziomie *zarządzania warstwą N* (ang. *N-layer Management),*
- na poziomie *zarządzania systemami* (ang. *Systems Management).*

Koncepcję zarządzania w środowisku systemów otwartych przedstawiono na rysunku.12



Rysunek 12 Zarządzanie OSI w odniesieniu do RM OSI

3.2.1 Operacje zarządzania realizowane w warstwie

Operacje w warstwie *N* są realizowane przez protokoły warstwy *N*, które nie są protokołami zarządzania *sensu stricto*. Z punktu widzenia zarządzania użyteczne są tylko wybrane funkcje tych protokołów i one właśnie określane są mianem operacji *w* warstwie *N*. Można podać wiele przykładów operacji w warstwie, między innymi:

- w warstwie sieci - protokół X.25 PLP: przesłanie pakietu *Call Request* Z wiadomością, że kosztem połączenia należy obciążyć odbiorcę a nie nadawcę lub przesłanie pakietu *clear* z informacjami dotyczącymi opłaty za połączenie;
- w warstwie łącza danych - protokół HDLC: przesłanie ramki z zawiadomieniem o odebraniu ramki z prawidłową sumą kontrolna, ale o niedopuszczalnej semantyce.

Do abstrakcyjnego przedstawienia zasobów realizujących operacje w warstwie *N* stosowane jest pojęcie *segmentu warstwy LE* (ang. *Layer Entity).*

3.2.2 Zarządzanie warstwą

Zarządzanie warstwą *N* służy zarządzaniu zasobami znajdującymi się w obrębie danej warstwy i opiera się na protokołach warstw niższych. W środowisku zarządzania systemami otwartymi, zgodnie z przyjętą ideą wymiany informacji (pozioma wymiana „logiczna" informacji i pionowa wymiana fizyczna) warstwa N+1 zleca warstwie N realizację różnych usług, w tym również usług zarządzania. Zarządzanie warstwą jest realizowane przez *segmenty zarządzania warstwą LME* (ang. *Layer Management Entity).* Segmenty LME komunikują się ze sobą przy pomocy *protokołów zarządzania warstwą LMP (ang. Layer Management Protocol)..*

Przykładami takich protokołów są: protokół *ES-IS (ang. End System – Intermediate System),* opisany w standardzie ISO – 9542 lub protokół zarządzania warstwą transportową NCMS *(ang. Network Connection Management Protocol),* opisany w standardzie ISO- -8073-1.

Zarządzanie warstwą *N jest* stosowane tylko wtedy, gdy nie jest możliwe zarządzanie na poziomie zarządzania systemami, gdy w systemie nie zaimplementowano warstw wyższych niż *N.*

3.2.3 Zarządzanie systemami

Zarządzanie w środowisku systemów otwartych jest realizowane przez *aplikacyjne procesy zarządzania aplikacyjne procesy zarządzania – SMAP (ang. System Management Application Process),* które przetwarzają i wymieniają między sobą *informacje zarządzania*

(ang. *Management Information).*

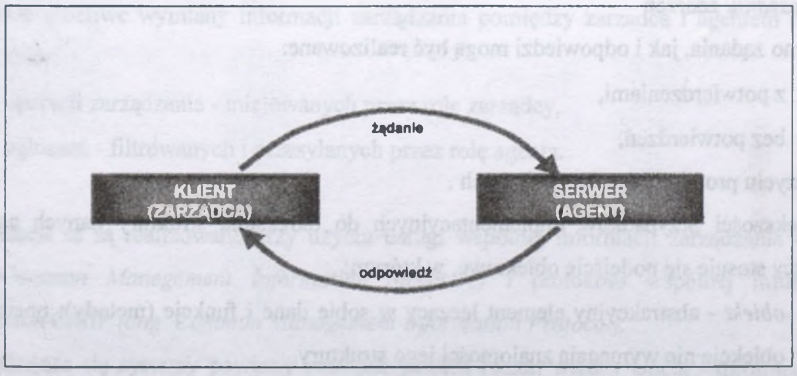
Za komunikację między procesami zarządzania odpowiada *segment aplikacyjny zarządzania* — SMAE *(ang. System Management Application Element),* korzystający z *protokołu zarządzania systemami.*

Standardy ISO/IEC dają wytyczne do tworzenia aplikacji zarządzania systemami otwartymi w zakresie:

- modelu zarządzania;
- wymaganych funkcji zarządzania;
- metod definiowania obiektów zarządzanych (metod opisów zasobów);
- protokołów wymiany informacji dla celów zarządzania.

3.3 Model zarządca - agent

Oddziaływanie między dwoma procesami SMAP opiera się na architekturze typu „klient – serwer", który w odniesieniu do zarządzania nazywany jest modelem wymiany informacji typu *zarządca-agent (ang. Manager-Agent Model),* co zostało zilustrowane na rysunku.13.



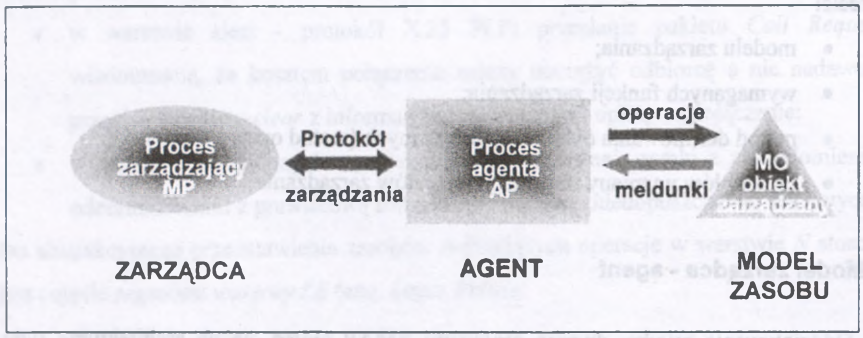
Rysunek 13 Relacje informacyjne w modelu klient-serwer

W modelu tym jeden z procesów *(proces zarządcy)* żąda *usług zarządzania* (ang. *management services)* od drugiego procesu *(procesu agenta)* korzystając z *protokołu zarządzania* (ang. *Management Protocol).*

Proces zarządcy (usługobiorca usług zarządzania), nazywany jest zarządzania *procesem zarządzającym MP* (ang. *Managing Process)* lub i *zarządcą*, zaś proces, który realizuje usługę (usługodawca usług zarządzania) określany jest mianem *procesu agenta*

AP (ang. *Agent Process)* lub agenta.

Proces zarządcy wydaje procesowi agenta polecenia przeprowadzenia operacji na zarządzanych obiektach oraz odbiera meldunki o zdarzeniach dotyczących zarządzanych obiektów. Idea takiego powiązania informacyjno – funkcjonalnego zarządcy z agentem została przedstawiona na rysunku.14.



Rysunek 14 Powiązania procesów zarządcy - agenta i zarządzanego obiektu

W zarządzaniu OSI przyjęto, że ca odpowiedzialność za zawiadomienie zarządcy o zdarzeniu spoczywa na agencie; ta model zarządzania nazywany jest *zarządzaniem opartym na zgłaszaniu* zdarzeń

Zarówno żądania, jak i odpowiedzi mogą być realizowane:

- z potwierdzeniami,
- bez potwierdzeń,

przy użyciu protokołów połączeniowych .

W większości przypadków implementacyjnych do określania struktury danych agenta i zarządcy stosuje się podejście obiektowe, w którym:

- *obiekt* - abstrakcyjny element łączący w sobie dane i funkcje (metody); operacje na obiekcie nie wymagają znajomości jego struktury,
- *klasa obiektu* - definicja obiektu, na podstawie której powstaje obiekt;
- *dziedziczenie* - określa zasady przekazywania definicji przez jedną z klas (nadklasa) innej klasie (podklasa),
- *polimorfizm* określa taką konstrukcję obiektu, która umożliwia komunikowanie się z tym obiektom w uniwersalny sposób używany do komunikacji z innymi obiektami

W ramach RM ISO/OSI między agentem a zarządcą zdefiniowano dwa typy usług zarządzania:

- *operacja zarządzania* - proces zarządcy wydaje procesowi agenta polecenie wykonania operacji zarządzania (ang. *Management Operation)* na zarządzanych obiektach,

przesyłanie meldunku o zdarzeniu (ang. *Event Notification)* - proces agenta przesyła meldunek o zmianie stanu obiektu procesowi zarządcy. *Zdarzeniem* (ang. *Event)* jest nazywana dowolna zmiana stanu zarządzanych obiektów a *meldunkiem* (ang. *Notification) jest* zawiadomienie o zdarzeniu.

Funkcja zarządcy lub funkcja agenta me jest trwale związana z danym procesem SMAP. Ten sam proces może w jednej sytuacji pełnić rolę agenta, a w innej rolę zarządcy. W zależności od roli, jaką pełni proces SMAP w danym systemie otwartym, system ten nazywany jest *systemem zarządzającym* (ang. *managing system)* lub *systemem zarządzanym* (ang. *managed system).* Systemy otwarte, w których funkcjonują procesy SMAP, mogą tworzyć zgodną z modelem OSI sieć zarządzającą o dowolnej konfiguracji.

3.4 Mechanizm zarządzania w Modelu Odniesienia Systemów Otwartych

Proces zarządzania, przyjmujący rolę agenta, jest wyposażany w bazę informacji zarządzania MIB *(ang. Management Information Base)*, która stanowi uporządkowany zbiór obiektów zarządzanych.

Wszystkie możliwe wymiany informacji zarządzania pomiędzy zarządcą i agentem tworzą spójny zbiór:

- operacji zarządzania - inicjowanych przez rolę zarządcy,
- zgłoszeń - filtrowanych i przesyłanych przez rolę agenta.

Operacje te są realizowane przy użyciu usługi wspólnej informacji zarządzania CMIS *(ang. Common Manegement Information Structure)* i protokołu wspólnej informacji zarządzania CMIP *(ang. Common Management Information Protocol).*

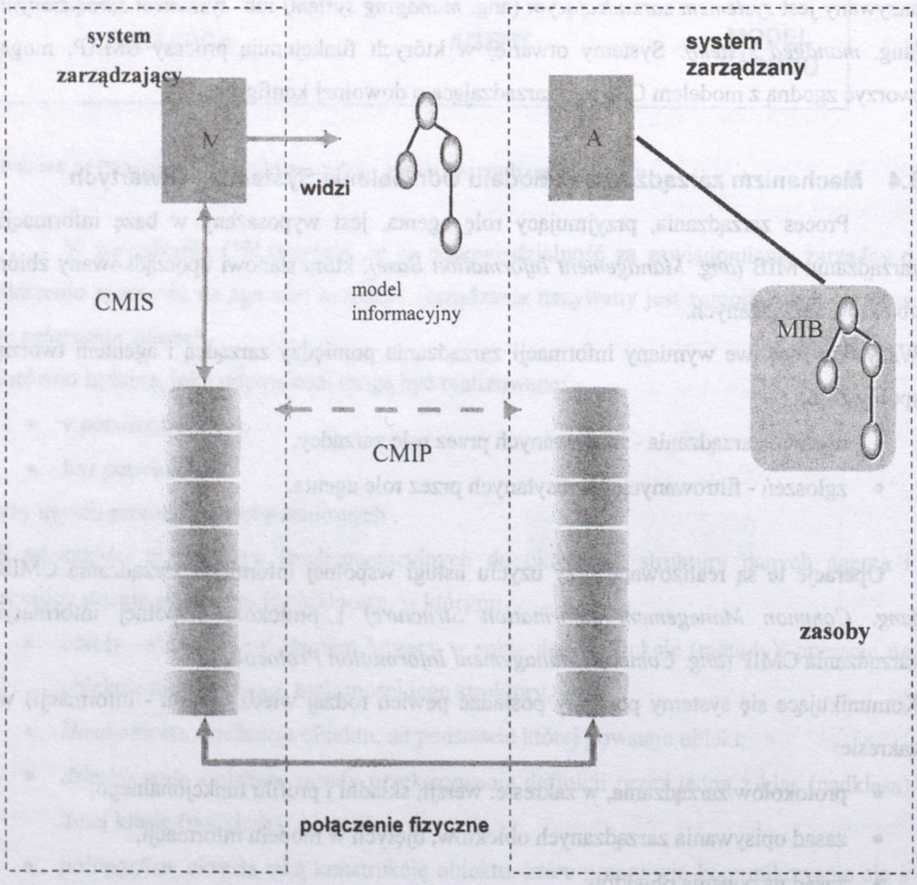
Komunikujące się systemy powinny posiadać pewien rodzaj wiedzy (meta - informacji) w zakresie:

- protokołów zarządzania, w zakresie: wersji, składni i profilu funkcjonalnego,
- zasad opisywania zarządzanych obiektów, ujętych w modelu informacji,
- zasad nazywania obiektów,
- adresów segmentów aplikacyjnych systemów zarządzania i ich punktów dostępu do usług,

- jednostek funkcjonalnych wybranych aplikacyjnych elementów usługowych oraz jednostek funkcjonalnych stosowanych w kolejnych warstwach danej implementacji modelu OSI,
- zasad odtwarzania połączenia, w razie jego przerwania, między procesem zarządzającym i procesem agenta.

Informacje te określa się jako *„wspólna wiedza zarządzania"* SMK *(ang. Shared Management Knowledge),* przy czym w przypadku braku wiedzy dotyczącej ww. obszarów przez komunikujące się systemy, przed właściwą komunikacją następuje *negocjacja kontekstu* (wymiana SMK).

Omówiony wyżej mechanizm został przedstawiony na rysunku.15.



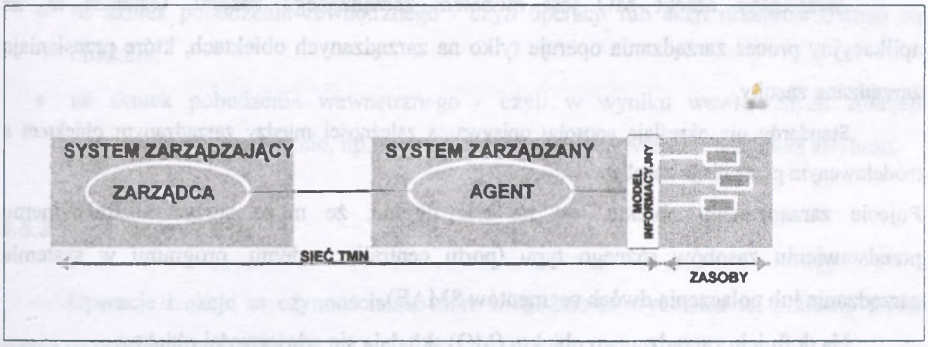
Rysunek 15 Mechanizm zarządzania w systemach otwartych

3.5 Charakterystyka obiektów zarządzanych w Modelu Odniesienia Systemów Otwartych

Omawiana poniżej problematyka została przedstawiona szerzej w [2],[4],[35].

3.5.1 Definicja obiektów zarządzanych

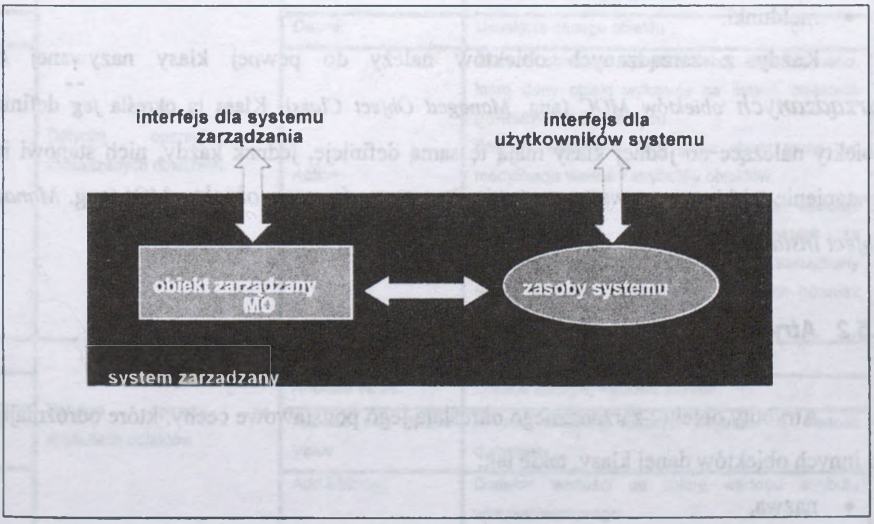
Wszystkie zasoby sieci, podlegające zarządzaniu, są reprezentowane dla zarządcy jako obiekty zarządzane MO *(ang. Management Object)*.



Rysunek 16 Zarządzane obiekty według koncepcji zarządzania OSI

Zarządzane zasoby realizują dwa typy usług:

- normalne usługi im przypisane (dla klientów),
- usługi dla zarządcy - usługi zarządzania.



Rysunek 17 Rodzaje interfejsów do zarządzanych obiektów

Nie ma wymogu odwzorowania bezpośredniego (jeden na jeden) między obiektami zarządzanymi a zasobami (fizycznymi czy logicznymi). Zasoby mogą być reprezentowane przez jeden lub więcej obiektów zarządzanych. Mogą istnieć obiekty zarządzane reprezentujące zasoby logiczne. Jeżeli jakieś zasoby nie są reprezentowane przez obiekt zarządzany, nie są widoczne dla systemu zarządzania i nie mogą być zarządzane. Obiekt zarządzany może prezentować obraz zasobów reprezentowanych przez inne obiekty zarządzane. Obiekty zarządzane mogą być zagnieżdżone (reprezentacja zasobów zawierających inne zasoby reprezentowane przez inne obiekty zarządzane).

Zarządzany obiekt MO jest modelem zarządzanego zasobu. Oznacza to, że aplikacyjny proces zarządzania operuje tylko na zarządzanych obiektach, które przesłaniają zarządzane zasoby.

Standardy nie określają sposobu opisywania zależności między zarządzanym obiektem a modelowanym przez niego zasobem.

Pojęcie zarządzanego obiektu jest na tyle ogólne, że może służyć abstrakcyjnemu przedstawieniu zasobów różnego typu (portu centrali, modemu, programu w systemie zarządzania lub połączenia dwóch segmentów SMAE).

Na definicję zarządzanego obiektu (MO) składają się właściwości obiektu:

- atrybuty,
- operacje,
- akcje,
- zachowanie,
- meldunki.

Każdy z zarządzanych obiektów należy do pewnej klasy nazywanej *klas zarządzanych obiektów MOC* (ang. *Managed Object Class).* Klasa ta określa *jeg* definicję. Obiekty należące do jednej klasy mają tę samą definicję, jednak każdy, nich stanowi inne wystąpienie tej klasy nazywane *wystąpieniem zarządzanego obiektu MOI* (ang. *Managed Object Instance).*

3.5.2 Atrybuty obiektów zarządzanych

Atrybuty obiektu zarządzanego określają jego podstawowe cechy, które odróżniają go od innych obiektów danej klasy, takie jak:

- nazwa,
- typ,
- wartość (zbiór wartości).

Przykład atrybutów zarządzanych obiektów.

Obiektem zarządzanym jest: *centrala telefoniczna.* Charakteryzuje ją ***atrybut*** o nazwie: *stan operacyjny*, który jest wyrażony ***typem***, w tym przypadku określonym jako: *tekstowy.*

Wartość atrybutu odnosząca się do stanu (np. *czynna* lub *nieczynna)* może być wyrażona liczbowo, jeśli określi się typ wartości atrybutu np. *liczbę całkowitą,* wówczas wartość może wynosić: *1, 2, 3, ...itp.*

Wartość atrybutu może ulec zmianie:

- na skutek pobudzenia zewnętrznego - czyli operacji lub akcji przeprowadzonej na obiekcie,
- na skutek pobudzenia wewnętrznego - czyli w wyniku wewnętrznych zdarzeń występujących w obiekcie, np.: przekroczenie ustalonej wartości progowej atrybutu.

3.5.3 Operacje i akcje

Operacje i akcje są czynnościami, które mogą zostać wykonane na obiekcie przez agenta na polecenie zarządcy.

W tabeli 1.przedstawiono wykaz operacji i akcji realizowanych przez zarządcę M *(ang. Manager)* w stosunku do zarządzanych obiektów MO.

Tabela 1 Operacje i akcje realizowane przez zarządcę w stosunku do zarzadzanych obiektów.

Nr	Czego dotyczy	Typ operacji/akcji	Charakterystyka działań
1.	Dotyczą operacji na zarządzanych obiektach	*Create:*	Utworzenie nowego obiektu
2.		*Delete:*	Usunięcie danego obiektu
3.		*Action:*	Zlecenie obiektowi wykonania akcji, czyli czynności, którą dany obiekt wykonuje na innych obiektach (również na sobie samym). Efektem wykonania akcji przez obiekt może być modyfikacja wartości atrybutów obiektów. Należy podkreślić, że w odróżnieniu od operacji, które zarządca wykonuje na obiektach za pośrednictwem agenta, akcje wykonuje zarządzany obiekt na innych zarządzanych obiektach (również na sobie samym)
4.	Dotyczą operacji na atrybutach obiektów	*Get Value:*	Odczyt bieżącej wartości atrybutu obiektu
5.		*Replace Value:*	Zmiana bieżącej wartości atrybutu
6.		*Replace with default Value:*	Zmiana bieżącej wartości atrybutu na wartość domyślną
7.		*Add Member:*	Dodanie wartości do zbioru wartości atrybutu wielowartościowego
8.		*Remove Member:*	Usunięcie wartości ze zbioru wartości atrybutu wielowartościowego.

3.5.4 Zachowanie i meldunki

Zachowanie określa:

- reakcję zarządzanego obiektu na przeprowadzoną na nim operację,
- znaczenie atrybutów, operacji, meldunków i innych elementów definicji obiektu,
- zależności między wartościami atrybutów i warunki spójności atrybutów,
- warunki, które muszą być spełnione przed i po wykonaniu operacji oraz wysłaniu meldunku,
- efekty oddziaływań z innymi obiektami,
- atrybuty, których wartość nie ulega zmianie na czas istnienia obiektu.

Meldunek jest wysyłany przez zarządzany obiekt w celu poinformowania o zdarzeniu dotyczącym obiektu lub zaobserwowanym przez obiekt.

3.5.5 Dostęp do zarządzanych obiektów

Definicje zarządzanych obiektów przechowuje się w ***bazie informacji zarządzania MIB*** *(ang. Management Information Base).*

Identyfikacja zarządzanych obiektów w bazie MIB jest możliwa dzięki hierarchicznemu ***drzewu informacji zarządzania MIT*** *(ang.Management Information Tree).*

3.6 Charakterystyka drzewa informacji zarządzania MIT

Każdemu węzłowi drzewa MIT przyporządkowana jest *etykieta* (ang. *label),* która określa nazwę obiektu.

Struktura drzewa może zmieniać się dynamicznie.

Określenie obiektu przez podanie samej tylko etykiety węzła nie jest jednoznaczne i tak określona nazwa obiektu jest *nazwą względnie rozróżnialną RON.* Dla jednoznacznego zdefiniowania obiektu w całej strukturze drzewa MIT należy podać 'jego *nazwę globalnie rozróżnialną,* nazywaną również w skrócie *nazwą rozróżnialną DN.*

Nazwę DN otrzymuje się przez dodanie do siebie etykiet węzłów na drodze od korzenia drzewa MIT do węzła, w którym znajduje się nazwa RDN danego obiektu.

Drzewo MIT określa nazwy obiektów i z tego powodu jest nazywane *drzewem nazywania.*

3.7 Charakterystyka bazy informacji zarządzania MIB

Wyróżnia się następujące funkcje bazy informacji zarządzania:

- przechowywanie wszelkich informacje zarządzania,
- reprezentacja zasobów zarządzanego systemu przez tzw. obiekty zarządzania.

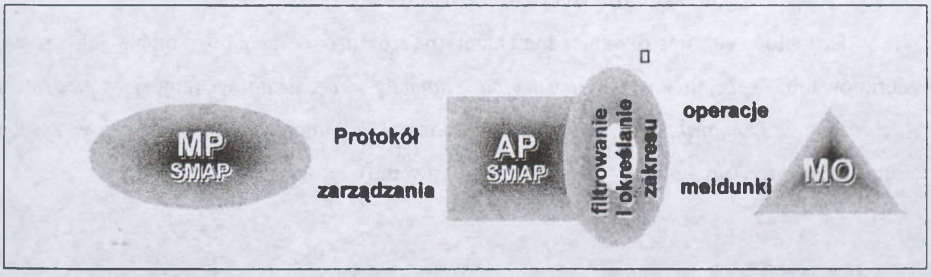
Należy zaznaczyć, że:

- struktura logiczna (abstrakcyjna) MIB jest określona przez standardy ISO/OSI,
- sposób implementacji i struktura wewnętrzna nie podlega standaryzacji TMN.

3.8. Filtrowanie i określanie zakresu

W ramach wykonywania usługi wspólnej informacji zarządzania (CMIS) na zbiorze obiektów zarządzania dokonywana jest selekcja, w ramach której:

- pierwszy etap polega na określeniu zakresu obiektów do dalszego przetwarzania w ramach usługi (zakres określa podzbiór zarządzanych obiektów na podstawie ich miejsca w drzewie nazywania, czyli na podstawie ich nazwy),
- drugi etap polega na odfiltrowaniu z wybranego zakresu obiektów spełniających pewne kryteria (filtrowanie pozwala wybrać podzbiór zarządzanych obiektów na postawie ich atrybutów).



Rysunek 18 Filtrowanie i określanie zakresu

Określanie zakresu pozwala odpowiedzieć na pytanie „*Które obiekty?*, natomiast ***filtrowanie*** pozwala odpowiedzieć na pytanie „*Jakie obiekty?*"

Po uzgodnieniu ostatecznego zbioru obiektów wykonywana jest na nim usługa CMIS z uwzględnieniem sposobu synchronizacji operacji na wszystkich wybranych obiektach.

Wybieranie zakresu *(ang. scoping)* może się odbywać w następujących wariantach:

- jedna instancja - jedynie obiekt bazowy,
- potomkowie obiektu bazowego na n-tym poziomie poddrzewa,
- obiekt bazowy oraz wszyscy potomkowie do n-tego poziomu włącznie,

- obiekt bazowy oraz wszyscy potomkowie - całe poddrzewo.

Po wybraniu zakresu powstaje tzw. zbiór SMO *(ang. scoped management objects).*

Filtrowanie jest to zestaw warunków dotyczących wartości lub obecności atrybutów w obiektach zbioru SMO.

Filtrowanie może odnosić się zarówno do operacji jak i meldunków.

Filtr może określać:

- jakich obiektów ma dotyczyć dana operacja,
- jakie meldunki (pochodzące od jakich obiektów) mają być przekazywane procesowi zarządzającemu.

3.9. Domeny zarządzania

Ze względów organizacyjnych zarządzane obiekty mogą być grupowane w *domenach zarządzania* (ang. *Management Domains).*

Do obiektów danej domeny stosuje się jednolity sposób zarządzania. Kryterium włączania obiektu do danej domeny jest dowolne, może nim być na przykład jego położenie geograficzne lub funkcje, jakie pełni (np. domena obiektów związanych z zarządzaniem konfiguracją). Dany obiekt może jednocześnie należeć do wielu domen.

Do celów administrowania domenami (nadzór nad domenami, zmiana ich granic) zdefiniowano specjalną *administracyjną domenę zarządzania* (ang. *Management Administrative Domain).* Obiekty należące do domeny administracyjnej podlegają wszystkie jednej organizacji (np. jednemu operatorowi krajowemu).

4 Charakterystyka funkcjonalna sieci zarządzania telekomunikacją – TMN

Sieć zarządzania telekomunikacją TMN *(ang. Telecommunications Management Network)* jest uniwersalną strukturą organizacyjną, wraz z regułami jej funkcjonowania, umożliwiającą realizację efektywnego wielopoziomowego (przedsiębiorstwo telekomunikacyjne – system telekomunikacyjny – sieć telekomunikacyjna – element sieci – użytkownik) zarządzania w różnych perspektywach czasowych (zarządzanie taktyczne – strategiczne – operacyjne) i różnych dziedzinach (ruch – uszkodzenia – usługi) opracowaną i doskonaloną przez ITU–T dla potrzeb podmiotów działających na rynku telekomunikacyjnym (operatorów telekomunikacyjnych, dostawców i subskrybentów usług, producentów sprzętu, użytkowników).

Pojęcie sieci zarządzania telekomunikacją zostało wprowadzone przez CCITT, obecnie ITU –T, w 1988 r. w rekomendacji M.30, następnie było rozszerzane i aktualizowane w latach 1988 – 1992, czego rezultatem było opublikowanie rekomendacji M.3010 *Principles for a telecommunications management network*. [4],[6], [11].[13], [15],[36]

Należy zaznaczyć, że TMN nie jest konkretnym rozwiązaniem technicznym lecz zbiorem zasad funkcjonalnych i organizacyjnych umożliwiających zarządzanie systemami, sieciami i urządzeniami telekomunikacyjnymi/teleinformatycznymi wykonanymi w różnych technologiach, z zastosowaniem różnych mechanizmów zarządzania i sterowania.

Celem wprowadzenia TMN jest ujednolicenie sposobu reprezentacji informacji o zarządzanym elemencie w systemie zarządzania, zbioru wspólnych komend służących do komunikacji między zarządzanym elementem i systemem zarządzającym.

TMN umożliwia zbieranie, przetwarzanie i przesyłanie danych dotyczących kontroli, nadzoru i utrzymania sieci telekomunikacyjnych.

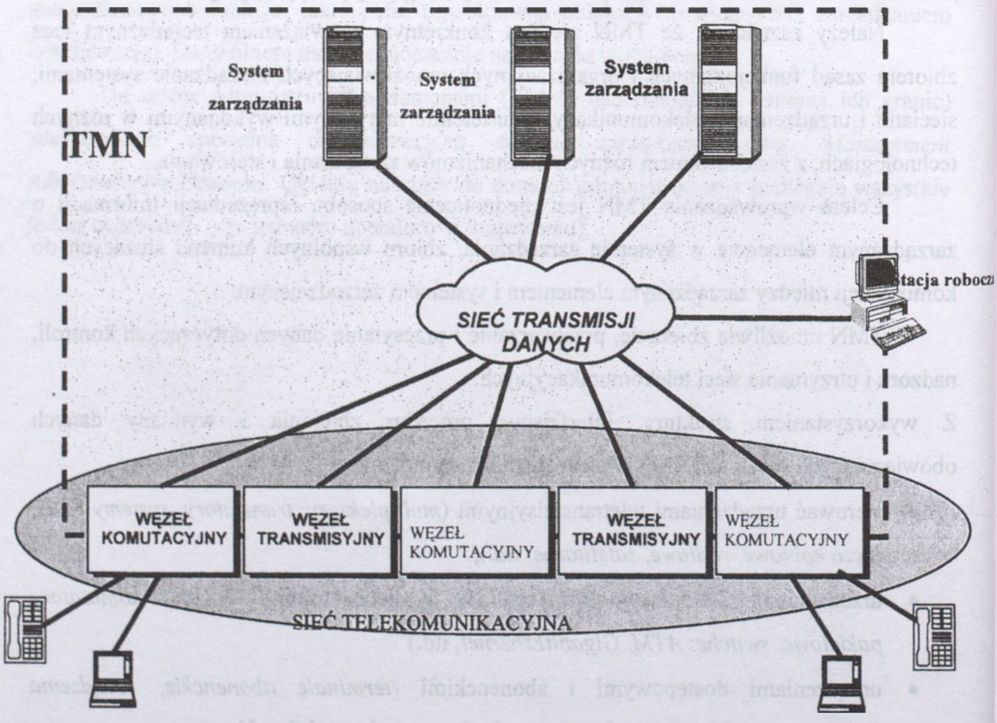
Z wykorzystaniem struktury, interfejsów, procedur zbierania i wymiany danych obowiązujących w ramach TMN system zarządzania może:

- sterować urządzeniami teletransmisyjnymi (*multipleksery, translatory, systemy SDH, łącza kablowe, radiowe, satelitarne, itd.*),
- urządzeniami komutacyjnymi (centrale i koncentratory, *PABX, komutatory pakietowe, switche: ATM, GigabitEthernet*, itd.)
- urządzeniami dostępowymi i abonenckimi *(terminale abonenckie, urządzenia końcowe sieci IN, stacje robocze, terminale systemów mobilnych)*,

- urządzenia teleinformatycznymi (elementy sieci *LAN, MAN, WAN*: routery, switche, koncentratory, serwery: aplikacji i danych oraz elementy systemów bezpieczeństwa: firewall'e, systemy identyfikacji włamań),
- urządzeniami pomocniczymi (*zasilanie central, testery, urządzenia klimatyzacyjne, systemy alarmowe*),
- inne urządzenia (rozwiązania dedykowane).

Zasadniczą ideą TMN jest zapewnienie zorganizowanej struktury, umożliwiającej połączenie różnych systemów zarządzania *OS (ang. Operations Systems)* z elementami sieci *NE (ang. Network Element)* za pomocą standardowych protokołów i interfejsów, z wykorzystaniem dedykowanej do tego celu sici transmisji danych DCN *(ang. Data Communication Network).*

TMN umożliwia również łączenie ze sobą systemów zarządzania działających w obszarze telekomunikacji i teleinformatyki oraz dołączanie ich do innych systemów zarządzania np. zarządzania kryzysowego, systemów finansowo–księgowych, systemów zarządzania biznesowego.



Rysunek 19 Idea funkcjonowania sieci TMN

Stąd też TMN powinien realizować:

- wymianę informacji zarządzania między siecią telekomunikacyjną a siecią zarządzania,
- przesyłanie informacji zarządzania między komponentami TMN,
- konwersję formatu informacji zarządzania przesyłanej wewnątrz TMN do jednolitej postaci,
- przetwarzanie informacji zarządzania (np. analiza uzyskanej informacji zarządzania, odpowiednie reagowanie na otrzymaną informację),
- dostarczanie informacji zarządzania do jej użytkownika,
- przekształcanie informacji zarządzania do takiej postaci, która jest użyteczna i zrozumiała dla jej użytkownika,
- zapewnienie ochrony dostępu do informacji zarządzania.

TMN umożliwia dostrzegania problematyki zarządzania z różnych perspektyw, takich jak

- dziedzina działań zarządczych,
- czas,
- zasoby.

Mając na uwadze dziedzinę działań zarządczych w ramach TMN, na podstawie zalecenia ITU-T X.700, wyróżnia się :

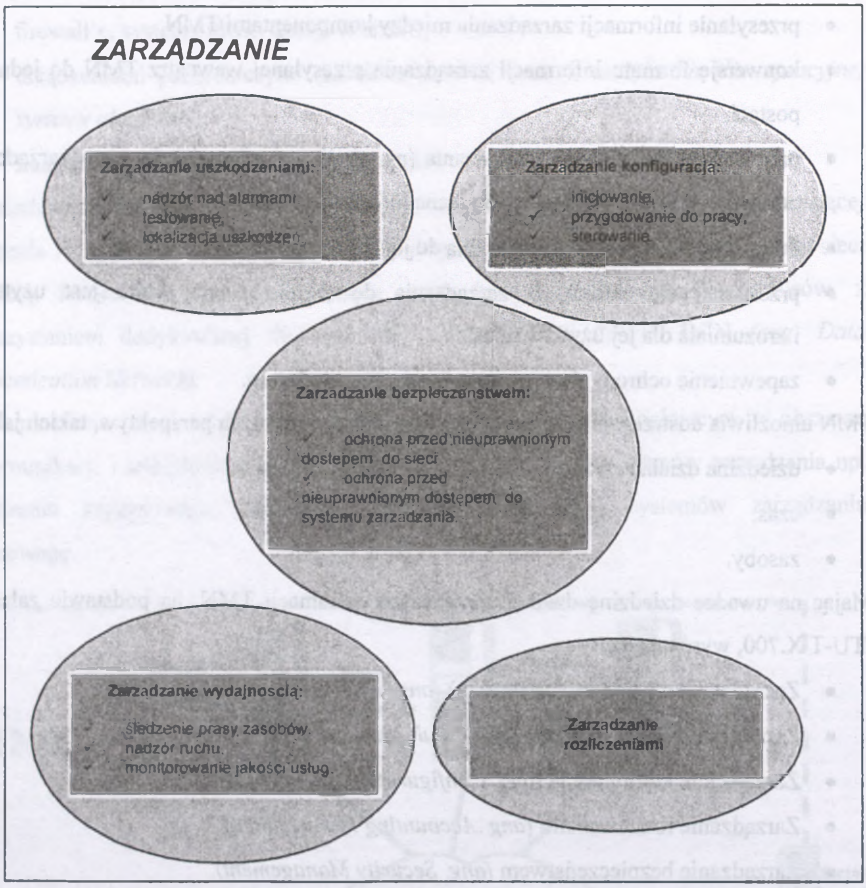
- Zarządzanie wydajnością (jakością) *(ang. Performance Management),*
- Zarządzanie uszkodzeniami *(ang. Fault Management),*
- Zarządzanie konfiguracją *(ang. Configuration Management),*
- Zarządzanie rozliczaniami *(ang .Accounting Management),*
- Zarządzanie bezpieczeństwem *(ang. Security Management).*

Podział ten został zilustrowany na rysunku.20.

Inny podział odnosi się do horyzontu czasowego realizowanych działań.

W ramach tego podziału wyróżnia się [15], [36]:

- Zarządzanie strategiczne *(ang. Strategical Management),*
- Zarządzanie taktyczne *(ang. Tactical Management),*
- Zarządzanie operacyjne *(ang. Operational Management).*



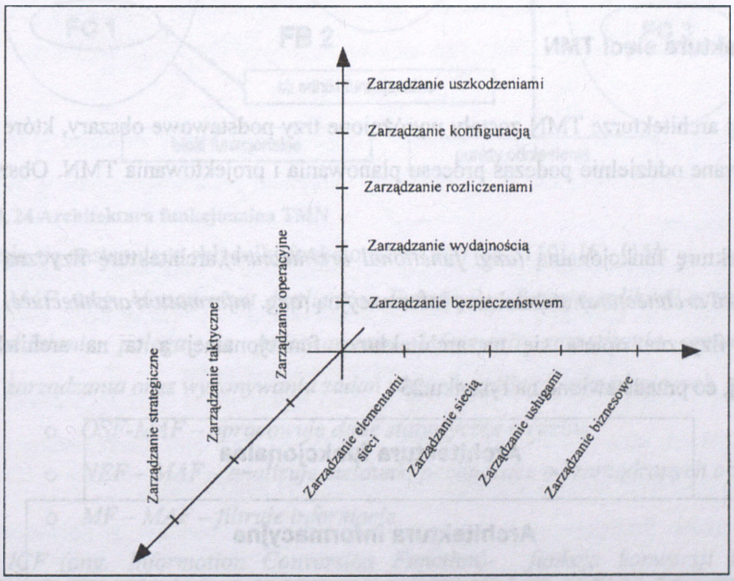
Rysunek 20 Działania zarządcze realizowane w ramach TMN

Mając na uwadze zarządzane zasoby można dokonać następującego podziału:

- Zarządzanie biznesowe (*ang. Business Management),*
- Zarządzanie usługami *(ang. Service Management),*
- Zarządzanie siecią *(ang. Network Management),*
- Zarządzanie elementem sieci *(ang. Network Element Management).*

Rysunek 21 Zarządzanie zasobami w TMN

Na rysunku ....przedstawiono różne spojrzenia na zarządzanie w telekomunikacji.



Rysunek 22 Perspektywy zarządzania w telekomunikacji

Warto zauważyć, że w trakcie realizacji codziennych działań zarządczych podmioty działające na rynku telekomunikacyjnym realizują jednocześnie szereg działań przypisanych do różnych perspektyw zarządzania.

Przykład. [4]

Dotyczy ilustracji rozumienia obszarów zarządzania zgodnie z ideą TMN.

Mamy na celu przeanalizowanie procesów działań TMN w odniesieniu do zarządzania siecią, w przypadku uszkodzenia węzła komutacyjnego.

Algorytm wykonywanych działań jest następujący:

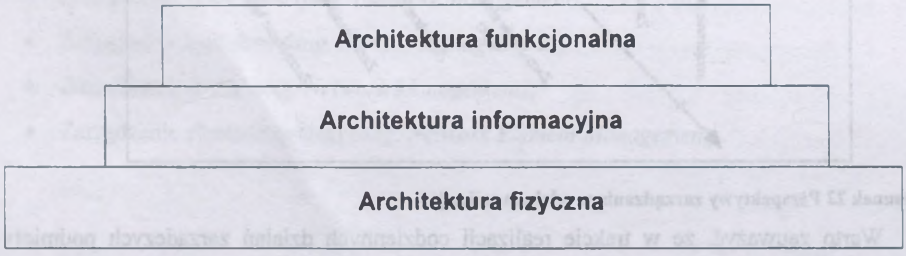
1. Wykrycie uszkodzenia - *zarządzanie uszkodzeniami,*
2. Wyłączenie węzła z sieci i skierowanie ruchu inną drogą - *zarządzanie konfiguracją,*
3. Rozesłanie komunikatu o możliwości przekłamań podczas komutowania przez uszkodzony węzeł - *zarządzanie bezpieczeństwem,*
4. Rozesłanie komunikatu o możliwości odpisania opłat za połączenia komutowane przez uszkodzony węzeł - *zarządzanie rozliczeniami,*
5. Naprawienie uszkodzonego węzła - *zarządzanie uszkodzeniami,*
6. Włączenie węzła po naprawie - zarządz*anie konfiguracją,*
7. Przeprowadzenie testów wydajności włączonego węzła - *zarządzanie wydajnością.*

4.1. Architektura sieci TMN

W ogólnej architekturze TMN zostały wyróżnione trzy podstawowe obszary, które mogą być rozpatrywane oddzielnie podczas procesu planowania i projektowania TMN. Obszary te obejmują:

- architekturę funkcjonalną *(ang. functional architecture),*architekturę fizyczną *(ang. physical architecture),*architekturę informacyjną *(ang. information architecture).*

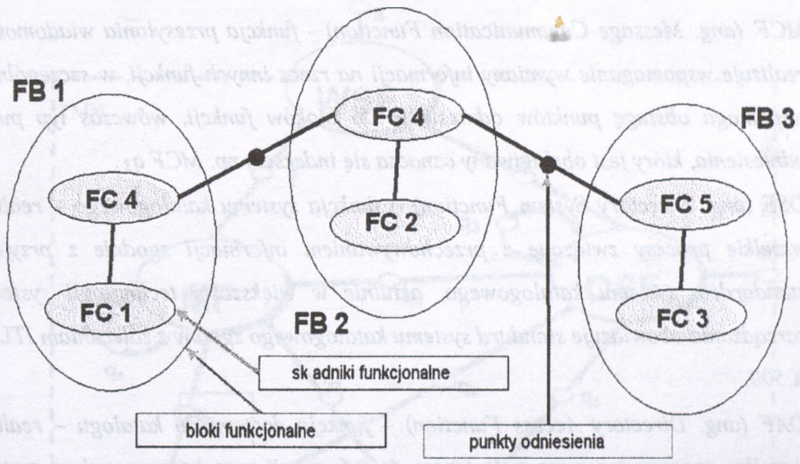
Architektura fizyczna opiera się na architekturze funkcjonalnej a ta na architekturze informacyjnej, co przedstawiono na rysunku.23



Rysunek 23 Architektury TMN

4.2. Architektura funkcjonalna TMN

Architektura funkcjonalna opisuje podstawowe funkcje TMN nazywane składnikami funkcjonalnymi FC *(ang. Functional Component).* Składniki funkcjonalne są elementarnymi (niepodzielnymi) funkcjami wyszczególnionymi w architekturze funkcjonalnej.
Składniki te łączone są w bloki funkcjonalne FB *(ang. Function Block),* pełniące określone funkcje. Miejsca symbolizujące powiązania między blokami określane są punktami odniesienia.
Idea działania architektury funkcjonalnej została przedstawiona na rysunku.24.



Rysunek 24 Architektura funkcjonalna TMN

Wyróżnia się następujące składniki funkcjonalne (FC) [M.3110], [6], [15]:

- *MAF (ang. Management Application Function) - funkcja aplikacji zarządzania – jej działanie polega na przetwarzaniu informacji zarządzania, realizacji usług zarządzania oraz wykonywaniu zadań różnych aplikacji zarządzających, np.:*
  - *OSF-MAF – opracowuje dane statystyczne o ruchu,*
  - *NEF – MAF – analizuje meldunki pochodzące od zarządzanych obiektów,*
  - *MF – MAF – filtruje informacje.*
- *ICF (ang. Information Conversion Function)- funkcja konwersji informacji – realizuje zamianę (konwersję) formatu informacji zgodnych z jednym modelem informacyjnym na format zgodny z innym modelem, zdefiniowanym dla innego interfejsu. We współczesnych systemach zarządzania zakładających szeroko pojętą otwartość i możliwość „nieskrępowanej" wymiany informacji ta funkcja jest szczególnie przydatna, gdyż umożliwia dokonanie zamiany (semantycznej i*

syntaktycznej) postaci informacji pomiędzy aktualnie wykorzystywanymi interfejsami takimi jak: q_3 lub g_x, m (TMN) – CORBA (OMG) – SNMP (IAB) – XML – XDR.

- *WSSF (ang. Workstation Support Function) – funkcja wspomagania stacji roboczej – realizuje działania ułatwiające personelowi odbiór, wprowadzanie, wizualizację i modyfikację informacji zarządzania oraz wspomagające personel w wydawaniu komend sterujących zarządzanymi zasobami.*
- *UISF (ang. User Interface Support Function) - funkcja wspomagania interfejsu użytkownika – dokonuje konwersji formatu informacji systemu zarządzania (systemów zarządzania) na postać akceptowalna przez WSSF.*
- *MCF (ang. Message Communication Function) - funkcja przesyłania wiadomości – realizuje wspomaganie wymiany informacji na rzecz innych funkcji, w szczególności wspomaga obsługę punktów odniesienia do bloków funkcji, wówczas typ punktu odniesienia, który jest obsługiwany oznacza się indeksem np. MCF q_3.*
- *DSF (ang. Directory System Function) – funkcja systemu katalogowego – realizuje wszelkie procesy związane z przechowywaniem informacji zgodnie z przyjętym standardem systemu katalogowego, aktulnie w większości technologii systemów zarządzania obowiązuje standard systemu katalogowego zgodny z zaleceniam ITU – T X.500.*
- *DAF (ang. Directory Access Function) – funkcja dostępu do katalogu – realizuje wszelkie procesu związane z dostępem do informacji przechowywanych w systemie katalogowym.*
- *SF (ang. Security Function) – funkcja bezpieczeństwa – zapewnia realizację usług bezpieczeństwa, zgodnych z ISO 7498-4: autentykacja, kontrola dostępu, poufność i integralność danych.*

Ze składników funkcjonalnych zbudowane są bloki funkcjonalne (FB). Oznacza to, że w zależności od zadań, jakie realizuje (lub będzie realizował) dany blok funkcjonalny w jego skład wchodzą określone, konkretne zdefiniowane składniki funkcjonalne.

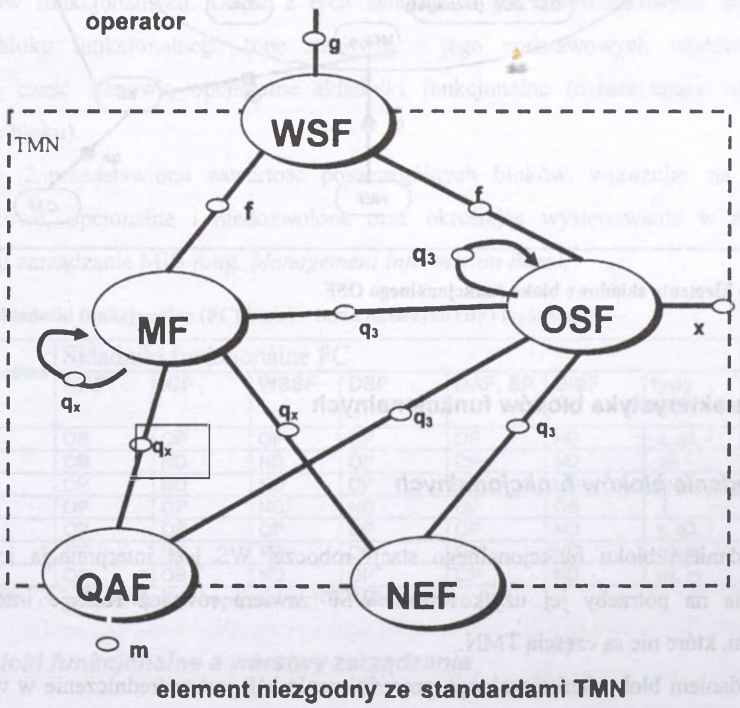
Tworzenie bloków funkcjonalnych przypomina budowanie obiektów z uniwersalnych, opracowanych wcześniej i dostępnych w TMN elementów (komponentów, składników) o ściśle zdefiniowanej funkcjonalności i określonym, zdeterminowanym sposobie użycia, realizacji powiązań i zadaniach. Tak jak budowanie nowych form z klocków „lego".

W podobny sposób tworzone są funkcje w sieciach inteligentnych IN *(ang. Inteligent Network)* oraz w sieciach następnej generacji NGN *(ang. Next Generation Network).*

Zalecenie M.3010 definiuje pięć bloków:

1. *Blok funkcjonalny systemów zarządzania OSF (ang. Operation Systems Function block),*
2. *Blok funkcjonalny pośredniczenia MF (ang. Mediation Function block),*
3. *Blok funkcjonalny adaptera Q QAF (ang. Q Adapter Function block),*
4. *Blok funkcjonalny elementu sieci NEF (ang. Network Element Function block),*
5. *Blok funkcjonalny stacji roboczej WSF (ang. Workstation Function block).*

Na rysunku 25 przedstawiono powiązanie bloków funkcjonalnych TMN [M.3010].

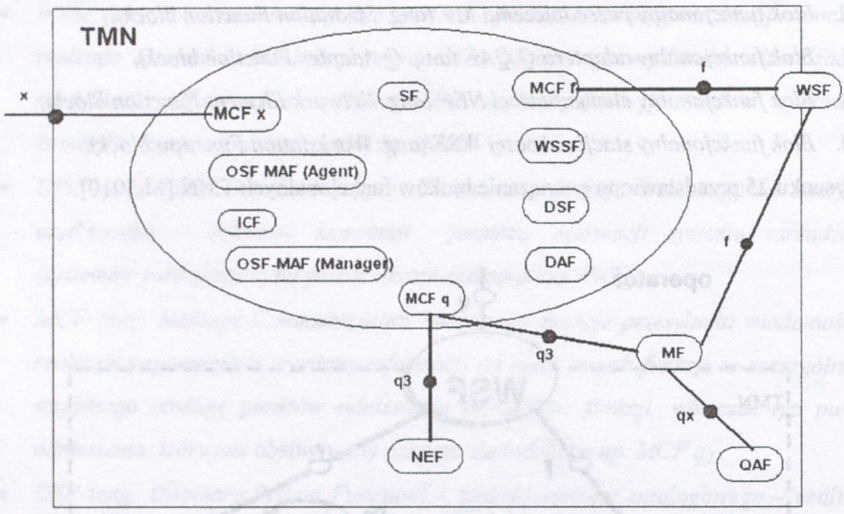


Rysunek 25 Powiązanie bloków funkcjonalnych TMN

Przedstawione na rysunku.25 powiązania wskazują na:

- zależność funkcyjną poszczególnych bloków w postaci przekazywania informacji umożliwiających realizację funkcji bloków,
- istnienie interfejsów *(q3 lub gx, m)* dedykowanych do obsługi określonych relacji pomiędzy blokami,
- możliwość samozasilania informacyjnego przez dany blok np. MF i OSF.

Dla przykładu, na rysunku.26 przedstawiono elementy składowe bloku funkcjonalnego systemów zarządzania OSF.



Rysunek 26 Elementy składowe bloku funkcjonalnego OSF

4.3. Charakterystyka bloków funkcjonalnych

4.3.1 Zadania bloków funkcjonalnych

Zadaniem bloku funkcjonalnego stacji roboczej WS jest interpretacja informacji zarządzania na potrzeby jej użytkownika. WSF zawiera również funkcje interfejsu z operatorem, które nie są częścią TMN.

Zadaniem bloku funkcjonalnego pośredniczenia MF jest pośredniczenie w wymianie informacji miedzy OSF i NEF (lub QAF) zapewniając dostosowanie informacji do potrzeb bloków funkcjonalnych dołączonych do MF.

MF może przechowywać, przystosowywać, filtrować, dokonywać kompresji informacji

Zadaniembloku funkcjonalnegosystemów zarządzania OSF jest przetwarzanie informacji związanych z zarządzaniem siecią telekomunikacyjną w obszarze monitorowania i sterowania funkcjami telekomunikacyjnymi oraz funkcjami zarządzania.

Zadaniem bloku funkcjonalnego elementu sieci NEF jest realizacja funkcji komunikacyjnych elementu zarządzanej sieci oraz funkcji utrzymaniowych niezbędnych w procesie zarządzania tym elementem. Funkcje komunikacyjne nie są częścią TMN, ale są reprezentowane przez NEF.

Zadaniem bloku funkcjonalnego adaptera Q QAF jest umożliwienie dołączenia do TMN systemów zarządzania i elementów sieci, które nie są zgodne ze standardem TMN. Więcej informacji na temat zadań poszczególnych bloków funkcjonalnych można znaleźć w [4].[13].[14],[15],[36].

4.3.2 Elementy składowe bloków funkcjonalnych

Każdy blok funkcjonalny składa się z określonych, zależnych od zadań bloku składników funkcjonalnych. Część z tych składników jest obowiązkowymi elementami danego bloku funkcjonalnego (one stanowią o jego podstawowych właściwościach), pozostałą cześć stanowią opcjonalne składniki funkcjonalne (rozszerzające możliwości użytkowe bloku).

W tabeli .2..przedstawiono zawartość poszczególnych bloków, wskazując na składniki obowiązkowe, opcjonalne i niedozwolone oraz określając występowanie w nich bazy informacji zarządzania MIB *(ang. Management Information Base).*[1]

Tabela 2 Składniki funkcjonalne (FC) bloków funkcjonalnych (BF) [czarnecki]

Bloki funkcjonalne FB	Składniki funkcjonalne FC							Obecność bazy MIB
	MAF	ICF	WSSF	DSF	DAF, SF	UISF	typy MCF	
OSF	OB	OP	OP	OP	OP	ND	x, q3, f	OP
NEF q3	OB	ND	ND	OP	OP	ND	q3	OB
NEF qx	OP	ND	ND	OP	OP	ND	qx	OB
WSF	OP	OP	ND	ND	OP	OB	f	OP
MF	OP	OB	OP	OP	OP	ND	x, q3, f	OP
QAF q3	OP	OB	ND	OP	OP	ND	q3, m	OP
QAF qx	OP	OB	ND	OP	OP	ND	qx, m	OP

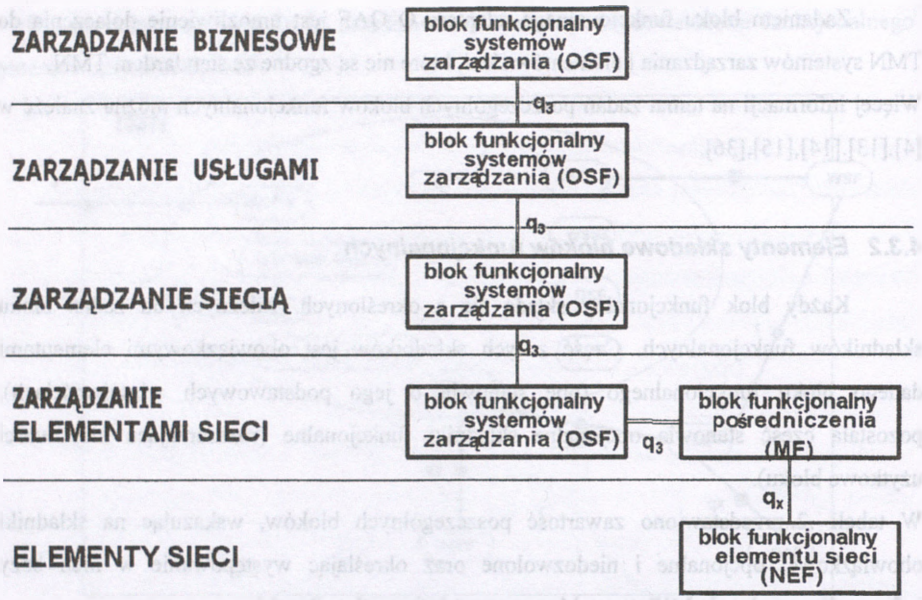
Legenda: OB – obowiązkowy, OP – opcjonalny, ND – nie dotyczy

4.3.3 Bloki funkcjonalne a warstwy zarządzania

Mając na uwadze perspektywę zarządzanych zasobów można dokonać przyporządkowania poszczególnych bloków funkcjonalnych BF do określonej warstwy. Takie przyporządkowanie określa złożoność oprogramowania użytkowego (aplikacji) realizującego poszczególne funkcje.

Przyporządkowanie bloków funkcjonalnych BF do warstw zarządzania poszczególnymi zasobami (biznesowej, usługowej, sieci i elementu sieci) zostało przedstawione na rysunku .27.

[1] MIB jest elementem informacyjnym gromadzącym dane dotyczące stanów zarządzanych obiektów.

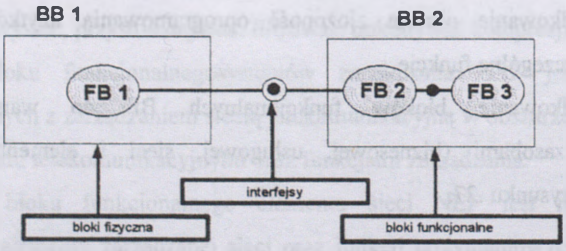


Rysunek 27 Przyporządkowanie bloków funkcjonalnych BF do warstw zarządzania zasobami

4.4. Architektura fizyczna TMN

Architektura fizyczna, scharakteryzowana w zaleceniu ITU – T M.3010, opisuje sposób implementacji funkcji TMN w zasobach fizycznych. Zasoby te dzielone są na bloki fizyczne BB *(ang. Building Bloks)*, które w zależności od pełnionych funkcji, zawierają wybrane bloki funkcjonalne BF. Bloki fizyczne wymieniają między sobą informacje poprzez standardowe interfejsy.

Koncepcję realizacji architektury fizycznej TMN przedstawiono na rysunku 28.



Rysunek 28 Architektura fizyczna TMN

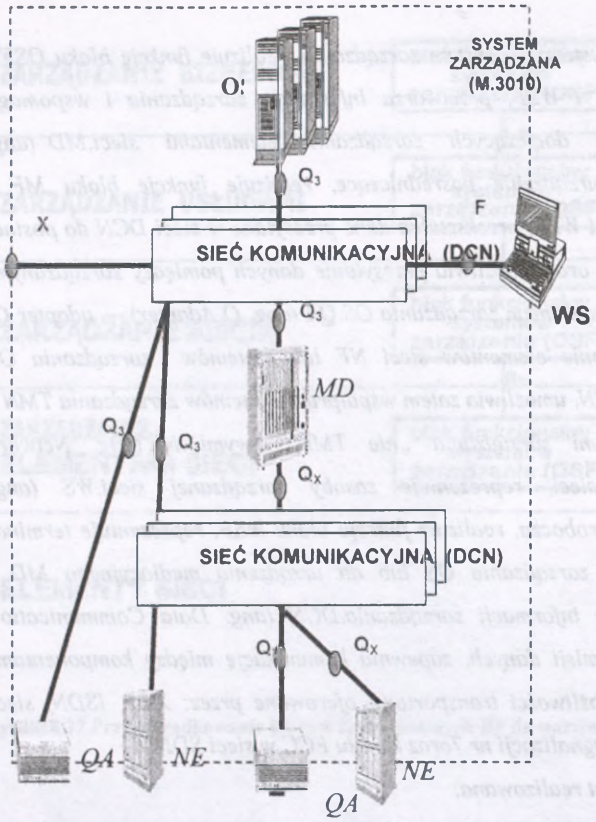
Wyodrębnia się następujące bloki fizyczne TMN:

1. *OS (ang. Operations System) — system zarządzania, realizuje funkcje bloku OSF i ewentualnie MF, QAF i WSF, przetwarza informacje zarządzania i wspomaga podejmowanie decyzji dotyczących zarządzania elementami sieci.MD (ang. Mediation Device)— urządzenie pośredniczące, realizuje funkcje bloku MF i ewentualnie OSF, QAF i WSF, przekształca dane przesyłane w sieci DCN do postaci akceptowanej przez OS oraz umożliwia przesyłanie danych pomiędzy zarządzanymi elementami sieci NE a systemem zarządzania OS.QA (ang. Q Adapter) — adapter Q, jego funkcją jest łączenie elementów sieci NE lub systemów zarządzania OS niekompatybilnych z TMN, umożliwia zatem współpracę systemów zarządzania TMN z elementami i systemami zarządzania „nie TMN –owymi".NE (ang. Network Element) — element sieci, reprezentuje zasoby zarządzanej sieci.WS (ang. Workstation) — stacja robocza, realizuje funkcje bloku WSF, reprezentuje terminal dołączony do systemu zarządzania OS lub do urządzenia mediacyjnego MD i umożliwia interpretację informacji zarządzania.DCN (ang. Data Communication Network) — sieć transmisji danych, zapewnia komunikację między komponentami TMN, wykorzystując możliwości transportowe oferowane przez: X.25, ISDN, sieci MAN, sieci WAN, sieć sygnalizacji nr 7oraz kanału FCC w sieci SDH.*

   W praktyce sieć DCN jest realizowana:

   - *w oparciu o sieć transportową (użytkową), świadczącą w ramach systemu telekomunikacyjnego usługi transmisyjne, w takim przypadku DCN również zarządza tą siecią – jest to rozwiązanie często spotykane, stosunkowo proste i tanie w realizacji, lecz wymagające posiadania w sieci użytkowej wolnych zasobów, właśnie na potrzeby DCN (warto zauważyć, że zasoby przydzielone dla DCN nie będą przynosiły dochodu, co stanowi jeden ze składników kosztów jej organizacji),*
   - *w oparciu o dedykowaną, specjalnie dla tego celu stworzoną sieć – rozwiązanie droższe i wymagające stworzenia oddzielnej, specjalnie zaprojektowanej struktury sieciowej.*

   Struktura fizyczna TMN została przedstawiona na rysunku 29.



Rysunek 29 Architektura fizyczna TMN

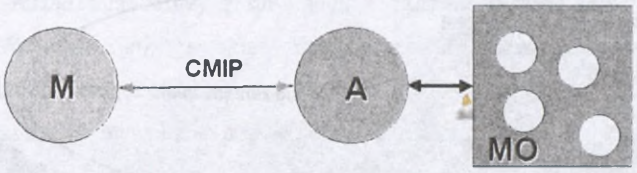
W strukturze TMN zostały określone następujące interfejsy:

- *interfejs Q składa się z następujących podklas:*
  - *interfejs Q3 — poprzez który do systemu zarządzania OS dołącza się inne systemy zarządzania danej sieci TMN, takie jak: MD, NE i QA. Protokoły związane z tym interfejsem zostały opisane w zaleceniach ITU-T Q.811 i Q.812*
  - *interfejs Qx — poprzez który do urządzenia mediacyjnego MD dołącza się inne urządzania pośredniczące, elementy sieci NE oraz adaptery QA. ITU – T nie narzuca konkretnych protokołów do obsługi tego interfejsu, pozostawiono swobodę wyboru protokołu,*
- *interfejs F — poprzez który stacja robocza (WS) dołączona jest do systemu operacyjnego (OS) i do urządzenia pośredniczącego (MD) za pośrednictwem sieci transmisji danych (DCN);*
- *interfejs X — służy do łączenia dwóch sieci TMN, lub do łączenia TMN z inną siecią zarządzania.*

Interfejsy zostały zilustrowane na rysunku 29.

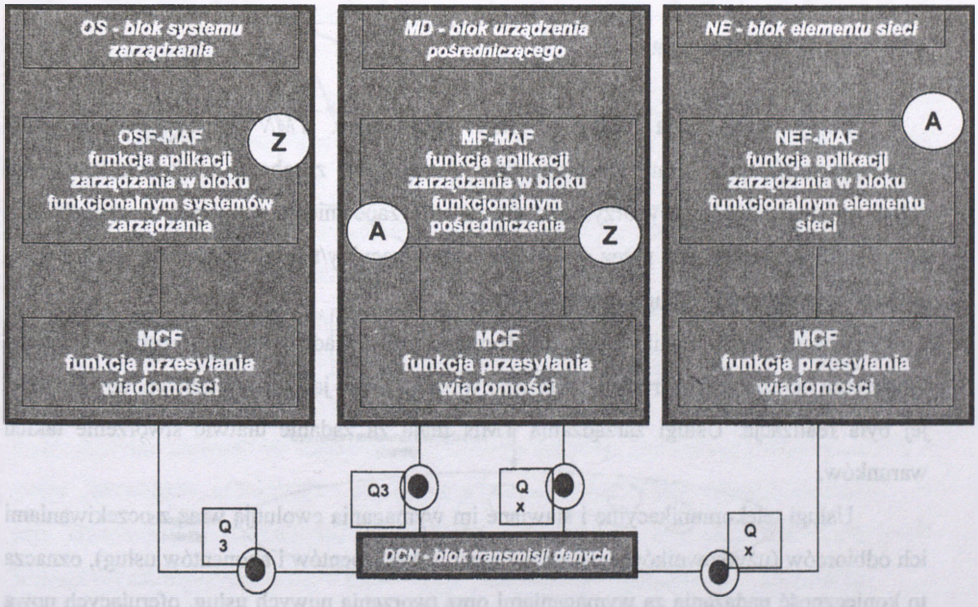
4.5. Architektura informacyjna TMN

Architektura informacyjna opisuje sposób modelowania wymiany informacji zarządzania, który jest oparty na modelu zarządca-agent *(ang. Manager – Agent)*. W dalszej części rozważań zarządcę będziemy oznaczać przez *Z* lub *M*, zaś agenta przez *A*., natomiast zarządzany obiekt MO *(ang. Managed Object)*. Architektura omawia również sposób modelowania zarządzanych zasobów przy zastosowaniu podejścia obiektowego.



Rysunek 30 Architektura informacyjna TMN

Model zarządca-agent architektury informacyjnej opisuje zależności w komunikacji pomiędzy blokami funkcjonalnymi i komponentami, został on przedstawiony na rysunku.31.

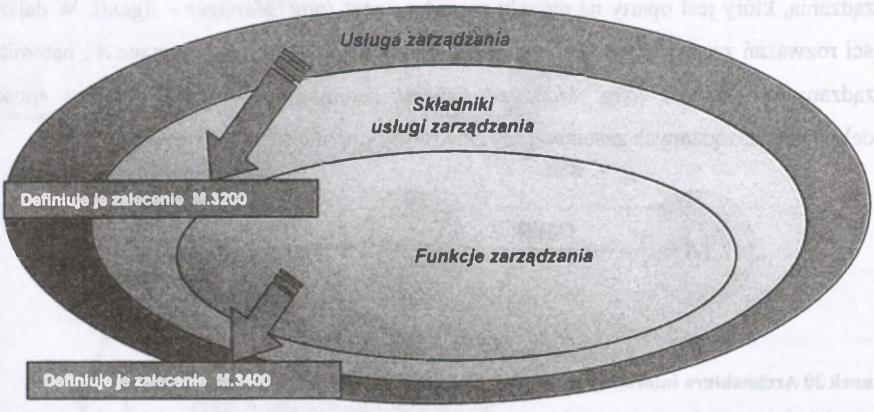


Rysunek 31 Model zarządca - agent w architekturze informacyjnej TMN

4.6. Usługa zarządzania TMN

Usługa zarządzania jest sferą działania dotycząca zarządzania telekomunikacją, opisana z punktu widzenia użytkownika systemu zarządzania.

Tak rozumianą usługę przedstawiono na rysunku..32.



Rysunek 32 Elementy składowe usługi zarządzania [4]

4.7. Usługi zarządzania

Usługi zarządzania TMN – TMN –MSs *(ang. TMN Management Services)* urzeczywistniają praktyczną realizację idei zarządzania zasobami telekomunikacyjnymi celem optymalizacji ich wykorzystania dla potrzeb zapewnienia wymaganych wskaźników jakości usług oferowanych przez system telekomunikacyjny/teleinformatyczny. Taki jest cel podstawowy tworzenia usług zarządzania TMN.

System telekomunikacyjny/teleinformatyczny świadczący daną usługę wymaga stworzenia określonych warunków, zarówno wewnętrznych jak i zewnętrznych, aby możliwa jej była realizacja. Usługi zarządzania TMN mają za zadanie ułatwić stworzenie takich warunków.

Usługi telekomunikacyjne i stawiane im wymagania ewoluują wraz z oczekiwaniami ich odbiorców (użytkowników systemów i sieci, subskrybentów i abonentów usług), oznacza to konieczność nadążania za wymaganiami oraz tworzenia nowych usług, oferujących nową funkcjonalność. Usługi telekomunikacyjne będąc atrakcyjniejszymi użytkowo stają się coraz bardziej złożone realizacyjnie, wymagają wykorzystania złożonych technologicznie metod.

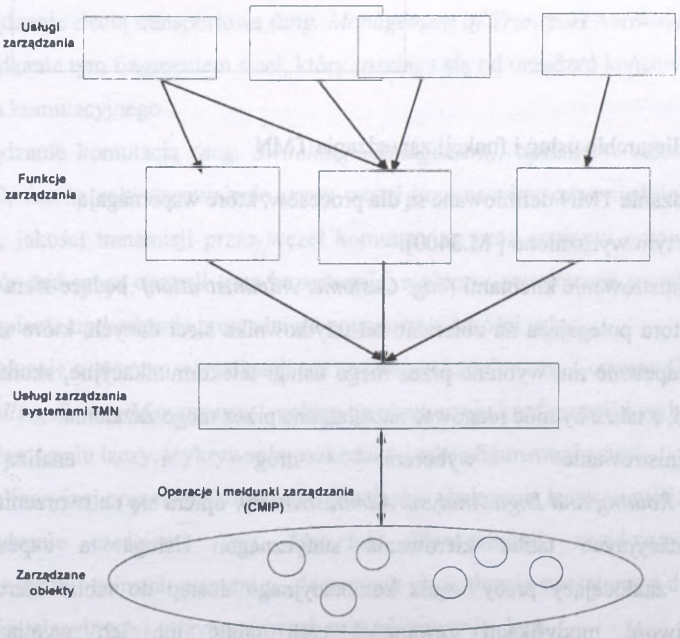
Dla systemów zarządzania i eksploatacji oznacza to konieczność opracowywania metod, technik i technologii, które nie ingerując w sposób udostępniania usługi telekomunikacyjnej oraz nie ograniczając jej właściwości użytkowych zapewnią wymaganą gotowość, żywotność, niezawodność oraz wysoką jakość na określonym poziomie.

Z tego powodu ITU –T cały czas pracuje nad identyfikacją potrzeb i definiowaniem nowych usług zarządzania TMN.

W zaleceniu M.3200 zostało zdefiniowanych szereg usług zarządzania, z których część została przedstawiona jedynie sygnalnie, „z nazwy" z zaznaczeniem, że będą one dokładnie określone w miarę pojawiających się potrzeb i rosnącego popytu na nowe usługi telekomunikacyjne, wymagające wsparcia w dziedzinach przez nie obsługiwanych.

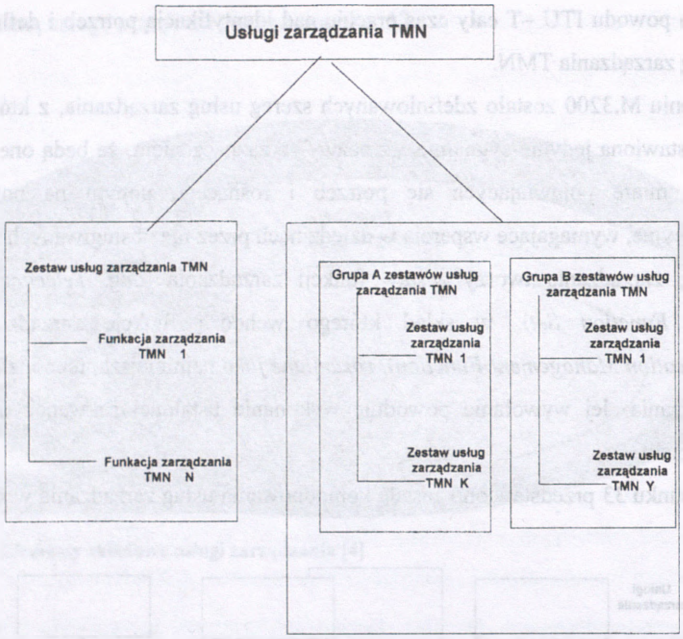
Usługę zarządzania tworzy zestaw funkcji zarządzania (*ang. Telecommunication Management Function Set),* w skład którego wchodzą funkcje zarządzania *(ang. Telecommunication Management Function), rozumiane jako* najmniejsza, niepodzielna część usługi zarządzania. Jej wywołanie powoduje wykonanie ustalonej sekwencji akcji przez zarządzany obiekt.

Na rysunku 33 przedstawiono zasadę komponowania usług zarządzania w środowisku TMN.



Rysunek 33 Zasada kompozycji usług zarządzania w środowisku TMN [15]

Hierarchię usług i funkcji zarządzania TMN przedstawiono na rysunku .34.



Rysunek 34 Hierarchia usług i funkcji zarządzania TMN

Usługi zarządzania TMN definiowane są dla procesów, które wspomagają.

W związku z tym wyróżniono [M.3400]:

1. Administrowanie klientami *(ang. Customer Administration)* ,będące sfera działalności operatora polegająca na zbieraniu od użytkownika sieci danych, które są potrzebne, aby zapewnić mu wybrane przez niego usługi telekomunikacyjne, skonfigurować te usługi, a także by móc reagować na zgłaszane przez niego zażalenia.
2. Administrowanie wyborem dróg i analizą cyfr *(ang. Routing and Digit Analysis Administration),* opiera się na tworzeniu *w* węzłach komutacyjnych tablic kierowania statycznego. Usługa ta zapewnia łatwy i nie zakłócający pracy węzła komutacyjnego dostęp do tablic kierowania oraz możliwość modyfikacji zawartości tych tablic lub ich wymiany zgodnie z wcześniej zdefiniowanym harmonogramem.
3. Administrowanie taryfami i naliczaniem opłat *(ang. Tariff and Charging Administration),* polega na tworzeniu, zbieraniu, uaktualnianiu i usuwaniu danych związanych z kosztami korzystania z usług sieci telekomunikacyjnej. Ważną rolę odgrywają metody weryfikacji poprawności naliczania opłat.

4. Zarządzanie ruchem *(ang. Traffic Management),* polega na zbieraniu informacji o ruchu od elementów sieci, przetwarzaniu tych informacji i rozsyłaniu poleceń rekonfiguracji sieci. Elementy sieci przesyłają informacje o ruchu okresowo lub, gdy zostanie przekroczony ustalony próg. Elementy sieci muszą być:
   - wyposażone wewnętrzny system pomiarowy umożliwiający zbieranie informacji o ruchu;
   - zdolne do przetwarzania zebranych informacji o ruchu i przedstawiania wyników w postaci ustalonych wskaźników;
   - zdolne do współpracy z systemami zarządzania, to jest do przesyłania wskaźników, odbierania poleceń i wykonywania ich.Zarządzanie dostępem klienta do sieci *(ang. Management of Customer Access),* obejmuje zarządzanie tym fragmentem sieci, który rozciąga się od urządzeń końcowych sieci do węzła komutacyjnego.
6. Zarządzanie siecią transportową *(ang. Management of Transport Networks),* obejmuje zarządzanie tym fragmentem sieci, który rozciąga się od urządzeń końcowych sieci do węzła komutacyjnego
7. Zarządzanie komutacją *(ang. Switching Management),* opisane w zaleceniach serii Q.500, ma na celu zapewnienie przez węzeł komutacyjny odpowiedniego poziomu usług, jakości transmisji przez węzeł komutacyjny oraz poziomu gotowości węzła. Nadzór nad pracą centrali trwa bezustannie, a alarmy generowane są wówczas, gdy wystąpienie uszkodzenia prowadzi do pogorszenia jakości usług.
8. Zarządzanie systemem sygnalizacji we wspólnym kanale *(ang. Common Channel Signalling System Management),* polega na planowaniu konfiguracji i wyboru dróg, wymiarowaniu łączy, wykrywaniu uszkodzeń i rekonfigurowaniu sieci sygnalizacyjnej oraz na wykonywaniu pomiarów obciążenia łączy sygnalizacyjnych.
9. Zarządzanie częściami *(ang. Materials Management),* znajdującymi się w magazynach i zainstalowanymi *w* elementach sieci ułatwia operatorowi dokonywanie prac instalacyjnych i utrzymaniowych oraz planowanie sieci.
10. Administrowanie pomiarami i analizą ruchu (ang. Traffic Measurement and Analysis Administration).
11. Zarządzanie bezpieczeństwem sieci TMN,
12. Zarządzanie sprzętem zlokalizowanym u klienta (*ang. Management of Equipment in Customer Premises),*
13. Administrowanie instalowaniem systemu (*ang. System Installation Administration),*

14. Administrowanie jakością usług i wydajnością sieci (*ang. QoS and Network Performance Administration)*,
15. Zarządzanie usługami kontrolowanymi przez klienta (*ang. Management of Customer Controlled Services)*,Zarządzanie sieciami inteligentnymi (*ang. Management of Intelligent Networks)*,.
17. Przywracanie i odtwarzanie (*ang.Restoration and Recovery)*,
18. Planowanie pracy personelu obsługującego (*ang. Staff Work Schedulling)*,
19. Zarządzanie siecią TMN (*ang. Management of the TMN).*

Poniżej przedstawiono omówienie funkcji zarządzania według obszarów zarządzania [M.3400].

Funkcje związane z zarządzaniem wydajnością

Zarządzanie wydajności (jakością) dostarcza funkcji do określania jakości pracy zarządzanej sieci i oferowanych usług.

Pozwala wnioskować o:

- funkcjonowaniu (skuteczności) sieci,
- oceniać funkcjonowanie sieci z punktu widzenia wydajności i jakości usług (QoS),
- opracowywać czynności korekcyjne.

Wyniki analizy często stanowią podstawę uruchomienia innych funkcji z innych obszarów, np. procedur testujących lub rekonfiguracji zasobów w celu zachowania zadanego poziomu jakości (wydajności).

Do funkcji związanych z zarządzaniem wydajnością należą:

1. Monitorowanie wydajności *(ang. preformance monitoring)*
   - funkcje ogólne, takie jak:
     - żądanie przesłania danych przez element NE,
     - przesłanie danych przez element NE,
     - przerwanie lub wznowienie przesyłania danych przez element NE,
   - funkcje monitorowania stanu ruchu, takie jak:
     - zgłoszenie dostępności elementu sieci,
     - zgłoszenie przeciążenia central,
     - zgłoszenie przeciążenia sieci sygnalizacyjnej,
   - funkcje monitorowania wydajności ruchowej, obejmujące:
     - przesłanie parametrów ruchowych dotyczących grup łączy,

- przesłaniem wyników pomiarów obciążenia i przeciążenia central oraz sieci sygnalizacyjnej.

2. Analiza wydajności *(ang. performance analysis)*, polegająca na przetwarzaniu i analizie danych dotyczących wydajności.
3. Sterowanie zarządzaniem wydajnością *(ang. performance management control)*, umożliwiające nadzorowanie procesu zarządzania wydajnością.

W tym zakresie wyróżnia się następujące grupy funkcji:

- funkcje ogólne, obejmujące:
  - ustalenie harmonogramu,
  - przesyłanie zgłoszeń dotyczących wydajności,
  - ustalenie wartości progowych,
  - uruchomienie lub ustalenie harmonogramu dotyczącego testów jakości QoS,
- funkcje sterowania ruchem, obejmujące uruchomienie, modyfikację i wyłączenie mechanizmów sterowania ruchem,
- funkcje administracyjne, obejmujące ustanowienie, modyfikację lub usunięcie harmonogramu pomiarów, utworzenie lub uaktualnienie bazy danych.

Funkcje związane z zarządzaniem uszkodzeniami

Zarządzanie uszkodzeniami obejmuje funkcje umożliwiające wykrywanie, izolację i poprawę nienormalnego funkcjonowania sieci telekomunikacyjnej i jej środowiska.Dostarcza procedur do:

- wykrywania błędów,
- nadzorowania informacji alarmowych,
- analizy logów z zapisami zdarzeń,
- testowania urządzeń,
- zarządzania informacjami o problemach w sieci,
- inicjalizacji operacji naprawczych.

1. Nadzorowanie alarmów (*ang. alarm surveillance*), polegające na realizacji następujących grup czynności:
   - przesyłanie alarmów, obejmujące:
     - wybór drogi dla zgłoszenia alarmu,
     - zezwolenie na zgłaszanie alarmów,
     - uniemożliwienie zgłaszania alarmów, podsumowywanie alarmów,ustalanie kryteriów alarmu,zarządzanie zawiadomieniami o alarmach,

- sterowanie dziennikiem.Lokalizowanie uszkodzeń *(ang. fault localisation)*, wykorzystuje funkcje przesyłania wyników testów diagnostycznych oraz funkcje ustalania harmonogramów testów rutynowych.

3. Naprawa uszkodzeń *(ang. fault correction),* związana z inicjacją działań naprawczych w systemie, takich jak: uruchomienie gorącej rezerwy (*ang. hot standby)* czy powtórne uruchomienie usługi.Testowanie (*ang. testing),* obejmujące:testowanie usług,
   - konfigurowanie dostępu dla testu, wraz z takimi działaniami jak zapewnienie, modyfikacja i zwolnienie dostępu urządzeń testujących do urządzeń testowanych,
   - konfigurowanie testowanych łączy,
   - sterowanie testowaniem, wraz z takimi działaniami jak dołączenie generatora sygnałów testowych, realizacja symulacji błędów transmisyjnych i symulacji powstawania uszkodzeń,
   - przesyłanie wyników testu,
   - zarządzanie ścieżką dostępu testowania,odtwarzanie sytuacji istniejącej przed testowaniem.5. Administrowanie zażaleniami (*ang. trouble administration),*

mające na celu wsparcie klientów w zakresie rozwiązywania problemów związanych z dostępem do sieci i korzystaniem z usług.

Funkcje związane z zarządzaniem konfiguracją

Funkcje z tej grupy pozwalają sprawować kontrolę nad siecią oraz zbierać i przechowywać dane o jej konfiguracji.

W zarządzaniu konfiguracją wyróżnia się podział na dwie dziedziny:na poziomie zarządzania usługami: tworzenie, udostępnianie usług o określonych parametrach (typ, czas trwania, szerokość pasma, jakość, itp.),

- na poziomie zarządzania zasobami (sieć + elementy): procedury rekonfiguracyjne sieci i/lub elementów w odpowiedzi na dynamiczne zmiany jej stanu lub w efekcie zmian planowych.

Na zarządzanie konfiguracją składa się:

1. Uruchamianie (*ang. provisioning*), obejmujące uruchamianie sprzętu po jego instalacji do stanu umożliwiającego świadczenie usług.

W ramach procesu uruchamiania można wydzielić następujące funkcje:

konfigurowanie elementów NE, wraz z działaniami:

- raportowanie o konfiguracji,
- raportowanie o dołączeniu nowego elementu,
- wykonywanie połączenia krosowego.

- administrowanie elementami NE,zarządzanie bazą danych o elementach.

2. Monitorowanie stanu i sterowanie elementami sieci *(ang. NE status and control)*, wraz z następującymi funkcjami:
   - funkcje ogólne, takie jak:
     - przesłanie zgłoszenia stanu,
     - ustalenie harmonogramu przesłania zgłoszeń stanu i harmonogramu dostępności usługi.
   - funkcje informujące o stanie elementu NE, a zwłaszcza o stanie sieci transmisyjnej, systemu dystrybucji wiadomości i stanie łączy dzierżawionych,
   - funkcje obsługujące instalację elementu NE.

Funkcje związane z zarządzaniem rozliczeniami

Zarządzanie rozliczeniami umożliwia obliczanie stopnia korzystania z zasobów (elementów i sieci) oraz usług wraz z kosztami z tym związanymi.

1. Zaliczanie *(ang. billing)*, polegające na naliczeniu poszczególnym klientom opłat za usługi.
2. Taryfikacja *(ang. taryffing)*, umożliwiająca określenie opłat za poszczególne usługi.*Funkcje związane z zarządzaniem bezpieczeństwem*

Zarządzanie bezpieczeństwem obejmuje mechanizmy zabezpieczające dostęp do zasobów telekomunikacyjnych systemu zarządzania oraz dostarcza administratorowi funkcji umożliwiających:1. Bezpieczeństwo dostępu (*ang. access security*),2. Ślady kontrolne (*ang. audit trails),*3. Alarmy bezpieczeństwa (*ang. security alarms),*4. Zgłaszanie akcji rewizyjnych (*ang. report audit actions),*5. Zarządzanie śladami kontrolnymi (*ang. management of audit trails),*6. Zażegnywanie włamań (*ang. intrusion recovery*),7. Informacje uwierzytelniające (*ang. credentials information*),8. Identyfikacja (*ang. identification*),9. Autentyfikacja (*ang. Authentificat.ion)*

5. Charakterystyka techniczno –użytkowa protokołu SNMP

Szczegółowa charakterystyka protokołu SNMP została zawarta w odnośnych dokumentach RFC, przytaczanych w dalszej części opracowania.
W opracowaniu tego rozdziału autor posiłkował się również informacjami przedstawionymi w [4], [6],[13], [14].

Prowadzenie rozważań dotyczących wykorzystania do zarządzania protokołu SNMP jest związane z przyjęciem modelu, który składa się trzech komponentów tj. ze struktury informacji SMI (ang. *Structure of Managment Information)*, bazy danych zarządzanych obiektów MIB (ang. *Managment Information Base*) oraz protokołu SNMP (ang. *Simple Network Managment Protocol).*

W opisanym modelu baza MIB zawiera szczegóły dotyczące obiektu, a protokół zapewnia komunikację pomiędzy agentem a zarządcą.

Protokół SNMP pomimo iż stanowi cześć rodziny TCP/IP jest nie zależny od protokołu IP i może być również używany np. w sieci Novell NetWare, wykorzystującej protokół IPX/SPX.

Przyjęty w 1990 roku standard SNMPv.1 została zdefiniowana w trzech dokumentach odpowiadających komponentom wymienionym powyżej tj. SMI w RFC1155, MIB w RFC 1212 i protokół SNMPv1 w RFC 1157.

Wersja 2 protokołu SNMP, ogłoszona w roku 1993 została zdefiniowana w ośmiu dokumentach RFC 1901-1908 i często określana jest jako SNMPv.2 framework.

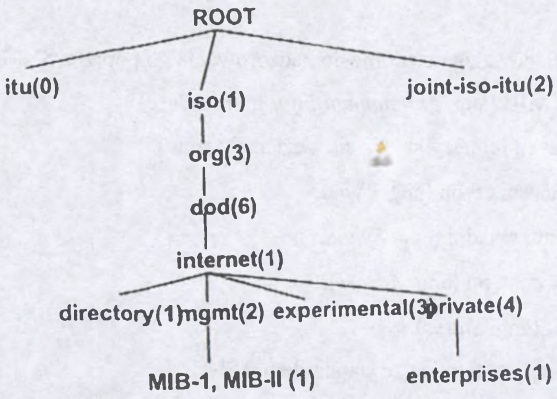
5.1 Struktura informacji zarządzania

Struktura informacji zarządzania SMI *(ang. Structure of Management Information)* zapewnia metodę do nadawania nazw obiektom i organizowania obiektów. Koncepcja, według której dokonywane jest umieszczanie obiektów w bazie MIB, wykorzystuje strukturę drzewa.

Obiekty w strukturze drzewa reprezentowane są poprzez kolejne gałęzie. SMI przypisuje każdemu obiektowi sekwencje liczb, które stanowią identyfikator, jednoznacznie identyfikujący obiekt w drzewie. Reprezentowane w ten sposób obiekty są zgodne z notacją ASN.1 (ang. *Abstract Syntax Notation),* która jest zalecana do stosowania w ramach współdziałania systemów otwartych zgodnych z RM OSI, określonym przez ISO.

Standard ASN.1 definiuje hierarchiczną przestrzeń nazw, dzięki czemu na podstawie nazwy każdej zmiennej można określić jej miejsce w hierarchii.

Hierarchię ASN.1 utworzono po to, aby prawo przyznawania nazw miało wiele organizacji. Na rysunku .35 przedstawiono schemat drzewa rejestracji nazw ASN.1.



Rysunek 35. Drzewo rejestracji nazw ASN.1.

W przedstawionej architekturze korzeń drzewa nie ma nazwy, ale ma gałęzie, które zwane są potomnymi. Różne organizacje i komitety standaryzacyjne administrują poszczególnymi gałęziami. Organizacja ITU-T, odpowiedzialna jest za gałąź 0, ISO za gałąź 1, natomiast zarówno ISO, jak i ITU-T są odpowiedzialne za gałąź 2.

W gałęzi *Internet* wszystkie identyfikatory obiektów zaczynają się od prefiksu {1.3.6.1}, co oznacza, że ich ścieżka od głównego korzenia prowadzi przez gałęzi iso, org, dod, Internet. Identyfikator Internet ma zdefiniowanych sześć obiektów tj. *directory(1), mgmt(2), experimental(3), private(4), security(5), SNMPv2(6).* Gałąź mgmt jest wykorzystywana przez IAB (ang.*Internet Activities Board*[2].)

SMI definiuje także typy danych dla SNMP tj. *NetWorkAddress, IPAddress, Counter, Gauge, TimeTicks.*

NetWorkAdress – reprezentuje adres charakterystyczny dla danej rodziny protokołów,

IPAddress - 32 bitowy adres internetowy,

Counter – licznik o pojemności 2^{32}-1, po czym jest następuje przepełnienie licznika,

Gauge - licznik o o pojemności 2^{32}-1, po czym jest następuje zatrzymanie licznika,

TimeTicks – licznik czasu reprezentowany przez nieujemną liczbę całkowitą, zliczający czas w setnych częściach sekundy.

[2] IAB (ang. Internet Activities Board)- jest organizacją zajmującą się zatwierdzaniem standardów w sieci Internet

5.2 Baza danych zarządzanych obiektów MIB

MIB definiuje informacje na temat obiektu, który jest zarządzany. Przyjęte zostały dwie wersje bazy MIB dla Internetu, MIB –1 w RFC 1156 oraz rozszerzona wersja MIB-2 w RFC 1213.

Każde urządzenie zdolne do nadzorowania go poprzez SNMP zawiera bazę informacji zarządzania MIB (ang. *Managment Information Base).*

Każda z pozycji tej bazy składa się z czterech części:

- oznaczenia typu (ang. *Type),*
- rodzaju składni (ang. *Synatax),*
- praw dostępu (ang. *Access*),
- stanu (ang. *Status*).

Struktura bazy jest zgodna ze standardem ASN.1.

Poszczególne pozycje oznaczają:

- Oznaczenie typu jest nazwą pozycji,
- Pole składni określa format wartości, na przykład łańcuch znaków lub liczba całkowita(nie wszystkie pozycje posiadają wartość),
- Pole praw dostępu określa dozwolony sposób korzystania z pozycji: tylko odczyt (ang. *Read Only)*, tylko zapis (ang. *WriteOnly)*, odczyt i zapis (ang. *Write/Read)* lub brak dostępu (ang. *NotAccessible),*
- Pole stanu określa czy dana pozycja musi zostać obowiązkowo wypełniona przez agenta (ang. *Mandatory)*, może zostać nie wypełniona (ang. *Optional)* lub nie jest już używana (ang. *Obsolete).*

Bazę MIB-1 wprowadzono w 1988 roku i zawiera ona 114 pozycji podzielonych na 7 grup. Urządzenie, aby uzyskać miano zgodnego z MIB-1 musi wypełniać wszystkie pozycje.

- Bazę MIB-2 wprowadzono w 1990 roku i zawiera ona 171 pozycji podzielonych na 10 grup. Grupy pochodzące z MIB-1 zostały rozszerzone, ponadto dodano trzy nowe grupy. Aby urządzenie uzyskało miano zgodnego z MIB-2, powinno być w stanie wypełnić wszystkie odpowiadające mu grupy.
- W tabeli 3 zostały zamieszczone zdefiniowane obecnie grupy.

Wprowadzenie bazy MIB-II spowodowało, że grupa AT wychodzi z użycia a funkcje przejęły grupy Transmission i SNMP.

Oprócz MIB-1 i MIB-2 niektórzy producenci sprzętu i oprogramowania (np. Hawlett Packard), stworzyli odrębne formaty MIB przeznaczone dla własnych produktów.

Tabela 3. Grupy zdefiniowane w bazie MIB-2

Grupa	ID obiektu	Opis
System	mib-2 1	Opis jednostki
Interface	mib-2 2	Liczba interfejsów sieciowych
At	mib-2 3	Tabele odwzorowań adresów fizycznych na adresy sieciowe
Ip	mib-2 4	Obsługa datagramów IP
Icmp	mib-2 5	Parametry i statystyki ICMP wejściowe i wyjściowe
Tcp	mib-2 6	Parametry i statystyki TCP wejściowe i wyjściowe
Udp	mib-2 7	Parametry i statystyki UDP wejściowe i wyjściowe
Egp	mib-2 8	Parametru i statystyki EGP wejściowe i wyjściowe
Transmission	mib-2 10	Parametry medium transmisyjnego
SNMP	mib-2 11	Parametry i statystyki SNMP

Jednym z przykładów jest MIB RMON wykorzystywany do zdalnego monitorowania pracy urządzeń sieci. Poniżej została zaprezentowana lista baz MIB zdefiniowanych przez IAB w odpowiednich dokumentach RFC (*ang. Request for Comments*). Należy dodać, że lista ta ciągle podlega modyfikacją ze względu na opracowywanie nowych baz MIB.

Tabela 4. Wykaz zdefiniowanych przez IAB baz MIB

RFC	Temat
1156	Management Information Base MIB-I
1212	Concise MIB Definitions
1213	Management Information Base MIB-II
1214	OSI Internet Management MIB
1315	DS1/E1 Interface Type MIB
1406	DS3/E3 Interface Type MIB
1407	Bridge MIB
1493	FDDI Interface Type MIB
1512	IEEE 802.3 Repeater MIB
1525	Source Routing Bridge MIB
1559	Decnet Phase IV MIB
1659	Rs-232 Interface type MIB
1660	Parallel Printer Interface Type MIB
1694	SMDS Interface Protocol (SIP) Interface Type MIB
1695	ATM MIB
1742	AppleTalk MIB
1748	IEEE 802.5 Token Ring Interface Type MIB
1757	Remote Network Monitoring (RMON) MIB
1759	Printer MIB
1850	OSPF version 2 MIB

Standard MIB podaje definicje zmiennych, które muszą być udostępniane w systemie zarządzania. Zmienne zdefiniowane w standardzie MIB, nie zawsze muszą mieć odwzorowanie w strukturach danych używanych przez system, ale oprogramowanie SNMP musi w takim przypadku umieć zasymulować zmienną MIB (dokonać emulacji w oparciu o tablicę translacji).

Zmienne MIB można podzielić na dwie klasy:

- zmienne proste,
- tabele.

Zmienne proste odpowiadają liczbą całkowitym ze znakiem i bez znaku oraz ciągom symboli. Jako zmienne proste są traktowane także porcje informacji mające postać struktur w języku C i rekordów w języku PASCAL.

Tabele odpowiadają jednowymiarowym tablicom.

Rozmiar zmiennych prostych jest znany, natomiast rozmiar tabeli może się zmieniać w czasie. Jako przykład może posłużyć tablica ARP (*ang. Adress Resolution Protocol*), w której przechowywana jest informacja o komputerach podłączonych do sieci, informacja ta jest dynamicznie zmieniana i ciągle ulega zmianom.

Każdy element tabeli MIB może mieć wiele pól, które same mogą być zmiennymi prostymi lub tabelami.

Oprogramowanie SNMP, przy przesyłaniu i odbieraniu nie przesyła nazw a używa notacji liczbowej, gdyż jest ona bardziej zwarta i oszczędza miejsce w pakietach. W wersji liczbowej notacji ASN.1, każdej etykiecie w nazwie jest przypisana mała liczba całkowita, dzięki takiej reprezentacji zmienna jest reprezentowana jako ciąg liczb. Przykładowo ciąg etykiet liczbowych dla nazwy zmiennej ipInRecives wygląda tak:

1.3.6.1.2.1.4.3

Jeżeli taki ciąg pojawia się w komunikacje SNMP i reprezentuje zmienną prostą to na końcu jest dodawane 0.

1.3.6.1.2.1.4.3.0

Oprogramowanie SNMP obsługuje tylko zmienne MIB dlatego wszystkie nazwy zmiennych mają ten sam prefiks, który można pominąć (iso, org, dod, internet, mgmt, mib) lub liczbowo (1.3..6.1.2.1).

Dzięki takiej reprezentacji system zarządzania po sprawdzeniu prefiksu i upewnieniu się, że nazwa rzeczywiście odnosi się do zmiennej MIB, może używać wewnętrznie tylko pozostałej części nazwy. Podobnie postępuje klient może oszczędzać czas dostając wspólny prefiks, gdy wszystko jest przygotowane do wysłania komunikatu.

5.3 Budowa Simple Network Management Protocol

Początkowo protokół SNMP miał być protokołem przejściowym, w którym rozwiązaniem docelowym miała strategia zarządzania bazująca na OSI.

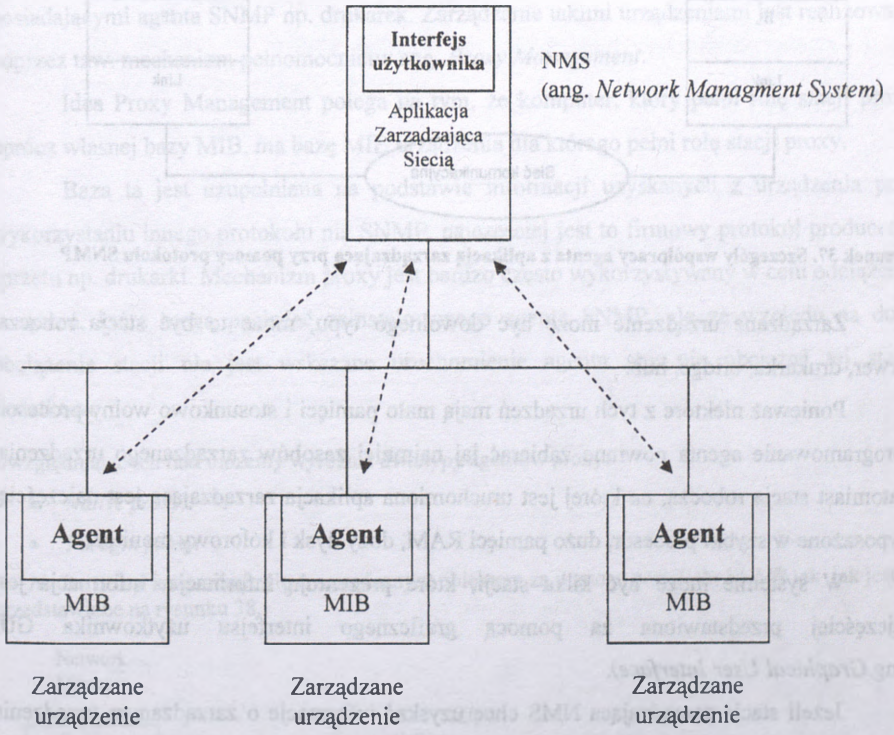
Uwzględniając obecny rynek produktów sieciowych można zauważyć, że SNMP jest stosowany na szeroką skale i stał się czymś więcej niż rozwiązaniem przejściowym. O tym jak popularny jest protokół SNMP może świadczyć fakt, że producenci urządzeń sieciowych i

komputerów wprowadzają oprogramowanie SNMP do oprogramowania firmowego zapisywanego w pamięci stałej. Urządzenia tego typu określa się często mianem *SNMP-Compliant*.

Trwające obecnie prace nad bazami danych MIB dla nowych technologii sieciowych.

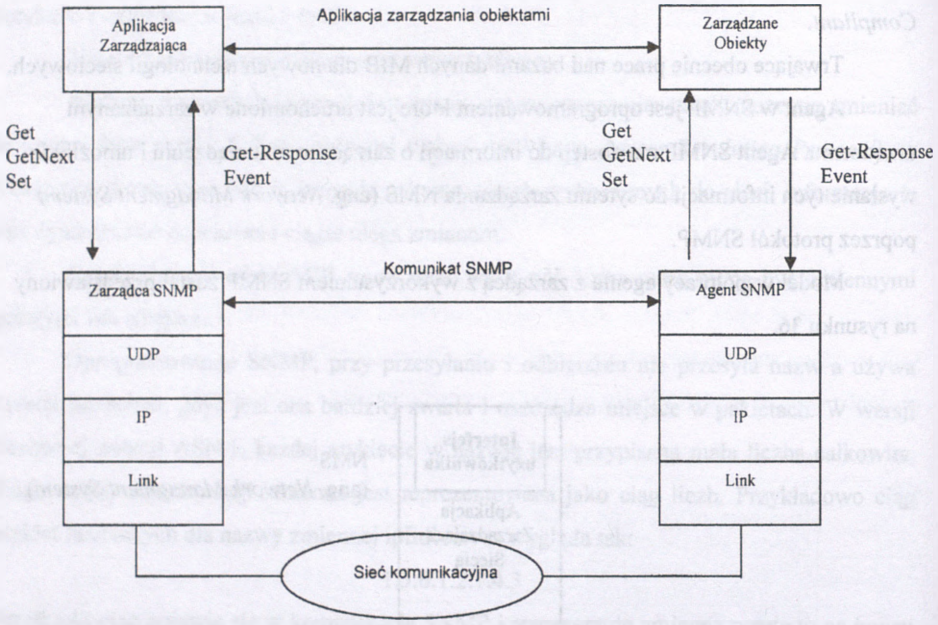
Agent w SNMP jest oprogramowaniem które jest uruchomione w zarządzanym urządzeniu. Agent SNMP ma dostęp do informacji o zarządzanym urządzeniu i umożliwia wysłanie tych informacji do sytemu zarządzania NMS (ang. *Network Managment System)* poprzez protokół SNMP.

Model współpracy agenta z zarządcą z wykorzystaniem SNMP został przedstawiony na rysunku 36.



Rysunek 36. Model współpracy agenta z aplikacją zarządzającą siecią NMS

Szczegóły współpracy aplikacji zarządzającej siecią NMS z agentem są przedstawione na rysunku 37.



Rysunek 37. Szczegóły współpracy agenta z aplikacją zarządzającą przy pomocy protokołu SNMP

Zarządzane urządzenie może być dowolnego typu, może to być stacja robocza, serwer, drukarka, bridge, hub.

Ponieważ niektóre z tych urządzeń mają mało pamięci i stosunkowo wolny procesor, oprogramowanie agenta powinno zabierać jaj najmniej zasobów zarządzanego urządzenia. Natomiast stacja robocza, na której jest uruchomiona aplikacja zarządzająca jest najczęściej wyposażone w szybki procesor, dużo pamięci RAM, duży dysk i kolorowy monitor.

W systemie może być kilka stacji, które prezentują informacje. Informacja jest najczęściej przedstawiona za pomocą graficznego interfejsu użytkownika GUI (ang.*Graphical User Interface).*

Jeżeli stacja zarządzająca NMS chce uzyskać informacje o zarządzanym urządzeniu wysyła zapytanie o interesujące ją informacje (zapytanie sformalizowane w postaci poleceń SNMP) dotyczące urządzenia zarządzanego. Urządzenie zarządzane odpowiada na pytanie.

Protokół stanowi synchroniczną aplikacje klient/serwer. Oznacza to, że zarówno klient i serwer mogą generować żądania, na które oczekują odpowiedzi.

Jednostkami komunikacyjnymi dla protokołu SNMP są datagramy UDP (ang. *User Data Protocol*) a protokołem sieciowym najczęściej IP (*ang. Internet Protocol)*, przy czym może być wykorzystywany inny np. IPX/SPX.

Komunikacja zarządcy z agentem nadzorowanego urządzenia odbywa się za pośrednictwem portu 161 (z wyjątkiem komunikatu Trap, kierowanego do portu 162.).

SNMP jest protokołem warstwy aplikacji, zaprojektowanym z myślą o wymianie informacji zarządzającej pomiędzy urządzeniami w sieci. Używając SNMP możemy mieć dostęp do takich informacji jak na przykład:

- ile kolizji jest w sieci,
- jak dużo pakietów zostało przesłanych przez sieć,
- informacje o błędnych pakietach..

Administrator sieci może w ten sposób łatwiej zarządzać siecią i szybciej rozwiązywać powstałe problemy.

Dużą zaletą protokołu SNMP jest możliwość zarządzania urządzeniami nie posiadającymi agenta SNMP np. drukarek. Zarządzanie takimi urządzeniami jest realizowane poprzez tzw. mechanizm pełnomocnictw ang. *Proxy Management*.

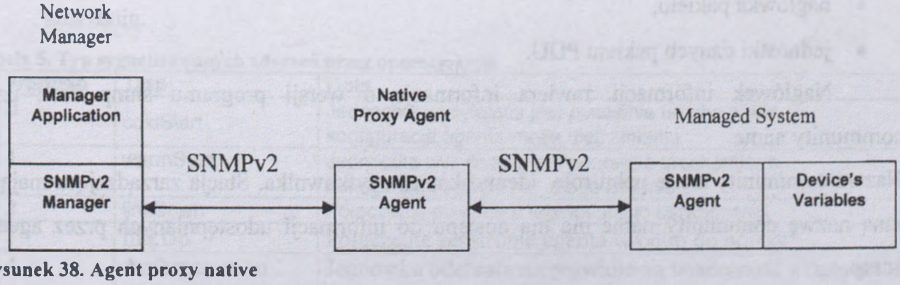
Idea Proxy Management polega na tym, że komputer, który pełni rolę stacji proxy oprócz własnej bazy MIB, ma bazę MIB urządzenia dla którego pełni rolę stacji proxy.

Baza ta jest uzupełniana na podstawie informacji uzyskanych z urządzenia przy wykorzystaniu innego protokołu niż SNMP, najczęściej jest to firmowy protokół producenta sprzętu np. drukarki. Mechanizm proxy jest bardzo często wykorzystywany w celu odciążenia urządzeń, które mogą posiadać zainstalowanego agenta SNMP, ale ze względu na duże obciążenie stacji nie jest wskazane uruchomienie agenta aby nie obciążać tej stacji dodatkowo.

Uwzględniając ten fakt możemy wyróżnić dwa typy agentów proxy:

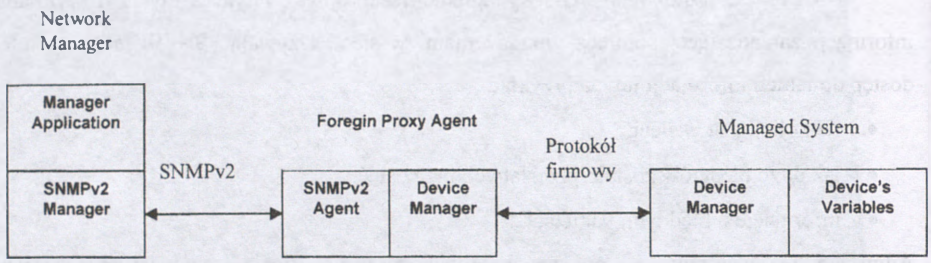
- *Native proxy,*
- *Foregin proxy.*

Native proxy komunikuje się z zarządzanym obiektem za pomocą protokołu SNMP tak ,jak jest to przedstawione na rysunku 38.



Rysunek 38. Agent proxy native

Foreign Proxy komunikuje się z zarządzanym obiektem za pomocą innego protokołu niż SNMP, co jest przedstawione na rysunku 39..



Rysunek 39. Agent proxy foregin

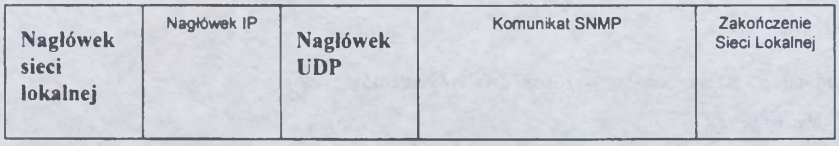
Poniżej zostaną scharakteryzowane dwie wersje protokołu SNMP:

- SNMPv.1
- SNMPv.2.

5.3.1 Protokół SNMP v.1

Jak już zostało wspomniane komunikat SNMP wykorzystuje protokół UDP, w którym po nagłówku umieszczona jest treść komunikatu.

Format ramki zawierającej komunikat SNMP jest przedstawiony na rysunku 40.



Rysunek 40. Komunikat SNMP wewnątrz przesyłanej ramki

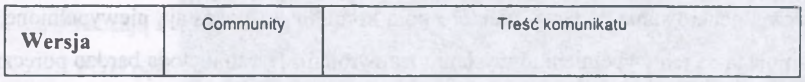
Komunikat w SNMPv.1 składa się z dwóch części:

- nagłówka pakietu,
- jednostki danych pakietu PDU.

Nagłówek informacji zawiera informacje o wersji programu snmp oraz tzw. community name.

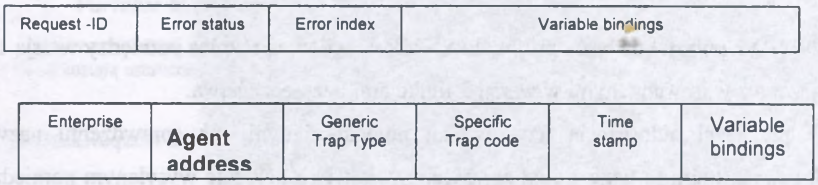
Nazwa community name pełni role identyfikatora użytkownika. Stacja zarządzająca mająca inną nazwę community name nie ma dostępu do informacji udostępnianych przez agenta snmp.

Struktura komunikatu SNMP v1 jest przedstawiona na rysunku 41.



Rysunek 41. Komunikat SNMP

Format części, która zawiera treść komunikatu dla funkcji get, get-next, set oraz dla funkcji trap.jest przedstawiony na rysunku 42.



Rysunek 42. Format jednostki danych dane w protokole SNMPv1

Zapytania get, get-next, set w wersji 1 protokołu SNMP zawierają następujące pola.

- ***Reguest-ID*** – identyfikator zapytania,
- ***Error status*** – status błędu,
- ***Error index*** – indeks błędu,
- ***Variable bindings*** – przypisane zmienne.

Komunikat Trap zawiera następujące pola:

- ***Enterprise-ID*** – pole identyfikuje obiekt, który wysłał informacje o zdarzeniu,
- ***Agent address*** – adres obiektu, który wysłał informacje o zdarzeniu,
- ***Generic trap type*** –informacja o typie zdarzenia, obecnie zdefiniowanych jest siedem możliwych wartości tego pola, przedstawionych w tabeli 5..
- ***Specific trap code*** - informacja o szczegółach zdarzenia,
- ***Time stamp*** – znacznik czasu pozwala na określenie czasu w jakim nastąpiło uszkodzenie,
- ***Variable bindings*** –listę zmiennych które zawierają informacje o zaistniałym zdarzeniu.

Tabela 5. Typ sygnalizowanych zdarzeń przez operacje trap

Wartość	Trap	Opis
0	coldStart	Jednostka wysyłająca jest ponownie uruchamiana, konfiguracja agenta może ulec zmianie
1	warmStart	Jednostka wysyłająca jest ponownie uruchamiana, konfiguracja agenta nie ulega zmianie
2	linkDown	Połączenie po stronie agenta uległo uszkodzeniu
3	linkUp	Połączenie po stronie agenta wróciło do normy
4	Authentication Failure	Jednostka odebrała nieprawidłową wiadomość z danymi do weryfikacji
5	egpNeighborLoss	EGP nie działa
6	enterpriseSpecific	Zdarzenie zdefiniowane przez producenta sprzętu

Podczas generowania żądania, niektóre pola komunikatu pozostają niewypełnione, a odpowiedz polega na ich wypełnieniu i wysłaniu z powrotem. Jest to metoda bardzo poręczna gdyż rozwiązuje problem istnienia skomplikowanego oprogramowania odszukującego zapytanie związane z otrzymaną właśnie odpowiedzą.

5.3.2 Protokół SNMP v.2

SNMP v2 powstał na bazie protokołu SNMP v1. Główna różnica pomiędzy wersją 1 a 2 jest związana z wprowadzonymi w wersji 2 funkcjami bezpieczeństwa.

W wersji pierwszej autoryzacja użytkownika polegała jedynie na sprawdzeniu nazwy *community name*, która to nazwa była przesyłana w każdym pakiecie wysyłanym pomiędzy aplikacją zarządzającą a agentem oraz identyfikacji stacji zarządzającej w aplikacji agenta poprzez umieszczenie wpisu w pliku konfiguracyjnym informacji dotyczącej stacji, która ma dostęp do usług agenta SNMP. W wersji 1 możliwe jest ustawienie opcji managment z wartością 32 stacji, które będą miały dostęp do funkcji agenta zaimplementowanego w zarządzanym urządzeniu.

Protokół SNMPv2 dostarcza kilka nowych typów danych i nową koncepcje odczytywania zmiennych typu tablica. Typ adres sieciowy w wersji może mieć długość 64 bitów w przeciwieństwie do obecnie stosowanego adresu sieciowego, który mógł być tylko 32 bitowy.

SNMP v2 wprowadza dwa dodatkowe komunikaty:

- ***InformRequest*** – struktura komunikatu jest taka sama jak pozostałych komunikatów, a umożliwia zarządcy wysyłać informacje o zdarzeniu do innego zarządcy i oczekiwać odpowiedzi,
- ***GetBulkRequest*** – struktura komunikatu jest odmienna od pozostałych, komunikat umożliwia odczytanie większej porcji informacji np. całą tablice bez konieczności pobierania informacji po jednej pozycji.

Ogólna koncepcja współpracy aplikacji zarządzającej z agentem jest taka sama jak w przy wykorzystaniu protokołu SNMP w wersji 1.

Wszystkie jednostki danych PDU z wyjątkiem *GetBulkRequest* mają ten sam format jednostki danych PDU. Postać jednostki danych jest przedstawiona na rysunku 43.

PDU type	Request ID	Error status	Error index	Variable bindings

Rysunek 43. Format jednostki danych PDU dla operacji Get, Get-next, Inform, Response, Set, Trap

Pola oznaczają :

- ***PDU type*** –podaje informacje o typie pakietu PDU,
- ***Request ID*** – identyfikator komunikatu, dokonuje powiązania odpowiedzi z pytaniem,
- ***Error status*** – status błędu,
- ***Error index*** – indeks błędu,
- ***Variable bindings*** - listę zmiennych.

Pole error status i error index mają wartość zero gdy wysyłamy komunikaty get, get-next, set, trap, inform. Pole te zostają ustawione tylko w przypadku otrzymania odpowiedzi.

GetBulkRequest używa jednostki danych PDU pokazanej na rysunku. 44.

PDU type	Request ID	No repeaters	Max-repetitions	Variable bindings

Rysunek 44. Format jednostki danych PDU dla operacji GetBulkRequest

Pola oznaczają:

- ***PDU type, Request ID, Variable bindings*** – spełniają tą samą funkcje jak dla komunikatu *Get, Get-next, Set, Response i Trap,*
- ***Norepeaters*** - podaje liczbę zmiennych, które występują w polu Variable bindings jako zmienne proste,
- ***Max repetitions*** – podaje liczbę zmiennych, które występują w polu Variable bindings jako tablice.

Należy zauważyć, że w wersji 2 protokołu SNMP komunikat *Trap* ma format jednostki danych PDU identyczny jak komunikaty *Get, Get-next, Set, Response*. Taki efekt uzyskano poprzez wprowadzenie w polu danych dwóch zmiennych, które jednoznacznie identyfikują obiekt zgłaszający komunikat.

Pierwsza zmienna ***sysUpTime.0*** podaje czas w którym nastąpiło zgłoszenie komunikatu i ***snmpTrapOID.0*** określająca obiekt zgłaszający komunikat.

Protokół SNMPv2 używa innej metody do zdefiniowania komunikatów typu trap niż protokół SNMPv1, który do tego celu wykorzystywał makro TRAP-TYPE.

W wersji 2 do zdefiniowania komunikatu *Trap* wykorzystywane jest makro NOFICATION-TYPE.

W celu zapewnienia współpracy z bazą MIB SNMPv1 musi nastąpić konwersja komunikatu z wersji 1 do 2 poprzez dokonanie następujących zmian:

- usuniecie klasy ENTERPRISES,
- zamiana klasy VARIABLES na klasę OBJECTS,
- dodanie klasy STATUS

- zmiana typu dla makra TRAP-TYPE z wartości INTEGER na wartość OBJECT IDENTIFIER, która jest wymagana przez makro NOTIFICATION-TYPE makro.

5.4 Bezpieczeństwo protokołu SNMP

Brak procedur bezpieczeństwa w stosowanym protokóle SNMP w wersji 1 był przyczyną, dla której cześć producentów sprzętu nie implementowało procedury set tym samym ograniczało to funkcje zarządzania do monitorowania obiektów bez możliwości dokonania zmian.

W wersji 2.0 są zaimplementowane procedury umożliwiające obronę przed:

- podszyciem się stacji nieuprawnionej pod stację zarządzającą,
- dokonanie zmian w treści komunikatu wysłanego przez stacje zarządzającą,
- możliwością skopiowania wcześniejszej odpowiedzi wysłanej przez stację zarządzającą w celu późniejszego jej wykorzystania poprzez modyfikacje czasu w pakiecie i wprowadzenie w błąd system zarządzania,
- ujawnieniem nazw i odpowiadających im wartości zarządzanych obiektów, uzyskując w ten sposób informacje o sieci.

Poniżej zostały przedstawione formaty komunikatów SNMP v.2. Na rysunku 45 zostały przedstawione formaty komunikatów bez zabezpieczenia, oraz pakiet z autoryzacją i szyfrowaniem.

Pakiet bez zabezpieczenia

Destination	Unused	Destination	Source	Contex	PDU

Pakiet autoryzowany

Destination	Digest	Destination Timestamp	Source Timestamp	Destination	Source	Context	PDU

Pakiet autoryzowany i szyfrowany

Dane są szyfrowane

Destination	Digest	Destination Timestamp	Source Timestamp	Destination	Source	Context	PDU

Rysunek 45. Format pakietu SNMP w wersji 2

W celu lepszego zrozumienia występujących różnic w przedstawionych formatach zostaną wyjaśnione poszczególne pola.

Pola oznaczają:

- ***Destination*** – identyfikator przeznaczenia, pole to ma dwa znaczenia. Pierwsze, które odnosi się do pola rozpoczynającego pakiet informuje gdzie dostarczyć wiadomość i drugie, które odnosi się do części, która jest szyfrowana.
- ***Source*** – identyfikacja nadawcy,
- ***Contex*** – odpowiednik community name pola z wersji 1,
- ***PDU*** –pole identyfikuje pożądane polecenie,
- ***Digest*** – wartość obliczona na podstawie części pola PDU według algorytmu message-digest,
- ***Destination timestamp*** – znacznik czasu odbiorcy, określa jaki czas upłynął od poprzedniej wymiany komunikatów miedzy nadawcą a odbiorcą,
- ***Source timestamp*** – zawiera znacznik czasu nadawcy,

Jak zostało zasygnalizowane wcześniej protokół SNMP v.2 może używać komunikatów :

- ***Nosecure*** – pole informujące że komunikat SNMP nie jest kodowany,
- ***Autentuicated but not private*** – zabezpieczony w ten sposób komunikat zapewnia że komunikat dotrze do jednostki uprawnionej. W algorytmie tym w polu ***Digest*** jest zapisywana informacja, która jest do odczytania przez jednostkę znającą prywatny klucz, który jest przechowywany na dysku lokalnym.
- ***Private and authenticated*** - zabezpieczony w ten sposób komunikat zapewnia, że informacja znajdująca się w treści komunikatu nie została zmodyfikowana. Stosowany mechanizm polega na obliczaniu dla każdego komunikatu pola ***Digest*** na podstawie zawartości pola danych. Odbiorca komunikatu po otrzymaniu komunikatu oblicza według tego samego algorytmu pole ***Digest*** i porównuje z odebranym, jeżeli występują różnice to komunikat jest odrzucany.

Nowy format komunikatów, stosowane procedury bezpieczeństwa sprawiają, że wersja 2 jest niekompatybilna z wersją 1. Pragnąc wykorzystywać urządzenia z agentami w wersji 1 i 2 najprostszym rozwiązaniem jest dokonanie upgrad'u aplikacji zarządzającej w celu zapewnienia współpracy. Jednak takie rozwiązanie wiąże się z dwoma problemami tj. z bazą danych i protokołem. W wersji 1 i 2 stosuje się notacje ASN.1 co zapewnia prawidłową współprace aplikacji zarządzającej w wersji 2 z agentami w wersji 1.

Dokonania translacji typów pomiędzy obiektami w SNMPv1 a SNMPv2. Występujące różnice w formacie komunikatów są do zaakceptowania przez stacje zarządzającą, natomiast agent w wersji 1 nie będzie obsługiwał komunikatów w ***GetBulkRequest*** oznacza to, że zmienne tablicowe będą musiały być odczytywane poprzez wykonywanie komunikatów ***GetNextRequest***.

6 Bezpieczeństwo zarządzania w telekomunikacji i teleinformatyce

Problematyka bezpieczeństwa systemów informacyjnych stanowi obszar dużego zainteresowania zarówno naukowego (opracowywanie nowych metod i technologii zwiększających bezpieczeństwo informacji w systemie), jak i organizacji standaryzacyjnych i urzędów państwowych odpowiedzialnych statutowo za ten rodzaj działalności. Zaowocowało to realatywnie duzą ilością publikacji i unormowań z tej dziedziny.

Dla potrzeb tego opracowania autor korzystał i posiłkował się wiedzą przedstawioną w [1],[2][3], [5], [7], [10],[12], [16].

Z pewnością można byłoby przytoczyć cały szereg pozycji literaturowych, które obejmują różne obszary szeroko rozumianego bezpieczeństwa informacyjnego, jednak mając na uwadze specyfikę systemów wspomagających zarządzanie w telekomunikacji i teleinformatyce postanowiono raczej rozszerzyć przedstwione poniżej rozważania o zagadnienia normatywne przedstwione w [19] – [34].

W informacyjnych systemach zarządzania, wykorzystywanych do wspomagania procesów zarządzania, utrzymania i administrowania systemami i sieciami telekomunikacyjnymi/teleinformatycznymi, ich zasobami oraz usługami przez nie świadczonymi można wydzielić następujące elementy:

- sprzęt,
- oprogramowanie,
- ludzie korzystający z systemu (użytkownicy i eksploatatorzy),
- procedury wykorzystania systemu i świadczenia usług.

Bezpieczeństwo tak zdefiniowanego systemu jest uzależnione od niezawodności sprzętu i oprogramowania, stopnia zaufania i odpowiedzialności ludzi korzystających z systemu (zarówno administratorów jak i użytkowników) oraz od skuteczności ustalonych zasad użytkowania i zarządzania systemem.

W dalszej części będziemy mając na myśli bezpieczeństwo zarządzania w telekomunikacji i teleinformatyce będziemy odnosić się do wszystkich aspektów bezpieczeństwa systemów informacyjnych występujących w szeroko rozumianym procesie zarządzania systemami, sieciami, zasobami, użytkownikami i usługami telekomunikacyjnymi i teleinformatycznymi.

W przypadku zarządzania systemami informacyjnych mamy do czynienia z następującymi zagadnieniami:

- zarządzanie bezpieczeństwem - wiąże się z zarządzaniem usługami i mechanizmami

bezpieczeństwa; jest to dostarczanie informacji zarządzania do tych usług i mechanizmów, jak i zbieranie oraz przechowywanie informacji o usługach i machanizmach, np.:

- zarządzanie kluczami (w tym dystrybucja klucza),
- dostarczanie sprawozdań dotyczących zdarzeń w systemie związanych z bezpieczeństwem (w tym informacji na temat przebiegu niektórych funkcji),

- bezpieczeństwo zarządzania - wiąże się z bezpieczną i rzetelną pracą sieci zarządzania (np.TMN); jest skomplikowanym, żmudnym (nie kończącym się) procesem; przykłady:
  - rzetelność informacji przechowywanych w bazach danych: ich dostępność, poprawność itp.,
  - odpowiedzialność od strony bezpieczeństwa za wszystkie poczynania związane z zarządzaniem,
- świadczenie usług ochrony informacji (bezpieczeństwa) - dostarczanie końcowym użytkownikom (klientom) usług bezpieczeństwa.

6.1 Potrzeba zabezpieczenia systemów zarządzania w telekomunikacji i teleinformatyce

W miarę jak podmiot świadczący usługi na rynku telekomunikacyjnym (operator, dostawca usług) zwiększa swe uzależnienie od technik informatycznych, w sposób naturalny zmniejszają się możliwości kontroli zasobów informacji, która jest przechowywana, przetwarzana, przesyłana i udostępniana w systemie.

Jednocześnie wzrasta wymierna wartość tych zasobów. Osoby odpowiedzialne za zarządzanie przedsiębiorstwami działającymi na rynku telekomunikacyjnym rzadko uświadamiają sobie ryzyko związane z utratą informacji i często nie dostrzegają znaczenia zabezpieczania swoich systemów informacyjnych, które są podstawowym elementem umożliwiającym „wytworzenie" oferowanych usług.

Prowadzenie przemyślanej polityki zabezpieczenia systemu informacyjnego (informatycznego i telekomunikacyjnego) może uchronić przedsiębiorstwa od poważnych kłopotów organizacyjnych i finansowych, wynikających z niewłaściwego funkcjonowania tych systemów.

Problem zabezpieczenia systemów informacyjnych przedsiębiorstw i podmiotów świadczących usługi telekomunikacyjne/teleinformatyczne nie doczekał się jeszcze całościowego opracowania. Istnieje obszerna literatura poświęcona technicznym aspektom

zarządzania zabezpieczeniem systemów informacyjnych, w szczególności analizie ryzyka. Znane i stosowane są zautomatyzowane eksperckie narzędzia analizy ryzyka. Najbardziej znanym systemem eksperckim jest CRAMM[3]. Podstawową wadą zautomatyzowanych systemów eksperckich jest przyjęcie założenia, że zabezpieczenie ma jedynie aspekt techniczny.

Tymczasem jest to problem z dziedziny zarządzania przedsiębiorstwem, a nie tylko techniki informacyjnej. Zatem zabezpieczenie systemu informacyjnego oparte jedynie na zautomatyzowanych narzędziach jest rozwiązaniem niekompletnym.

Dla systemu zabezpieczenia należy zdefiniować procesy zarządzania zabezpieczeniem *(security management),* które powinny być wbudowane w system zarządzania przedsiębiorstwem i dostosowane do procedur świadczenia usług, a ponadto powinny uwzględniać uwarunkowania technologiczne wynikające ze środowiska, w którym działają.

6.2 Bezpieczeństwo systemu informacyjnego

System informacyjny uznaje się za bezpieczny, jeśli gwarantuje spełnienie następujących kryteriów:

- **poufności** ***(confidentiality)***- zapewnia ochronę przed ujawnieniem informacji nieuprawnionemu odbiorcy,
- **integralności** ***(integrity)***- zapewnia ochronę przed modyfikacją lub zniekształceniem zasobów informacyjnych przez osobę nieuprawnioną,
- **dostępności** ***(availability)*** - zapewnia uprawniony dostęp do zasobów informacyjnych przy zachowaniu określonych rygorów czasowych,
- **rozliczalności** ***(accoutability)*** - zapewnia określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu informacyjnego,
- **autentyczności** ***(authentication)*** - zapewnia weryfikację tożsamości podmiotów lub prawdziwość zasobów systemu informacyjnego.
- **niezawodność** ***(reliability)*** – zapewnia gwarancję odpowiedniego/wymaganego zachowania się systemu informacyjnego w

[3] CRAMM *(CCTA Risk Analysis and Management Methodology)* - program komputerowy oparty na metodologii analizy i zarządzania ryzykiem opracowanej przez brytyjskie agencje rządowe i BIS Applied Systems Limited.

założonym środowisku eksploatacyjnym i określonym czasie.

Zabezpieczanie systemów informacyjnych obejmuje wszelkie działania związane ze zdefiniowaniem, osiągnięciem i utrzymaniem stanu spełnienia kryteriów zabezpieczenia.

6.3 Podstawowe usługi i mechanizmy ochrony informacji

Norma [ISO 7498-2] ochrona informacji w systemach otwartych określa następujące, podstawowe, uniwersalne usługi ochrony informacji:

- **kontrola dostępu** ***(ang. access control)*** - ochronę przed nieuprawnionym dostępem do zasobów,
- **integralność danych** ***(ang. data integrity)*** - gwarancję- spójności danych; ochronę przed modyfikacją, wtrąceniem, wymazaniem danych,
- **uwierzytelnienie** ***(ang. authentication)*** - kontrolę tożsamości stron lub danych wymienianych pomiędzy nimi np. podczas sesji komunikacyjnej,
- **niezaprzeczalność** ***(ang. non-repudation)*** - metodę rozstrzygnięcia ewentualnego sporu pomiędzy nadawcą a odbiorcą dotyczącego zarówno faktu nadania i odbioru informacji jak i jej treści,
- **poufność danych** ***(ang. confidentiality)*** - ochronę danych przed nieuprawnionym uzyskaniem przez strony nieupoważnione.

Kontrola dostępu jest pierwotna względem pozostałych usług, realizuje się ją przed wykorzystaniem zasobów.

Poufność może być zapewniona niezależnie od integralności, uwierzytelnienia i niezaprzeczalności.

Niezaprzeczalność zawsze wiąże się z uwierzytelnieniem, natomiast uwierzytelnienie z integralnością.

Dla systemów informacyjnych, oprócz wspomnianych podstawowych pięciu usług, wprowadza się ([ISO 10181-1]) usługę związaną w dużym stopniu z przetwarzaniem danych: **audyt i alarmy** ***(ang. security audit and alarms).***

Jest to zbiór metod umożliwiających wgląd do systemu oraz ocenę poprawności jego pracy z punktu widzenia bezpieczeństwa.

W modelu odniesienia ISO/OSI warstwa sesji, służąca do nawiązania połączenia jest

"uwolniona" od usług ochrony informacji. Poufność może być realizowana we wszystkich pozostałych warstwach. Kontrola dostępu, integralność danych, uwierzytelnienie będą zapewnione w warstwach: sieciowej, transportowej oraz prezentacji i aplikacji. Niezaprzeczalność będzie realizowana w warstwach najwyższych: prezentacji i aplikacji.

Usługi audytu i alarmów są stosowane do odnotowywania zdarzeń związanych z bezpieczeństwem występujących w środowisku systemów otwartych traktowanym jako całość.

Podstawowe usługi są budowane na bazie mechanizmów, określonych w normie ISO 7498-2, do których należą:

- **szyfrowanie**, które może zapewnić poufność informacji lub strumienia danych.

  Wyróżnia się dwie klasy algorytmów szyfrujących:
  - symetryczne (tj. z kluczem tajnym),
  - asymetryczne (tj. z kluczem publicznym),
- **podpis cyfrowy**, dla którego określa się dwie procedury:
  - podpisywanie - stosuje się informację, która jest unikalną i poufną (prywatną) własnością podpisującego,
  - weryfikację - stosuje się informację publicznie dostępną.
- **mechanizmy kontroli dostępu** - używane w celu określenia i przestrzegania praw dostępu do zasobów,
- **mechanizmy integralności danych** - używane do zachowania integralności danych (najczęściej korzysta się- z kryptograficznych sum kontrolnych - funkcji skrótu),
- **wymiana uwierzytelniająca** - używana do uwierzytelnienia stron, opiera się na trzech parametrach zmiennych w czasie:
  - na technice wyzwania,
  - znacznikach czasu,
  - liczbach kolejnych,
- **wypełnianie ruchu** - zapewnia ochronę przed analizami ruchowymi - np. ukrywa informację o aktywności źródła,
- **sterowanie doborem trasy** - umożliwia dobór trasy w taki sposób by transmitowane dane mogły podążać jedynie przez fizycznie bezpieczne łącza lub podsieci,
- **mechanizmy notaryzacji** - służą do zabezpieczenia komunikacji przed zaprzeczeniem.

6.4 Zarządzanie bezpieczeństwem

Zarządzanie bezpieczeństwem wiąże się ze sterowaniem od strony zabezpieczeń komunikacją i przetwarzaniem danych m.in. poprzez wymianę informacji niezbędnych do przeprowadzenia tego procesu.
Zarządzanie bezpieczeństwem jest działalnością wykraczającą poza podstawowe operacje telekomunikacyjno-obliczeniowe występujące w systemie informacyjnym.

Ze względu na charakter zarządzanych obiektów wyróżniamy trzy obszary zarządzania:

- **zarządzanie usługami,** czyli zarządzanie kontrolą dostępu, poufnością, integralnością,uwierzytelnieniem, niezaprzeczalnością, audytem i alarmami,
- **zarządzanie kluczami,**
- **zarządzanie polityką zabezpieczeń (bezpieczeństwa).**

Zarządzanie kluczami jest niezbędne do poprawnej realizacji większości usług ochrony informacji (klucz jest parametrem szyfru, szyfr jest składnikiem większości usług ochrony informacji).

Zarządzanie polityką zabezpieczeń (bezpieczeństwa) jest konieczne do właściwej pracy urzędów bezpieczeństwa, czy też delegowanych przez nie zarządców poszczególnych usług ochrony informacji.

6.4.1 Informacje bezpieczeństwa

Zarządzanie bezpieczeństwem wiąże się z:

- przetwarzaniem,
- badaniem stanu,
- porządkowaniem

informacji bezpieczeństwa IB ***(ang. SI - Security Information),*** które są niezbędne do realizacji usług bezpieczeństwa (ISO 10181-1]).

Przykładami tego typu informacji są:

- ***informacje konieczne do zrealizowania specyficznej usługi ochrony informacji*** np. informacja uwierzytelniająca zawierająca dane o tęczówce konkretnego człowieka,
- ***informacje wspólne dla kilku usług bezpieczeństwa***:
  - **etykiety bezpieczeństwa** *(ang. security labels)* - używane do oznaczenia

atrybutów bezpieczeństwa dla danego podmiotu,

- **kryptograficzne sumy kontrolne** *(ang. cryptographic checkvalues)* - czyli podpisy cyfrowe, skróty i koperty,
- **certyfikaty** *(ang. security certificates)* - cyfrowe świadectwa wydane przez określony urząd bezpieczeństwa,
- **tokeny** *(ang. tokens)* - zbiory danych zabezpieczone, co najmniej jedną usługą ochrony informacji,

- ***zasady polityki zabezpieczeń (bezpieczeństwa).***

6.4.2 Podstawowe udogodnienia

Z zarządzaniem wiążą się tzw. **udogodnienia** ***(ang. facilities)*** czyli akcje związane z informacjami bezpieczeństwa, bądź z usługami (ISO 10 181-1).

Następujące udogodnienia związane z zarządzaniem są przeprowadzone przez urząd bezpieczeństwa i współpracujący z nim element:

- **Instaluj IB** ***(ang. Install SI)*** - ustanowienie inicjującego zbioru IB, przyporządkowanemu pewnemu elementowi,
- **Deinstaluj IB** ***(ang. Deinstall SI)*** – usunięcie IB, które deklaruje przynależność elementu do domeny bezpieczeństwa,
- **Zmień IB** ***(ang. Change SI)*** - modyfikacja IB skojarzonej z elementem,
- **Uaktywnij IB** ***(ang. Validate SI)*** - aktywne powiązanie IB z elementem, przeprowadzana przez urząd bezpieczeństwa,
- **Wycofaj IB** ***(ang. Invalidate SI)*** - deaktywacja użycia (ale nie usunięcie z systemu) IB skojarzonego z elementem, przeprowadzane przez urząd bezpieczeństwa,
- **Deaktywuj/Aktywuj usługę** - ***(ang. Disable/Re-enable security service)*** - deaktywacja usługi lub jej określonego poziomu,
- **Odnotuj** ***(ang. Enrol)*** - rejestracja przez urząd bezpieczeństwa informacji skojarzonej z danym podmiotem (np. rejestracja żądania),
- **Zmaż** ***(ang. Un-enrol)*** - usunięcie infonnacji; oczywiście polityka bezpieczeństwa może nie dopuszczać by niektóre informacje były usuwane,
- **Udostępnij IB** ***(ang. Distribute SI)*** - udostępnienie danej informacji innym podmiotom,
- **Stwórz listę IB** ***(ang. List SI)*** - tworzenie listy IB skojarzonych z danych elementem.

Oprócz wymienionych uniwersalnych udogodnień związanych z zarządzaniem wyróżnia się **udogodnienia związane z operacjami:**

- **Rozpoznaj zaufany urząd bezpieczeństwa** (*ang. Identify trusted security authorites*) - dzięki temu udogodnieniu dany element jest w stanie rozpoznać właściwy urząd bezpieczeństwa o odpowiednich kompetencjach (tj. wynikających z polityki bezpieczeństwa),
- **Rozpoznaj bezpieczne zasady współpracy** *(ang. Identify secure interaction rules)* - dzięki temu udogodnieniu dwa elementy negocjują lub wykorzystują ustalone zasady współpracy,
- **Nabyj IB** *(ang. Acquire SI)* - nabycie IB - pierwotne względem aktywności podmiotu,
- **Generuj IB** *(ang. Generate SI)* - generacja IB dla konkretnej usługi bezpieczeństwa,
- **Weryfikuj IB** *(ang. Verify SI)* - weryfikacja ważności IB.

Udogodnienia związane z zarządzaniem i operacjami, a także informacje bezpieczeństwa określają zasady sterowania daną usługą ochrony informacji. Dopiero ich całościowe przedstawienie daje obraz zarządzania daną usługą.
Udogodnienia związane z zarządzaniem odnoszą się do działalności urzędu bezpieczeństwa (lub jego delegata), który operując na informacjach bezpieczeństwa i łącząc je w różnych relacjach z podmiotem, pośrednio czuwa nad prawidłowym przebiegiem operacji.

Przykład - Zarządzanie kontrolą dostępu

Kontrola dostępu, czasem określana mianem autoryzacji, jest usługą dzięki, której tylko uprzywilejowane podmioty mogą otrzymać dostęp do zasobów.
Podmiotem może być zarówno człowiek jak i proces, zasobem - proces, system sieciowy.

6.4.3 Model kontroli dostępu

W modelu kontroli ([ISO 10181-3], [RACE CFS H211], [RACE CFS H407]) wykorzystuje się następujące określenia:

- **inicjator** *(ang. initiator)* - podmiot, który próbuje uzyskać dostęp do innego podmiotu,
- **cel (ang. target)** - podmiot, do którego następuje **próba dostępu, czyli akcja,**
- **informacja kontroli dostępu** *(ang. ACI - Access Control Information)* - dowolna informacja używana przy procesie kontroli dostępu,
- **funkcja decyzyjna kontroli dostępu** *(ang. ADF - Access Control Decision Function)* - specjalistyczna funkcja kontrolująca decyzję o dostępie poprzez zastosowanie reguł polityki bezpieczeństwa na pożądanej akcji, ACI i kontekstu, w jakim żądanie zostało użyte,

- **informacja decyzyjna kontroli dostępu** ***(ang. ADI - Access Control Decision Information)*** – zbiór ACI niezbędnych ADF do podjęcia decyzji,
- **funkcja przeprowadzająca kontrolę dostępu** ***(ang. AEF - Access Control Enforcement Function)*** - specjalistyczna funkcja będąca ścieżką dostępu pomiędzy inicjatorem a celem, przeprowadzająca kontrolę dostępu.

AEF jest odpowiedzialna za poprawność akcji zdeterminowanych przez ADF wykonywanych pomiędzy inicjatorem a celem.
Kiedy podmiot inicjujący żąda wykonania akcji na podmiocie docelowym, AEF komunikując się z ADF otrzymuje informację o podjętej decyzji.
Decyzja jest przeprowadzana na podstawie ADI skojarzonych z inicjatorem, celem i akcją.

6.5 Polityka zabezpieczenia systemu informacyjnego w przedsiębiorstwie telekomunikacyjnym

Realizacja procesu zabezpieczenia systemów informacyjnych zarządzania w telekomunikacji i teleinformatyce wymaga zdefiniowania **polityki zabezpieczenia systemu informacyjnego przedsiębiorstwa telekomunikacyjnego/teleinformatycznego**.

Polityka zabezpieczenia systemu informacyjnego jest dokumentem, w którym kierownictwo przedsiębiorstwa jasno określa:

- cele - co ma być osiągnięte,
- strategie - jak osiągnąć cele,
- konieczne działania - co należy zrobić.

Zdefiniowanie wymagań w zakresie zabezpieczenia systemu informacyjnego bez określenia polityki zabezpieczenia tegoż systemu prowadzi niejednoznaczności (sporu) co do stwierdzenia faktu naruszenia zabezpieczenia, gdyż brak definicji poufności dokumentów i danych może prowadzić do ujawnienia tajemnic przedsiębiorstwa itp.

6.6 Zarządzanie zabezpieczeniem systemu informacyjnego

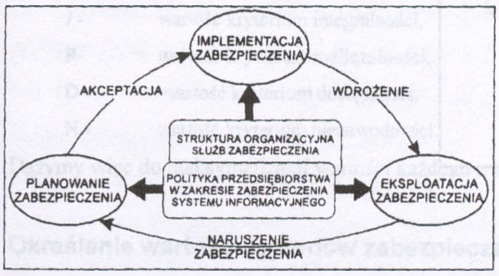
Jeśli system informacyjny w znacznym stopniu decyduje o funkcjonowaniu nowoczesnego przedsiębiorstwa, a zwłaszcza o jego pozycji rynkowej to problematykę jego zabezpieczenia należy traktować jako jeden z zasadniczych elementów strategii działania firmy.

Zabezpieczenie systemu informacyjnego wymaga **zdefiniowania procesów zarządzania zabezpieczeniem.**

Proces zarządzania zabezpieczeniem systemu informacyjnego można podzielić na trzy zasadnicze podprocesy:

- planowania zabezpieczenia,
- implementacji planu zabezpieczenia,
- eksploatacji zabezpieczenia,

których wzajemne powiązania zostały przedstawione na rysunku.46.

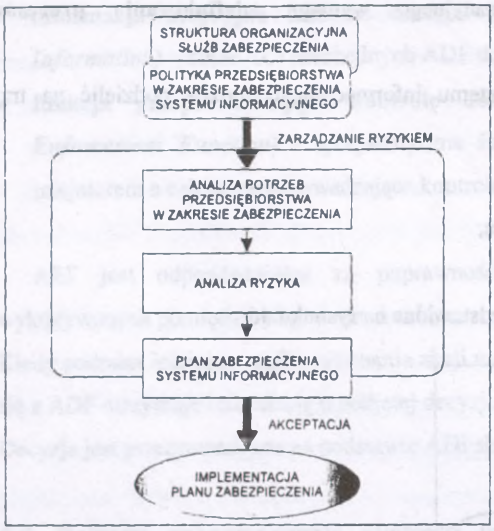


Rysunek 46. Procesy zarządzania zabezpieczeniem.

Realizacja tych podprocesów musi być zgodna z określoną w przedsiębiorstwie polityką zabezpieczenia systemu informacyjnego. Stwierdzenie niezgodności z polityką w jednej z faz zarządzania zabezpieczeniem powinno powodować uruchomienie mechanizmów planowania zabezpieczenia.

6.6.1 Planowanie zabezpieczenia

Na rysunku 47 przedstawiono kolejne fazy procesu planowania zabezpieczenia systemu informacyjnego. W wyniku działań zgodnych z przedstawionym tu schematem powstanie **plan zabezpieczenia systemu informacyjnego przedsiębiorstwa.** Należy podkreślić, że niezwykle rzadko zdarza się, aby w systemie informacyjnym nie istniały żadne zabezpieczenia. Dlatego planowanie zabezpieczenia polega nie tyle na jego tworzeniu, co na dokonywaniu jego modyfikacji, tzn. wymianie mechanizmów na bardziej skuteczne, wprowadzaniu nowych procedur itp. Kluczowym elementem fazy planowania zabezpieczenia jest **zarządzanie ryzykiem.**



Rysunek 47. Proces planowania zabezpieczenia.

Zarządzanie ryzykiem

Wszelkie działania podejmowane w systemie informacyjnym niosą ze sobą ryzyko. Całościowa identyfikacja zagrożeń i określenie niezbędnego zakresu ich kontrolowania lub akceptowania na wyznaczonym poziomie nosi nazwę *analizy ryzyka.*

Rezultatem analizy ryzyka jest określenie jego poziomów *(szacowanie ryzyka)* dla wszystkich aktywów systemu informacyjnego. Całość przyjętych zabezpieczeń ma na celu *ograniczenie ryzyka* do akceptowalnego poziomu. Proces identyfikowania, kontrolowania i unikania lub minimalizowania skutków niepożądanych zdarzeń nosi nazwę *zarządzania ryzykiem.*

Każde przedsiębiorstwo telekomunikacyjne/teleinformatyczne pragnące podwyższyć poziom zabezpieczenia swego systemu informacyjnego musi rozważyć, jaka strategia zarządzania ryzykiem jest najodpowiedniejsza dla środowiska, w którym to przedsiębiorstwo działa oraz czy zapewnia ona efektywny sposób oszacowania ryzyka. Nie zawsze najefektywniejszą drogą jest przeprowadzenie szczegółowej analizy ryzyka, ale także błędem jest pominięcie obszarów, w którym ryzyko naruszenia zabezpieczenia jest poważne. Wyboru racjonalnej strategii należy dokonać, opierając się na ogólnej analizie potrzeb przedsiębiorstwa w zakresie zabezpieczenia, czyli **wyznaczenia poziomu zabezpieczenia.**

Poziom zabezpieczenia jest funkcją spełnienia podstawowych kryteriów zabezpieczenia i można go obrazowo przedstawić w następujący sposób:

$$PZ = > max\ (P, I, D, A, R, N)$$

gdzie:

PZ- wartość poziomu zabezpieczenia,
P- wartość kryterium poufności,
A - wartość kryterium autentyczności,
I - wartość kryterium integralności,
R- wartość kryterium rozliczalności,
D- wartość kryterium dostępności,
N - wartość kryterium niezawodności.

Dążymy więc do maksymalizacji wartości każdego z kryteriów.

Określenie wartości kryteriów zabezpieczenia

Wartość kryterium odzwierciedla powagę sytuacji, będącej następstwem niespełnienia kryterium, czyli odpowiednio utraty poufności, integralności, dostępności, autentyczności, rozliczalności i niezawodności. Ponieważ przeprowadzana analiza ma charakter jakościowy, skala wartości może być następująca: maksymalna - wysoka - niska - nie dotyczy.

Pojęcie poufności w systemie informacyjnym obejmuje poufność zawartości transmisji, danych przechowywanych w systemie, wybranych obszarów baz danych oraz sesji komunikacyjnych. Należy rozważyć, jakie szkody może ponieść przedsiębiorstwo wskutek utraty poufności w swoim systemie informacyjnym.

Przykładowo może to być:

- utrata zaufania publicznego, dobrego imienia firmy,
- konsekwencje prawne z tytułu naruszenia ustawy o ochronie danych osobowych,
- narażenie zdrowia lub życia ludzkiego,
- strata finansowa.

Integralność jest jednym z najważniejszych kryteriów zabezpieczenia. Opisuje stan poprawności działania sprzętu i oprogramowania oraz poziom ochrony przed nieupoważnioną modyfikacją danych.

W systemach otwartych pojęcie integralności zostało rozszerzone również na mechanizmy transferu informacji. Integralność komunikacji obejmuje poprawność transmisji, uwierzytelnienie źródła i ujścia danych oraz protokołów.

Utrata integralności w systemie informacyjnym przedsiębiorstwa może spowodować następujące konsekwencje:

- podjęcie nieprawidłowych decyzji opartych na zafałszowanej informacji,
- straty finansowe,
- negatywne skutki prawne wynikające z niewłaściwej ochrony danych osobowych,
- utratę zaufania publicznego lub dobrego imienia firmy, załamanie działalności przedsiębiorstwa.

Kolejno należy rozważyć, jakie konsekwencje może mieć utrata dostępności do informacji lub aplikacji pracującej w systemie informacyjnym, a więc określenie działań firmy, które mogą nie być zrealizowane w żądanym czasie.

Przedmiotem uwagi powinna być także analiza w przypadku krytycznej utraty dostępności, np. utraty danych lub fizycznego zniszczenia urządzeń.

Przykładowo, utrata dostępności może prowadzić do następujących zdarzeń:

- braku możliwości realizacji krytycznych zadań,
- utraty zaufania publicznego lub dobrego imienia firmy, strat finansowych,
- znaczących kosztów odtworzenia aktywów.

Pojęcie autentyczności obejmuje jednoznaczną identyfikację oraz uwierzytelnienie użytkownika, procesu czy systemu informacyjnego. W zakresie tego pojęcia mieści się także kontrola dostępu, weryfikacja przywilejów oraz niezaprzeczalność. Określając wartość kryterium autentyczności należy mieć na uwadze jego powiązanie z kryterium dostępności oraz rozliczalności.

Utrata autentyczności może np. prowadzić do:

- braku możliwości przypisania odpowiedzialności za działania niezgodne z prawem,
- utraty zaufania publicznego i dobrego imienia firmy,
- konsekwencji prawnych i finansowych.

Zabezpieczenie niektórych systemów informacyjnych, w szczególności systemów otwartych, zależy od określenia kryterium rozliczalności.

Aby móc spełnić kryterium rozliczalności, należy dysponować mechanizmami separacji użytkowników danych i procesów, jednoznacznego uwierzytelnienia oraz systemem audytu.

Utrata rozliczalności może prowadzić do następujących zdarzeń:

- utraty zaufania publicznego,
- fałszowania elektronicznych dokumentów,

- konsekwencji prawnych wynikających z naruszenia dóbr osobistych,
- strat finansowych.

Niezawodność jest pojęciem historycznie nie związanym ściśle z pojęciem zabezpieczenia. Pojęcie to było uprzednio określane jako współdziałanie trzech czynników: niezawodności, utrzymania i dostępności *(RMA - reliability, maintainability, availability).* Koncepcja systemów odpornych na błędy i uszkodzenia opierała się na nadmiarowości konfiguracji oraz rozbudowanej funkcji serwisowania.

Współczesne systemy informacyjne mają charakter rozproszony i często niezawodność ich działania opiera się na niezawodności interakcji między poszczególnymi ich elementami. Zależność pracy systemu od pewności komunikacji między urządzeniami stale się zwiększa.

Niezawodność pojmowana jako gwarancja spójności zamierzonego zachowania oraz otrzymanych wyników musi być rozpatrywana jako kryterium zabezpieczenia.

W pewnych sytuacjach jest lepiej, aby urządzenie było niedostępne niż zawodne.

Utrata niezawodności może prowadzić do następujących zdarzeń: niemożności realizacji krytycznych zadań,

- utraty zaufania publicznego i dobrego imienia firmy,
- znacznych kosztów odtworzenia aktywów systemu informacyjnego.

Rozważając oddzielnie poszczególne kryteria zabezpieczenia, należy jednak mieć na względzie, że w praktyce często kryteriów tych nie da się wyraźnie oddzielić.

Przykładowo, pojęcia integralności i niezawodności zasobów systemu informacyjnego są zbliżone. Utrata dostępności, niezawodności i integralności może spowodować niemożność realizacji konkretnej usługi informacyjnej. Utrata autentyczności może być powiązana z utratą rozliczalności. Utrata poufności może spowodować także utratę integralności. Ogólna analiza potrzeb powinna zatem uwzględniać także zależności między kryteriami.

6.6.2 Określenie wymaganego poziomu zabezpieczenia

Po przeprowadzeniu ogólnej analizy potrzeb w zakresie zabezpieczenia można odpowiedzieć na pytanie, jaki poziom zabezpieczenia jest wymagany dla przedsiębiorstwa oraz jego systemu informacyjnego.

Zgodnie z ogólnym wzorem przedstawionym wyżej, poziom zabezpieczenia dla danego systemu informacyjnego przyjmuje najwyższą wartość ze zbioru wartości kryteriów zabezpieczenia wyznaczonych dla tego systemu.

Ogólna analiza potrzeb w zakresie zabezpieczenia oraz wyznaczony poziom zabezpieczenia systemu informacyjnego pozwala także scharakteryzować typ przedsiębiorstwa, w którym system ten pracuje, co zostało przedstawione w tabeli.6.

Tabela 6 Profil przedsiębiorstwa i wyznaczony poziom zabezpieczenia jego systemu informacyjnego

Profil przedsiębiorstwa	Poziom zabezpieczenia
Uszkodzenie systemu informacyjnego prowadzi do całkowitego załamania przedsiębiorstwa i może mieć poważne konsekwencje polityczne, społeczne lub ekonomiczne.	Maksymalny
W przypadku uszkodzenia systemu informacyjnego część organizacji nie może funkcjonować, dłuższe utrzymywanie się tego stanu może mieć poważne konsekwencje dla przedsiębiorstwa lub jego partnerów	Wysoki
Konsekwencją poważnego i długotrwałego uszkodzenia systemu informacyjnego może być upadek przedsiębiorstwa	Średni
Uszkodzenie systemu informacyjnego może spowodować jedynie niewielkie perturbacje w funkcjonowaniu przedsiębiorstwa	Niski

Odpowiednie zabezpieczenia można określić, adaptując międzynarodowe lub krajowe normy, normy lub zalecenia przemysłowe, rozwiązania przyjęte przez przedsiębiorstwa o podobnym profilu (typ działalności, wielkość, taki sam system informacyjny, aplikacje)

Istotnym elementem w zapewnieniu wymaganego poziomu bezpieczeństwa systemu informacyjnego jest analiza ryzyka (ogólna i szczegółowa), przeprowadzona dla przyjętego profilu przedsiębiorstwa.

Charakterystykę działań związanych z realizacją analizy ryzyka zawarto w [].

W wyniku analizy ryzyka zostaje określona grupa istniejących stale elementów ryzyka, które można formalnie zidentyfikować i całkowicie określić w odniesieniu do odpowiednich mechanizmów zabezpieczeń, na których podstawie zostaje wyznaczony ostateczny poziom akceptowalnego ryzyka.

Następnie tworzony jest plan zabezpieczenia systemu informacyjnego, będący dokumentem zawierającym opis działań, które należy podjąć w celu wdrożenia w systemie informacyjnym pożądanych mechanizmów zabezpieczeń.

Plan zabezpieczenia powinien zawierać:

- wymagania dotyczące zabezpieczenia systemu w zakresie zachowania integralności, poufności, dostępności, autentyczności, rozliczalności i niezawodności,
- analizę ryzyka opisaną w poprzednim rozdziale,

- oszacowanie ryzyka szczątkowego - pozostającego po wdrożeniu odpowiednich mechanizmów zabezpieczeń - którego poziom może być zaakceptowany,
- listę wdrażanych mechanizmów zabezpieczeń oraz listę mechanizmów istniejących wraz z oszacowaniem ich efektywności i zasad współdziałania,
- oszacowanie kosztów instalacji oraz eksploatacji wdrażanych mechanizmów, w tym także kosztów osobowych,
- szczegółowy harmonogram implementacji.

6.6.3 *Implementacja zabezpieczenia systemu informacyjnego*

W ramach implementacji zabezpieczenia systemu informacyjnego realizowane są:

- uświadamianie, szkolenie i edukacja,
- testowanie i implementacja zabezpieczeń,
- akredytacja.

Realizacja polityki zabezpieczenia systemu informacyjnego przedsiębiorstwa telekomunikacyjnego/teleinformatycznego oprócz działań opisanych wyżej wymaga ciągłego doskonalenia (adaptacyjnego do nowych zagrożeń oraz warunków funkcjonowania) przyjętych zabezpieczeń, edukacji pracowników przedsiębiorstwa oraz zdefiniowania i wdrożenia do codziennej praktyki eksploatacyjnej procedur reagowania kryzysowego (awarie, katastrofy). Poniżej przedstawiono charakterystykę tych działań.

Uświadamianie, szkolenie i edukacja

W zabezpieczeniu systemów informacyjnych najważniejszą rolę odgrywają ludzie. Oni też są przeważnie najsłabszym jego ogniwem. Wdrożenie planu zabezpieczenia nie może zakończyć się powodzeniem, jeśli pracownicy pozostaną nieświadomi celów podejmowanych działań. Powinien być opracowany program upowszechniania zasad systemu zabezpieczenia na wszystkich poziomach organizacji przedsiębiorstwa.

Zminimalizowanie zagrożeń w postaci błędów i przeoczeń, nadużyć i nieupoważnionych działań podejmowanych przez własnych pracowników wymaga odpowiedniego uświadamiania, szkolenia i edukacji.

Uświadamianie pracowników w zakresie zabezpieczenia systemów informacyjnych obejmuje:

- przedstawienie celów polityki zabezpieczeń prowadzonej w przedsiębiorstwie oraz pokazanie, w jaki sposób ta polityka przyczynia się do realizacji celów działalności i ochrony aktywów przedsiębiorstwa,

- całkowite zrozumienie wytycznych w zakresie zabezpieczenia systemu informacyjnego.

Celem szkolenia jest przekazanie pracownikom umiejętności, które sprawią, że będą oni wykonywali swe zadania zgodnie z procedurami określonymi w polityce zabezpieczenia systemu informacyjnego. Aby szkolenie było efektywne, musi być zorientowane na poszczególne kategorie odbiorców. Podstawowymi kategoriami są użytkownicy wymagający szkolenia ogólnego oraz część personelu, która potrzebuje szkolenia specjalizowanego lub zaawansowanych umiejętności.

Celem szkolenia ogólnego jest wpojenie pracownikom zasad odpowiedniego postępowania z zasobami systemu informacyjnego, a w szczególności:

- zasad ochrony informacji poufnej będącej tajemnicą przedsiębiorstwa,
- fizycznego zabezpieczenia pomieszczeń oraz zasobów systemu informacyjnego,
- ochrony haseł lub innych środków uwierzytelnienia (np. kart inteligentnych) umożliwiających dostęp do zasobów systemu,
- przekazywania informacji o dostrzeżonych anomaliach działania systemu, które mogą być efektem naruszenia zabezpieczenia.

Szkolenie specjalistyczne może dotyczyć kierownictwa i obejmować np. umiejętność szacowania ryzyka lub administratorów, którzy muszą umieć instalować dane mechanizmy zabezpieczeń.

Edukacja sięga głębiej niż szkolenie i jest skierowana do osób zawodowo zajmujących się zabezpieczeniami systemów informacyjnych. Ta działalność przeważnie nie znajduje się w zakresie programów szkoleniowo-uświadamiających, a jedynie stanowi element doskonalenia zawodowego niektórych pracowników.

Akredytacja

Akredytacja jest przyjęciem i nadaniem uprawnień do użytkowania wdrożonego planu zabezpieczenia zgodnego z założeniami polityki zabezpieczenia. Akredytacja jest ważna w ograniczonym przedziale czasowym i dla ściśle zdefiniowanego systemu informacyjnego; każda jego zmiana wymaga rewizji akredytacji.

Proces akredytacji składa się z przeglądu dokumentacji i odbioru technicznego. Przegląd dokumentacji obejmuje sprawdzenie jej kompletności, wewnętrznej spójności i zgodności z innymi dokumentami.

Odbiór techniczny opiera się na kontroli zgodności ze standardami i może być powierzony specjalizowanym instytucjom certyfikującym.

Po przeprowadzeniu procesu akredytacji można przystąpić do eksploatacji zabezpieczenia.

6.7 Eksploatacja zabezpieczenia systemu informacyjnego

Ten proces zarządzania zabezpieczeniem jest zwykle pomijany w opracowaniach, ale pełni bardzo ważną rolę. Istniejące i wdrożone w efekcie modyfikacji planu mechanizmy zabezpieczeń wymagają utrzymania.

Celem działań utrzymaniowych jest zapewnienie prawidłowego funkcjonowania systemu zabezpieczenia w czasie jego eksploatacji, na co składa się:

- zarządzanie konfiguracją,
- monitorowanie systemu zabezpieczeń,
- audyt systemu zabezpieczeń.

6.7.1 Zarządzanie konfiguracją

Zarządzanie konfiguracją jest procesem śledzenia zmian zachodzących w systemie informacyjnym.

Głównym celem tego procesu jest zapewnienie, że wprowadzane zmiany nie zmniejszają efektywności mechanizmów zabezpieczeń i ogólnego bezpieczeństwa przedsiębiorstwa. Jeśli jednak w systemie informacyjnym muszą zostać dokonane zmiany, które mają wpływ na stan zabezpieczenia przedsiębiorstwa, to zarządzanie konfiguracją powinno uruchomić procesy szacowania poziomu zabezpieczenia i ewentualnej modyfikacji planu zabezpieczenia.

Innym celem procesu zarządzania jest wprowadzanie stosownych zmian w procedurach wyjścia ze stanów awaryjnych i katastrofalnych.

6.7.2 Monitorowanie systemu zabezpieczenia

Monitorowanie jest ważnym aspektem eksploatacji zabezpieczenia. Należy monitorować mechanizmy zabezpieczeń, aktywa systemu informacyjnego i zagrożenia; jakiekolwiek zmiany w środowisku mogą mieć wpływ na powyższe elementy.

Monitorowanie mechanizmów zabezpieczeń ma na celu kontrolę ich jakości i efektywności w miarę upływu czasu od momentu ich wdrożenia. Monitorowanie zagrożeń umożliwia wykrycie zmian w ich charakterze lub stopnia znaczenia oraz wczesne rozpoznanie nowych zagrożeń. Monitorowanie aktywów systemu informacyjnego pozwala na wykrycie zmian ich wartości oraz uwzględnia proces dodawania nowych składników.

6.7.3 *Audyt systemu zabezpieczenia*

Efektem działania wielu mechanizmów zabezpieczeń są rejestry zdarzeń. Audyt jest procesem analizy tych rejestrów w celu sprawdzenia zgodności z polityką zabezpieczenia i procedurami eksploatacyjnymi oraz wykrycia naruszeń systemu zabezpieczenia.

Jakkolwiek audyt jest z natury rzeczy procesem analizy przeszłości, to zabezpieczenie systemu informacyjnego ma charakter dynamiczny i podlega stałemu rozwojowi. Z tego względu audytu nie należy traktować jako procesu skończonego. Oczywiście w celu analizy efektywności mechanizmów zabezpieczeń, istnieje konieczność chwilowego, formalnego zdefiniowania zakresu audytu. Jednakże wykorzystanie audytu tylko do analizy *post facfum* jest równoznaczne z rezygnacją z bardzo potężnego mechanizmu zabezpieczenia. Zastosowanie metod statystycznych w procesie audytu umożliwia wczesne wykrycie zmian tendencji oraz nasilania niepożądanych zjawisk. Efektem przeprowadzenia audytu może być konieczność wprowadzenia zmian w polityce zabezpieczenia oraz w planie zabezpieczenia.

Mimo stworzenia planu zabezpieczenia systemu informacyjnego nie sposób w codziennej jego eksploatacji uniknąć sytuacji awaryjnych czy wręcz kryzysowych.

6.8 Procedury postępowania w przypadku naruszenia zabezpieczenia systemu informacyjnego oraz w stanach awaryjnych i kryzysowych

Naruszenie zabezpieczenia systemu informacyjnego wymaga podjęcia właściwych kroków. Przedsiębiorstwa muszą mieć plany: postępowania w przypadku naruszenia zabezpieczenia oraz wyjścia systemu ze stanu katastrofy.

Zarządzanie w przypadku naruszenia zabezpieczenia wymaga zdefiniowania, opracowania i udokumentowania planu awaryjnego, uaktywnianego bezpośrednio po wykryciu zdarzenia, w wyniku którego system informacyjny nie może funkcjonować z normalną wydajnością.

Plan ten służy ograniczaniu zasięgu konsekwencji poważnego naruszenia zabezpieczenia. Tylko uprzednio przygotowany plan działań i wymaganych decyzji umożliwia szybką reakcję i pomaga ograniczyć zasięg szkód.

Procedura postępowania w sytuacjach naruszenia zabezpieczenia zawiera dwa elementy:

- sposób postępowania przy bezpośrednim naruszeniu zabezpieczenia,
- tworzenie kopii bezpieczeństwa zasobów informacyjnych systemu.

Procedura postępowania musi także obejmować prowadzenie chronologicznej dokumentacji wszystkich zdarzeń i podejmowanych działań.

Zapis taki umożliwi wyśledzenie źródła zdarzenia, a ponadto pozwoli na uniknięcie podobnego zdarzenia w przyszłości. W ten sposób niepożądane zdarzenie spełni pozytywną rolę, zwiększając gotowość kierownictwa do przeznaczenia dodatkowych nakładów na zabezpieczenie.

Analizy *post mortem*, która powinna odpowiedzieć na następujące pytania:

- co i kiedy zdarzyło się,
- jaka jest ocena działania personelu, czy postępował on zgodnie z planem,
- czy personel otrzymał potrzebne informacje we właściwym czasie,
- jakie zmiany w planach postępowania zostały zaproponowane.

Odpowiedzi na powyższe pytania pomogą zrozumieć istotę powstałych zdarzeń, co może w efekcie ujawnić potrzebę modyfikacji polityki zabezpieczenia.

Procedura wyjścia ze stanów awaryjnych lub katastrofalnych jest zespołem działań, które muszą zostać podjęte w celu odtworzenia zniszczonego w wyniku katastrofy systemu informacyjnego i doprowadzenia go do stanu normalnej aktywności.

Zarządzanie w stanach awarii lub katastrofy wymaga określenia kryteriów stanu awarii lub katastrofy, wprowadzenia planów awaryjnych, działań w celu przywrócenia poprzedniego stanu, opisu podjętych działań.

6.9 Projektowanie bezpiecznego TMN

Wszelkie metody zabezpieczeń stosowane w sieci zarządzania telekomunikacją TMN mają swój rodowód w rekomendacjach ITU- T i standardach ISO/IEC.

Zarządzanie bezpieczeństwem systemu informacyjnego zgodne z jego polityką zabezpieczeń (bezpieczeństwa) jest podstawą bezpiecznego zarządzania i wykracza poza typowo techniczne ramy, gdyż staje się obszarem organizacji przedsiębiorstw.

Na obecnym etapie rozwoju technologii informatycznych (wspomagania decyzyjnego, automatycznej identyfikacji i oceny zagrożeń) zarządzania bezpieczeństwem systemów informacyjnych nie można zautomatyzować, co wynika z charakteru spotykanych w rzeczywistości zagrożeń oraz dynamiki ich zmian.

Przy tworzeniu bezpiecznej sieci zarządzania telekomunikacją TMN można wyróżnić trzy fazy [RACE CFS H210]:

- fazę początkową,
- fazę projektowania, przeglądu i zatwierdzenia *(ang. design, review and*

accreditaion phase),

- fazę operacyjną *(ang. operational phase).*

6.9.1 Charakterystyka fazy początkowej

W fazie początkowej wyłania się interdyscyplinarną grupę ekspertów sterującą całym procesem analizy, wprowadzania, realizacji i obsługi zabezpieczeń w TMN.
Grupa powinna stanowić rzeczywisty przekrój wszystkich stron powiązanych z zarządzaniem: użytkowników, przedstawicieli poszczególnych działów operatora, a także prawników, ekonomistów, specjalistów od bezpieczeństwa, inżynierów i techników implementujących system.

6.9.2 Charakterystyka fazy projektowania, przeglądu i akredytacji

Podczas fazy projektowania, przeglądu i akredytacji realizowane są następujące czynności:

- ustala się strategię zabezpieczeń,
- określa się chronione zasoby,
- przeprowadza się analizę ryzyka, na podstwie której określa się wymagania bezpieczeństwa,
- proponuje się rozwiązania spełniające wymagania,
- przeprowadza się ocenę "koszty / zyski",
- tworzy się ostateczną politykę zabezpieczeń (bezpieczeństwa).

Wynikiem całej fazy jest plan systemu zabezpieczeń.

Strategia zabezpieczeń

Strategia zabezpieczeń określa zasady zarządzania bezpieczeństwem na poziomie organizacyjnym. Dotyczy to w szczególności zabezpieczeń zasobów obliczeniowych i sieciowych.

Istotnym czynnikiem kształtującym strategię zabezpieczeń są przepisy prawne, co ma szczególne znaczenie przy rozważaniu zabezpieczeń styku fizycznego X - łączącego zarówno operatorów lokalnych (krajowych) jak i międzynarodowych.

Określenie strategii wiąże się ze:

- stworzeniem oficjalnego słownika wyrazów powiązanych z bezpieczeństwem,
- nakreśleniem celu zabezpieczeń,
- zdefiniowaniem zakresu zabezpieczeń,
- zdefiniowaniem relacji i odpowiedzialności pomiędzy wszystkimi uczestniczącymi stronami.

Określenie chronionych zasobów

Określenie zasobów, które podlegają ochronie i określenie poziomu zabezpieczeń jest niezbędnym krokiem przy projektowaniu bezpiecznego TMN.

Określenie powinno zawierać:

- opis rozmieszczenia i typ każdego z zasobów (architekturę),
- koszt związany z wyjawieniem danych lub przejęciem sprzętu.

Przykładami zasobów są:

- funkcje TMN,
- dane przechowywane w TMN (zarządzane obiekty),
- sprzęt.

Analiza ryzyka

Analiza ryzyka jest szczegółową analizą zagrożeń *(ang. threats)*, słabych punktów *(ang. vulnerabilites)* i skutków *(ang. impacts)*.

Wymagania bezpieczeństwa

Wymagania bezpieczeństwa są określane po wykonaniu analizy ryzyka i przeanalizowaniu problemów natury prawnej.

Rozwiązania

Proponowane rozwiązania mają na celu spełnienie określonych i uświadomionych wymagań.

Usługi i mechanizmy bezpieczeństwa mogą być wybrane z biblioteki technik ochrony informacji. Usługi i mechanizmy bezpieczeństwa grupuje się w tzw. podprofile bezpieczeństwa (oferujące pożądany poziom bezpieczeństwa np. militarny - znaczny, komercyjny - przeciętny).

Ocena "koszty / korzyści"

Zaproponowane rozwiązania są oceniane pod kątem potencjalnych kosztów i korzyści.

Koszty określające pożądany poziom bezpieczeństwa nie powinny przekraczać zysków z zastosowanych usług bezpieczeństwa.

Polityka zabezpieczeń (bezpieczeństwa)

Polityka bezpieczeństwa jest zbiorem praw, zasad i sposobów, które regulują zarządzanie, przetwarzanie, użycie, zabezpieczenie i rozpowszechnianie informacji i zasobów systemu.

Plan systemu zabezpieczeń

Jest ostatecznym wynikiem działań przeprowadzanych w fazie projektowania, przeglądu i zatwierdzenia. Zawiera definicję zabezpieczanych zasobów, wyniki analizy ryzyka i politykę bezpieczeństwa.

Charakterystyka fazy operacyjnej

Faza operacyjna określa szkielet funkcjonowania zabezpieczeń w działającym TMN.
W tej fazie można wyróżnić trzy etapy:

- wykrycie,
- ocena,
- przetwarzanie zdarzeń związanych z bezpieczeństwem.

Wykrycie

Wykrycie zdarzeń związanych z bezpieczeństwem jest uwarunkowane dwoma czynnikami:

- polityką zabezpieczeń (bezpieczeństwa), dzięki której zdarzenia istotne z punktu widzenia bezpieczeństwa są rozpoznawane i obsługiwane,
- mechanizmami wykrywającymi niezwykłe zdarzenia.

Ocena

Ocena zdarzenia polega na odpowiedz na pytanie czy dane zdarzenie jest znane:

- jeśli tak jest, podejmowana decyzja, czy zdarzenie ma znaczący wpływ na stan systemu.
- jeśli zdarzenie nie jest znane, powinno nastąpić złagodzenie strat i szybkie skorygowanie planu zabezpieczeń systemu (są to procesy ostatniego etapu przetwarzania).

Przetwarzanie

Jeśli zdarzenie nie jest znaczące - powinno zostać rozpatrzone w przyszłości przy korekcie projektu zabezpieczeń. Jeśli natomiast zostało uznane za znaczące powinno zostać obsłużone podobnie jak zdarzenie nieznane (złagodzenie strat i szybkie skorygowanie projektu).

6.10 Wymagania bezpieczeństwa dla systemów zarządzania w telekomunikacji i teleinformatyce

System operacyjny informatycznego systemu zarządzania powinien:

- spełniać co najmniej wymagania grupy F-B1, E3 ITSEC *(ang. Information Technology Security Evaluation Criteria),* co odpowiada grupie B1 TCSEC *(ang. Trusted Computer System Evaluation Criteria*) oraz spełniać wymagania stawiane przed systemami tej klasy.
- Wykorzystywać obowiązkową kontrolę dostępu, posiadać hierarchiczny system bezpieczeństwa dający możliwość zakwalifikowania każdego użytkownika do określonej klasy o zdefiniowanych uprawnieniach.

Administrator systemu powinien mieć możliwość nadawania i odbierania uprawnień dostępu do systemu użytkownikom lub grupom użytkowników. Uprawnienia te dotyczą odczytu, zapisu, monitorowania danych aktualnych lub historycznych. W tym względzie system operacyjny powinien mieć możliwość rejestrowania dostępu i prób dostępu do określonych zasobów.

Użytkownik systemu powinien być rejestrowany w systemie przez:

- system haseł,
- wykorzystanie karty magnetycznej lub karty z hasłem jednokrotnego użytku,
- systemu identyfikacji osobistej (badanie odcisku palca, tęczówki oka, itp.)

System uwierzytelniania powinien być wielostopniowy i w związku z tym aplikacje powinny chronić szczególnie ważne zasoby, żądając podania dodatkowego hasła zabezpieczającego.

Powinna istnieć możliwość ochrony stacji roboczych i terminali przed dostępem osób niepowołanych, jeśli uprawniony użytkownik opuści stanowisko i pozostawi uruchomioną aplikację.

Ze względu na szczególne znaczenie baz danych, system operacyjny powinien gwarantować określony poziom bezpieczeństwa przechowywanych danych i zawierać narzędzia przeznaczone do archiwizacji i wykonywania kopii bezpieczeństwa.

Powinna istnieć możliwość zastosowania urządzeń szyfrujących, jeśli takie wymagania pojawią się na skutek konieczności transmisji danych na nie chronionych kanałach między systemem (elementami systemu) a operatorami telekomunikacyjnymi, zasilającymi system w informacje o posiadanych zasobach, siłach i środkach.

System powinien umożliwiać realizację podziału kompetencji w procesie podejmowania decyzji sterujących oraz odzwierciedlać strukturę funkcjonalną podsystemu zarządzania i utrzymania, w szczególności dla każdego poziomu w hierarchii powinny być określone:

- klasyfikacja informacji przesyłanej w podsystemie zarządzania pod względem przeznaczenia i stopnia pilności,
- prawa dostępu operatora do informacji o systemie,
- wykaz operacji, do których operator jest upoważniony,
- wykaz operacji, które operator może realizować tylko po uzyskaniu akceptacji szczebla nadrzędnego.

System powinien zapewnić:

- uwierzytelnianie użytkowników w systemie (w którego skład wchodzi logowanie się użytkownika),
- bezpieczny dostęp do bazy danych, obejmujący zabezpieczenie:
  - kont poszczególnych użytkowników systemu,
  - uprawnień dla grup występujących w systemie,
- bezpieczny dostęp do danych w bazie,
- sterowanie uruchamianiem procesów działających w systemie,
- sprawowanie nadzoru (monitorowanie) nad zachowaniem poszczególnych użytkowników,
- monitorowanie stanu bezpieczeństwa poszczególnych procesów w systemie.

Oprogramowanie dające możliwość wprowadzenia swoich danych przez użytkownika powinno:

- zostać powiązane z oprogramowaniem realizującym uwierzytelnianie i ograniczanie dostępu do określonych funkcji systemu,
- zostać powiązane z oprogramowaniem ograniczającym dostęp do określonych zasobów nadzorowanych urządzeń,
- nałożyć ograniczenia czasowo-ilościowe na użytkowników wprowadzających dane do weryfikacji.

Hierarchia praw dostępu użytkownika do systemu i jego obiektów, powinna umożliwiać:

- tworzenie i zarządzanie przez osoby uprawnione grupami użytkowników systemu (profilami użytkowników),

- dodawanie i usuwanie użytkowników do lub z danej grupy,
- nadawanie użytkownikom indywidualnych przywilejów zezwalających lub zabraniających określonych czynności w systemie.

7 Charakterystyka technologii realizacji systemów zarządzania w telekomunikacji i teleinformatyce

Zarządzanie w telekomunikacji i teleinformatyce jest dziedziną interdyscyplinarną, obejmuje bowiem w zakresie realizacji systemów wspomagających procesy wykonawcze (eksploatacji i zarządzania) wykorzystanie technologii zapewniających maksymalizację efektywności prowadzonych działań, aby osiągnąć wymaganą jakość oferowanych przez przedsiębiorstwo telekomunikacyjne usług.

W praktyce oznacza to, że struktury organizacyjne systemów zarządzania ulegają dynamicznej zmianie (ewuluują), dopasowując się do potrzeb obsługiwanych zadań, zaś wykorzystywane technologie mają zapewnieć wsparcie funkcjonalne, informacyjne i realizacyjne procesów zarządczych.

Rozległa struktura systemów i sieci telekomunikacyjnych/teleinformatycznych, realizacja większości usług w czasie rzecywistym (*ang. real time)* lub do niego zbliżonym (*ang. quasi real time)* oraz wiele innych uwarunkowań natury realizacyjnej narzuca konieczność stsosowania rozwiązań technicznych opracowanych z myślą o systemach rozproszonych.

W opracowaniu tego rozdziału pomocne okazały się informacje przedstawione w [6], [8], [9], [11], [13], [14], [15] oraz [18].

Z dziedziną zarządzania siecią jest silnie związane *przetwarzanie rozproszone* (ang. *distributed processing):* zarządzanie siecią polega w znacznej mierze na zbieraniu i przetwarzaniu danych pochodzących ze środowiska rozproszonego. W dziedzinie przetwarzania rozproszonego ITU i ISO opracowały model odniesienia ODP *(ang.Open Distributed Processing),* opisany przez ISO w standardzie ISO 10746, a przez ITU - w zaleceniach serii X.900. Celem wprowadzenia modelu ODP jest określenie architektury pozwalającej producentom sprzętu w jednolity sposób opisywać systemy rozproszone i ich składniki.

Ze względu na złożoność i wielostronność zagadnienia ODP nie stworzono jednego zwartego modelu, a opracowano pięć uzupełniających się modeli, określanych mianem *punktów widzenia* (ang. *viewpoints):*

- ***obliczeniowy punkt widzenia*** (ang. *computational viewpoint)* - pozwala opisywać system rozproszony jako zbiór współdziałających obiektów, które funkcjonują opierając się na ustalonych algorytmach i wymieniają między sobą dane (algorytm programu obsługującego system rozproszony);

- ***punkt widzenia przedsiębiorstwa*** (ang. *Enterprise viewpoint),*- pozwala opisywać usługi systemu rozproszonego na podstawie wymagań użytkowników tego systemu, pracujących w danym przedsiębiorstwie;
- ***informacyjny punkt widzenia*** (ang. *information viewpoint)* - dotyczy modelowania informacji opisującej system rozproszony (modelami rzeczywistych zasobów są *obiekty informacyjne,* powiązane zależnościami i zasadami spójności);
- ***inżynierski punkt widzenia*** (ang. *engineering viewpoint)* - pozwala sporządzić projekt systemu realizującego algorytm opisany z obliczeniowego punktu widzenia;
- ***techologiczny punkt widzenia*** (ang. *technology viewpoint)* - pozwala opisać sposób implementacji projektu systemu opisanego z inżynierskiego punktu widzenia..

Funkcje przetwarzania rozproszonego ODP (ang. ODP *functions),* realizowane przez system zgodny z ODP, podzielono w standardzie na cztery grupy:

- *grupę funkcji zarządzania* (np. funkcja zarządzania obiektami),
- *grupę funkcji koordynowania* (np. funkcja przesiania meldunku o zdarzeniu),
- *grupę funkcji przechowywania danych;grupę funkcji bezpieczeństwa* (np. funkcja kontroli dostępu).

Niektóre z funkcji przetwarzania rozproszonego pełnią podobną rolę do funkcji zarządzania systemami SMF.

7.1 Środowisko przetwarzania rozproszonego – DME

Organizacja *Open Software Foundation (OSF)* powstała w 1988 roku i zrzesza obecnie wielkich producentów sprzętu informatycznego (IBM, DEC/COMPAQ, HP, Bull, Philips, Siemens). OSF jest aktywna głównie w dziedzinie przetwarzania rozproszonego. Celem OSF jest wypracowywanie standardowych rozwiązań na bazie produktów, które wcześniej sprawdziły się w praktyce. Gdy OSF rozpoczyna prace nad danym zagadnieniem, wydaje dokument o nazwie RFT *(Request for Technology),* w którym zwraca się do producentów o przedstawienie produktów, które mogą znaleźć zastosowanie w danym przypadku. Tym sposobem OSF opracowało standardową wersję systemu operacyjnego UNIX (OSF/1 UNIX), standardowy interfejs zapewniający użytkownikowi dostęp do programu aplikacyjnego (OSF/.Motif AUI) i środowisko przetwarzania rozproszonego OSF/DCE *(Disfributed Communications Environment).*

W środowisku przetwarzania rozproszonego DCE wykorzystuje się mechanizm *zdalnego wywoływania procedur RPC* (ang. *Remote Procedure Call)* oraz *wątki* (ang. *threads).*

DCE zapewnia cztery podstawowe usługi:

- *usługę katalogową* (ang. Directory Service), która pozwala lokalizować zasoby i procesy w sieci;
- *usługę rozproszonego bezpieczeństwa* (ang. *Distributed Security* Service), która w sposób scentralizowany zapewnia między innymi autentyfikację oraz szyfrowanie przesyłanych danych;
- *usługę rozproszonego czasu* (ang. *Distributed Time* Service), która pozwala synchronizować procesy;
- *usługę rozproszonego dostępu do plików* (ang. *Distributed File* Service).

W dziedzinie zarządzania OSF opracowała *środowisko zarządzania rozproszonego* DME *(Distributed Management Environment).* Głównymi elementami tego środowiska są:

- *interfejsy użytkowników zarządzania* (ang. *management user interface,* które zapewniają użytkownikom możliwość korzystania z programów aplikacyjnych zarządzania;
- programy *aplikacyjne zarządzania* (ang. *management aplications),* które realizują funkcje zarządzania i mogą być uruchamiane w środowisku DCE;
- *usługi dostępu do zarządzanych obiektów* (ang. *object request broker);programy narzędziowe wspomagające projektowanie;graficzny interfejs użytkownika (GUI).*

Do realizacji DME organizacja OSF wybrała następujące produkty:

WizDom: platforma programowa wraz z interfejsami programowania aplikacyjnego, która dostarcza usług zapewniających:

- bezpieczeństwo,
- zarządzanie danymi,
- spis użytkowników,
- dostęp do obiektów.

WizDom jest również wyposażony w interfejs GUI oparty na X Windows (producent - Tivoli Systems

Network Logger: zapewnia obsługę zdarzeń, czyli filtrowanie i przekazywanie meldunków oraz ich przechowywanie w dziennikach (producent - Banyan Systems);***Consolidated ManagementI-API:*** interfejs programowania aplikacyjnego (zestaw funkcji w języku C) zapewniający dostęp do protokołów zarządzania SNMP i CMIP (producent - Bull);***OpenView Network Management Server:*** oprogramowanie, które zapewnia obsługę protokołów SNMP i CMIP (producent - Hewlett-Packard);

HP Software Distribution Utilities (HP SDU): oprogramowanie narzędziowe ułatwiające tworzenie rozproszonych programów aplikacyjnych (producent - Hewlett-Packard);***Network Licence Server (NetLS):*** pozwala monitorować wykorzystanie programów (producent - Hewlett-Packard);***NetLS PC Ally + Client Library:*** umożliwia korzystanie z NetLS również do monitorowania wykorzystania programów zainstalowanych na komputerach osobistych PC (producent - Gradient Technologies);

PC Agent Component: umożliwia zdalny dostęp do komputera PC i wykonywanie funkcji zarządzania i przesyłania danych (producent - Gradient Technologies);

PC *Event Component:* umożliwia przesyłanie meldunków w razie nieprawidłowego funkcjonowania komputera PC (producent - Gradient Technologies);

***Palladium version* 2:** obsługa drukowania w środowisku rozproszonym (producenci - MIT, DEC, HP i IBM);

Data Engine: umożliwia monitorowanie wydajności zasobów i sterowanie nimi (producent - IBM).

W DME mogą być stosowane protokoły SNMP, CMIP, a także zdalne wywoływanie procedur (RPC), zdefiniowane dla środowiska DCE. Specyfikacji obiektów w DME dokonuje się w *języku I4DL (Interface, Inheritance, Implementation, Instanciation Description Language.*OSF współpracuje z ISO i NM Forum, a także z *OMG (Object Management Group)* w ramach grupy *HOG (Hilton Object Group*).

Katalog

Zalecenia opisujące *Katalog* (ang. *Directory)* zostały opracowane przez ISO i ITU po to, by ułatwić tworzenie *systemów wyszukiwania informacji.* Katalog może być wykorzystywany w zarządzaniu siecią do pełnienia funkcji pomocniczych związanych z przechowywaniem danych i dostępem do nich.

Na przykład w Katalogu mogą być przechowywane (w notacji ASN.1) formaty jednostek danych PDU: proces, który potrzebuje formatu danej jednostki PDU, przesyła do Katalogu jej

nazwę rozróżnialną DN i w odpowiedzi otrzymuje potrzebny mu opis tej jednostki PDU w notacji ASN.1.

Dane znajdujące się w Katalogu są przechowywane w *bazie informacji Katalogu DIB* (ang. *Directory Information Base),* która odgrywa rolę podobną do roli bazy MIB. Jednostką organizacyjną w bazie DIB jest *pozycja katalogowa* (ang. entry*).* Każda pozycja katalogowa zawiera atrybuty, które mają wartość i typ. Pozycje katalogowe tworzą *drzewo informacji Katalogu DIT* (ang. *Directory Information Tree).*

Usługi Katalogu zostały zaszeregowane do czterech grup, które podano poniżej:

grupa *Pytań (Interrogation),* która zawiera następujące usługi:

- *Read:* odczytanie wartości atrybutów wybranej pozycji katalogowej;
- *Compare.* porównanie danej wartości z wartością wybranego atrybutu pozycji katalogowej;
- *List:* uzyskanie listy pozycji podrzędnych danej pozycji katalogowej (znajdujących się poniżej w drzewie DIT);
- *Search:* odczytanie atrybutów wszystkich pozycji katalogowych, które spełniają dany warunek,
- *Abandon:* przerwanie przez użytkownika wykonywania zlecenia skierowanego do Katalogu;

grupa Modyfikacji (Modification), *do* której zakwalifikowano następujące usługi:

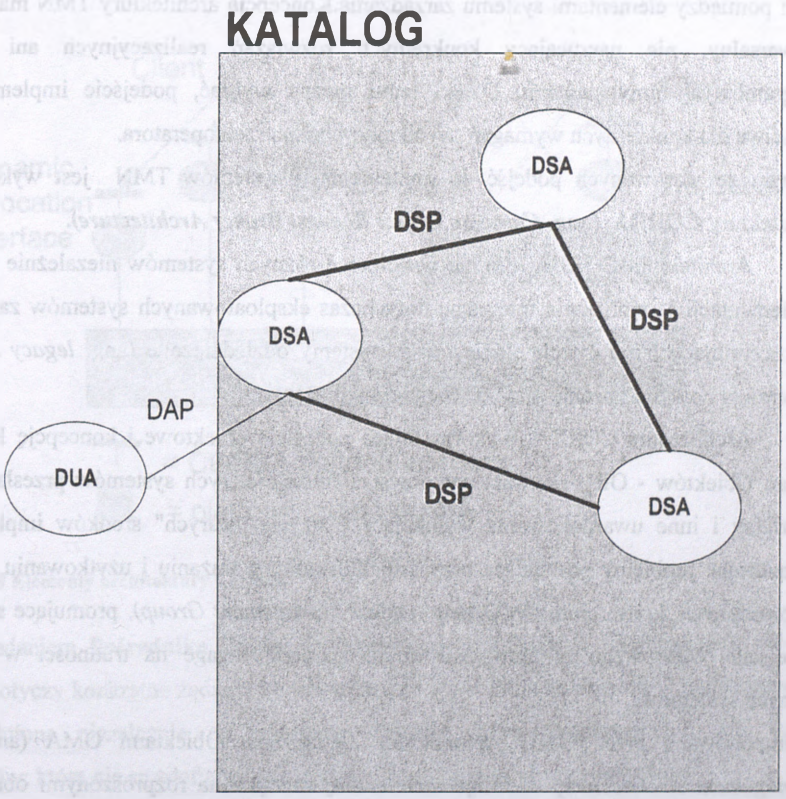
- *Add Entry:* dodanie nowej pozycji katalogowej do Katalogu;
- *Remove Entry.* usunięcie istniejącej pozycji z Katalogu;
- *Modify Entry:* modyfikacja pozycji katalogowej (dodanie, usunięcie lub zmiana typu lub wartości atrybutu);
- *Modify RDN:* zmiana nazwy RDN pozycji katalogowej w drzewie DIT;

grupa *Jakości Usługi (Service Quality),* w której znalazły się następujące usługi:

- *Controls_*- ustalenie zasad dostępu do Katalogu i dokonywania w nim modyfikacji (np. czas trwania dostępu, rozmiar uzyskiwanych danych);
- *Security* - ustalenie procedur związanych z bezpieczeństwem Katalogu (np. hasło, autentyfikacja);
- *Filters.*- definiowanie warunków, które muszą spełniać wyszukiwane dane;

grupa *Usług Innych,* która zawiera następujące usługi:

- *Errors* - ustalenie warunków i sposobu przesyłania przez Katalog zawiadomień o biedach;
- *Rcfcrrals* - podanie przez Katalog odnośnika do innej pozycji katalogowe), w które) mogą się znaleźć szukane dane



Rysunek 48 Model rozproszonego systemu katalogowego

Użytkownik uzyskuje dostęp do Katalogu poprzez proces *agenta użytkownika Katalogu DUA* (ang. *Directory User Agent).* Jeśli Katalog jest realizowany w sposób rozproszony, to jego model opiera się na współpracujących ze sobą procesach *agenta systemu Katalogu DSA* (ang. *Directory System Agent).* Procesy DSA wymieniają między sobą dane korzystając z *protokołu DSP* (ang. *Directory System Protocol),* a dostęp procesu DUA do dowolnego procesu DSA odbywa się przy pomocy *protokołu DAP* (ang. *Directory Acccss Protocol).*

7.2 CORBA

Sieć Zarządzania Telekomunikacją TMN stanowi szeroko akceptowaną architekturę jednolitego zarządzania zasobami sieci i usługami, która wprowadza znormalizowany sposób-modelowania usług zarządzania, informacji zarządzania oraz określa standardowe styki pomiędzy elementami systemu zarządzania.Koncepcja architektury TMN ma charakter uniwersalny, nie narzucający konkretnych rozwiązań realizacyjnych ani środków programowych implementacji. Dzięki temu można wybrać, podejście implementacyjne właściwe dla konkretnych wymagań wynikających z potrzeb operatora.

Jednym ze stosowanych podejść do implementacji systemów TMN jest wykorzystanie architektury **CORBA (ang. *Common Object Request Broker Architecture).***

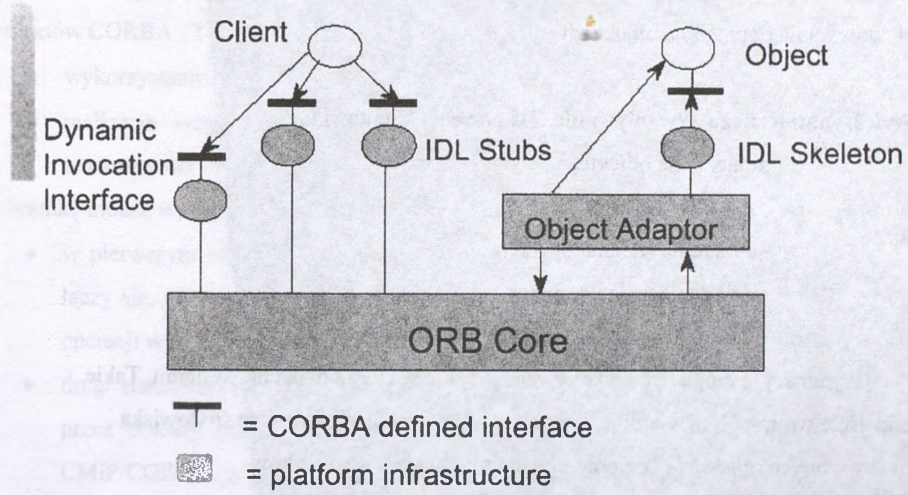
Architektura CORBA, oferuje współpracę różnych systemów niezależnie od języka implementacji i umożliwia integrację dotychczas eksploatowanych systemów zarządzania, wykorzystujących stare technologie - tzw. systemy odziedziczone (ang. *legacy sytems),* z systemami nowymi obecnie projektowanymi i wdrażanymi.

Architektura CORBA, wykorzystująca podejście obiektowe i koncepcję Pośrednika Żądań Obiektów - ORB pozwala wykorzystać funkcje starych systemów przesłaniając ich interfejsy i inne uwarunkowania wynikające z użycia "starych" środków implementacji. Rozpatrując problemy powstające przy projektowaniu, wdrażaniu i użytkowaniu systemów rozproszonych, konsorcjum OMG (ang. *Object Management Group),* promujące stosowanie podejścia obiektowego w oprogramowaniu, zwróciło uwagę na trudności w integracji różnych systemów.

Zaproponowana przez OMG Architektura Zarządzania Obiektami OMA (ang. *Object Management Architecture)* definiuje architekturę zarządzania rozproszonymi obiektami na wysokim poziomie abstrakcji.

OMA specyfikowana jest poprzez określenie styków (interfejsów) i protokołów. Konkretne specyfikacje opierają się na istniejących technologiach, spełniających wymagani techniczne OMG. Architektura OMA jest architekturą odniesienia i jest podstawą do tworzenia aplikacji.Podstawowymi elementami specyfikacji CORBA są:

- Pośrednik Żądań Obiektów (ang. *Object Request Broker)*
- Język Definicji Styków (ang. *Interface Definition Language)*
- Styk Dynamicznego Wywoływania (ang. *Dynamie Invocation Interface)*



Rysunek 49 Elementy architektury CORBA

Zadaniem **Pośrednika Żądań Obiektów** jest znajdywanie implementacji obiektu, którego dotyczy konkretne żądanie i przekazywanie wywołania do obiektu. Żądanie powinno być obsłuione niezależnie od położenia obiektu, języka implementacji lub innych parametrów; które nie są żdefiniowane w styku obiektu (ang. *object's interface).*

Klient, który chce skorzystać z usług (metod) innego obiektu przy pomocy ORB, może to zrobić na dwa sposoby: wykorzystując styk obiektu opisany nagłówkiem (ang. *stub)* wygenerowanym z pliku opisu w Języku Definicji Styków IDL lub wykorzystując Styk Dynamicznego Wywoływania DII, niezależny od styku obiektu docelowego.

Z kolei ORB przekazuje dane do implementacji obiektu oraz wywołuje usługi obiektu wykorzystując tzw. szkielet IDL lub szkielet dynamiczny. Szkielety są powiązane z konkretną implementacją Adaptera Obiektów (ang. *0bject Adapter)* i mogą wywoływać funkcje ORB przez Adapter Obiektów.

Język Definicji Styków IDL. służy do definiowania obiektów w postaci styku obiektu, czyli, zbioru operacji i parametrów związanych z tymi operacjami. IDL jest ogólnym opisem obiektu pozwalającym określić operacje (usługi) jakie obiekt może wykonać i parametry wymagane do wywołania konkretnej operacji. Nie jest on jednak językiem

programowania, językiem implementacji - nie określa wewnętrznej struktury obiektów, nie służy do tworzenia implementacji obiektów, a jedynie do opisu obiektów, których implementacja w konkretnym języku programowania jest dana lub będzie stworzona później.

IDL jest językiem obiektowym, udostępniającym mechanizm dziedziczenia (także wielokrotnego) oraz obsługę wyjątków (ang. *exception). W* wyniku kompilacji pliku z opisem obiektów w języku IDL powstaje tzw. nagłówek (ang. *stub),* wykorzystywany przez ORB do wywoływania operacji na obiektach

Styk Dynamicznego Wywoływania DII pozwala klientowi na:

- znalezienie obiektu,
- znalezienie styku obiektu,
- stworzenie żądania operacji,
- wywołanie żądania operacji,
- otrzymania wyniku wykonania operacji

Czynności te mogą być wykonywane jedynie w czasie działania systemu. Takie podejście we współpracy aplikacji z obiektami pozwala korzystać ze środowiska rozproszonych obiektów, bez potrzeby uaktualniania wersji styków.

7.3 CORBA a TMN

Połączenie dwóch systemów zarządzania, wykorzystujących różne technologie - TMN i CORBA - wymaga odwzorowania modeli informacyjnych oraz umożliwienia współpracy pomiędzy różnymi protokołami. Konieczne jest więc ustalenie sposobu opisywania modelu odniesienia TMN w technologii CORBA, w szczególności przetwarzanie obiektów modelu, zapisanych w języku formalnym (notacja ASN.l w przypadku obiektów TMN), na definicje obiektów w architekturze CORBA, posługującej się językiem IDL. Potrzebne jest więc ustalenie zasad Przetwarzania Specyfikacji (ang. *Specificatinn Translation)* pomiędzy Siecią Zarządzania Telekomunikacją - 'I'MN a architekturą CORBA.Oprócz ustalenia schematu przetwarzania modeli obiektowych należy również określić mechanizm dynamicznej konwersji protokołów i zachowań występujących w dwóch środowiskach. Przetwarzanie Interakcji (ang. *Interaction Translation)* powinno umożliwiać w pełni obsługę obiektu, niezależnie w której domenie się znajduje, tzn. dostęp do obiektów TMN dla obiektów spoza domeny, wykorzystujących technologię CORBA w celu wykonania operacji na obiekcie, powinien być taki sam jak obiektów należących do domeny TMN. Z kolei obiekty TMN powinny móc w ten sam sposób wywoływać operacje na obiektach spoza domeny TMN w

jaki wykonują operacje na obiektach wewnątrz domeny. Możliwość wykonywania operacji na obiekcie nie powinna być zależna od domeny implementacji. Wykorzystanie architektury CORBA jako wspólnej platformy dla obiektów zaimplementowanych w różnych językach programowania; pozwala na wiele różnych sposobów realizacji dostępu do zarządzanych obiektów TMN. Formułując wymagania na propozycje specyfikacji styków dla aplikacji telekomunikacyjnych konsorcjum OMG przedstawiło następujące warianty współpracy obiektów CORBA i TMN:

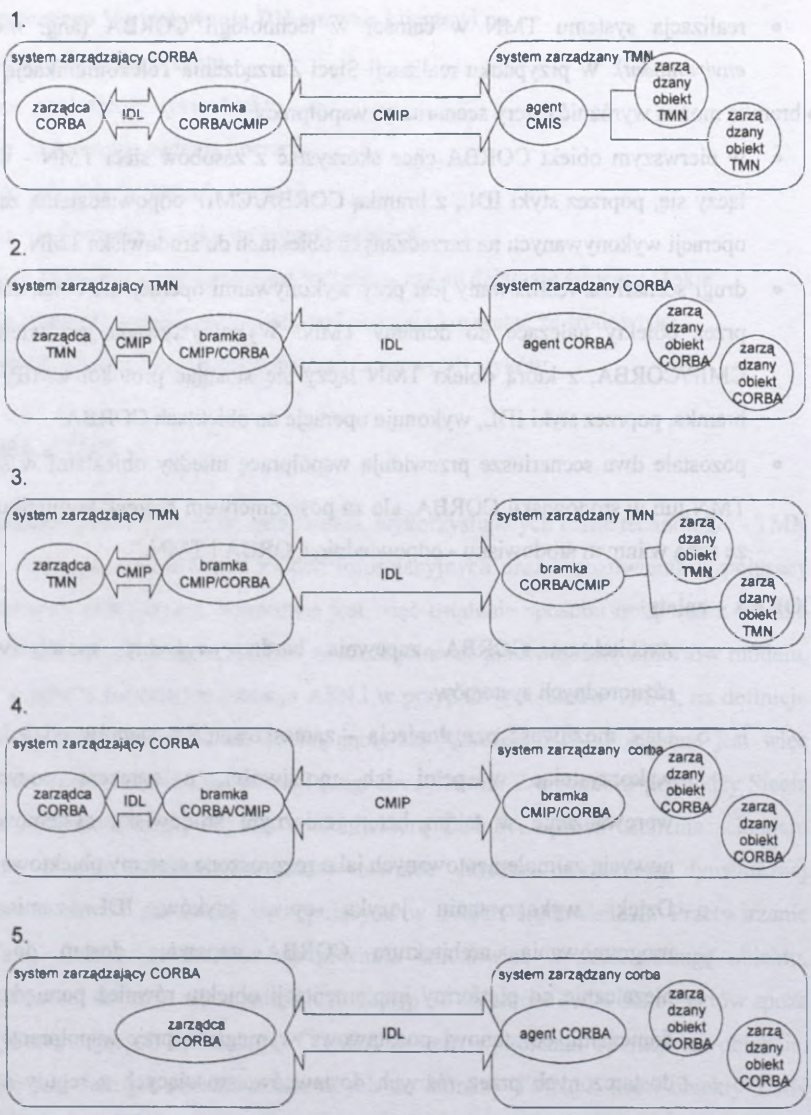
- wykorzystanie "bramki" do systemu TMN (ang. *gateway environment),*
- realizacja systemu TMN w całości w technologii CORBA (ang. *non-gateway environment).* W przypadku realizacji Sieci Zarządzania Telekomunikacją w oparciu o bramkę można wyróżnić cztery scenariusze współpracy:
- w pierwszym obiekt CORBA chce skorzystać z zasobów sieci TMN - w tym celu łączy się, poprzez styki IDL, z bramką CORBA/CMIP odpowiedzialną za translację operacji wykonywanych na zarządzanych obiektach do środowiska TMN.
- drugi scenariusz realizowany jest przy wykonywaniu operacji na obiektach CORBA przez obiekty należące do domeny TMN. Wykorzystywana jest wtedy bramka CMIP/CORBA, z którą obiekt TMN łączy się stosując protokół CMIP, natomiast bramka, poprzez styki IDL, wykonuje operacje na obiektach CORBA.
- pozostałe dwa scenariusze przewidują współpracę między obiektami w środowisku TMN lub w środowisku CORBA, ale za pośrednictwem bramek komunikujących się ze sobą w innym środowisku - odpowiednio CORBA i TMN.

CORBA – zalety

- Architektura CORBA zapewnia bardzo wygodny sposób współpracy różnorodnych systemów.
- Daje możliwość przesłonięcia - zamaskowania systemów odziedziczonych, wykorzystując w pełni ich możliwości, a zarazem pozwalając na wprowadzenie w takim heterogenicznym środowisku systemów zupełnie nowych, zaimplementowanych jako rozproszone systemy obiektowe.
- Dzięki wykorzystaniu języka opisu styków IDL zamiast języka programowania, architektura CORBA zapewnia dostęp do obiektów niezależnie od platformy implementacji obiektu również pomiędzy różnymi domenami, co stanowi podstawowe wymaganie przy współpracy systemów dostarczonych przez różnych dostawców, stosujących z reguły specyficzne rozwiązania firmowe.Dostęp do systemów odziedziczonych jest istotny również z powodu o wiele dłuższego czasu życia urządzeń i systemów

telekomunikacyjnych w stosunku do systemów informatycznych. Spowodowane jest to głównie wysokimi kosztami uruchomienia systemu oraz długim czasem zwrotu inwestycji telekomunikacyjnej.

- Technologia CORBA oferuje możliwość włączenia nawet bardzo starych systemów do współpracy ze sprzętem i oprogramowaniem nowszej generacji, co może okazać się konieczne ze względu na potrzebę zachowania ciągłości funkcji zarządzania usługami i sprzętem.



Rysunek 50 CORBA w systemach zarządzania

CORBA - wady

Rozwiązania wykorzystujące architekturę CORBA mają jednak dość istotną wadę - wydajność nie jest zadowalająca w zastosowaniach wymagających efektywnego działania w czasie rzeczywistym. Może być ona natomiast stosowana do realizacji różnych funkcji zarządzania siecią i usługami. które nie są krytycznie uwarunkowane czasowo. Na przykład z powodzeniem może zostać wykorzystana w aplikacjach służących do sprawdzania stanu elementów sieci, tworzenia różnego rodzaju raportów, zgłaszania pewnych rodzajów alarmów. Wydajność dostępnych platform sprzętowych nie pozwala obecnie zastosować technologii CORBA np. do obsługi połączeń i realizacji usług telekomunikacyjnych na dużą skalę.

7.4 TINA

Złożone usługi telekomunikacyjne oraz coraz bardziej zaawansowane systemy komunikacji osobistej, telefonia ruchoma, systemy multimedialne, czy też usługi świadczone w sieciach szerokopasmowych itd. wymagają bardziej elastycznego sposobu dostępu niż ten, jaki są w stanie zapewnić istniejące sieci.

Ciągłe dążenie do minimalizacji kosztów związanych z uruchamianiem nowych usług powoduje, że takie cechy oprogramowania sterującego siecią, jak: przenośność *(portability),* możliwość współpracy *(interoperability)* czy możliwość wielokrotnego stosowania tego samego oprogramowania *(reuse)* zaczynają odgrywać podstawową rolę w procesie definiowania i wdrażania usług.

Przed producentami sprzętu i operatorami sieci pojawiło się zadanie stworzenia architektury sprzętowo-programowej pozwalającej na tworzenie i świadczenie nowych usług oraz umożliwiającej zarządzanie nimi.W tym celu w październiku 1992 roku podczas konferencji ISS *(International Switching Symposium)* w Yokohamie powstało konsorcjum nazwane TINA-C (TINA-C - *Telecom-munication Information Networking Architecture Consortium)* jako inicjatywa mająca na celu współpracę naukowo-badawczą między głównymi światowymi operatorami telekomunikacyjnymi oraz producentami sprzętu teleinformatycznego.

Celem konsorcjum TINA jest zdefiniowanie otwartej architektury sieci oferującej usługi telekomunikacyjne, a jednocześnie pozwalającej na sprawne zarządzanie zarówno samą siecią, jak i realizowanymi w niej usługami, testowanie tej architektury oraz jej promocja.

Członkami organizacji TINA-C są trzy grupy instytucji:

- operatorzy telekomunikacyjni i związane z nimi instytuty badawcze (AT&T, Bellcore, BNR, British Telecom, CSELT, Deutsche Telekom AG, Dutch Telecom, France Telecom, Korea Telecom, Norwegian Telecom, NTT, Portugal Telecom, Swiss Telecom PTT, Tele Danmark, Telenor, TELIA Research, Bell Atlantic, Ameritech, US West, Beli South, Southwestern Beli);
- dostawcy sprzętu telekomunikacyjnego (Alcatel, Ericsson, Fujitsu, Hitachi, NEC, Nokia, Northern Telecom, OKI Siemens);
- dostawcy sprzętu informatycznego (DEC, Hewlett Packard, Stratus Computer, Samsung, Sun, Unisys).**Cele powstania TINA**

- TINA jest architekturą wspomagającą konstruowanie platform oprogramowania telekomunikacyjnego. Pozwala to na opis syntaktyczny i semantyczny modułów oprogramowania, jak i na specyfikację rozproszonego środowiska, w którym oprogramowanie to będzie instalowane.
- TINA jest również architekturą opisującą usługi telekomunikacyjne oraz aplikacje związane z zarządzaniem nimi.
- Dokumentacja architektury TINA zawiera wykaz prostych komponentów, przy użyciu których, według określonych zasad, można definiować nowe usługi (pojęcie komponentów zaczerpnięto z koncepcji sieci inteligentnych).Komponenty usługowe pozwalają również na tworzenie aplikacji związanych z zarządzaniem nowo powstającymi usługami. To podwójne zastosowanie komponentów przyspiesza równoległy rozwój oprogramowania realizującego usługę oraz oprogramowania nią zarządzającego.

Architektura ta powinna zatem spełniać cztery warunki:

- zapewniać modularność i przenośność *(reuse)* oprogramowania,
- tworzyć środowisko pozwalające na współpracę wielu producentów,
- mieć jasną, przejrzystą, warstwową strukturę oprogramowania,
- realizować integrację usług i aplikacji zarządzania.Architektura ta wykorzystuje techniki stosowane w przetwarzaniu rozproszonym zorientowanym obiektowo oraz istniejące już standardy, stosowane w telekomunikacji: ODP, OMG/CORBA, IN, TMN, ATM, OMT.

Zasadniczą strategią dominującą w pracach konsorcjum jest integracja usług, zarządzania, aspektów technologicznych oraz przetwarzania rozproszonego.

Prace projektowe realizowane w ramach konsorcjum skupiają się przede wszystkim na projektowaniu oprogramowania, a nie na projektowaniu bądź produkcji sprzętu.

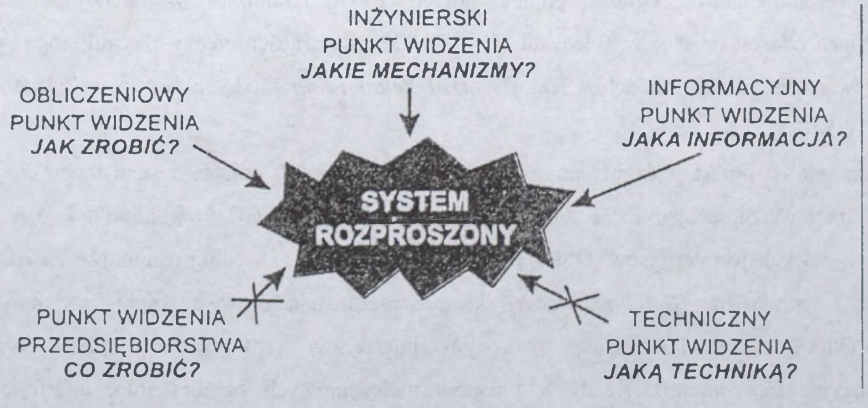
Prace badawcze realizowane w ramach konsorcjum można podzielić na cztery obszary:

- architektury obliczeniowej (architektury logicznej),
- architektury usług, czyli specyfikacji, metodyki tworzenia usług oraz zarządzania nimi,
- architektury zarządzania oraz metodyki zarządzania zasobami,
- zaleceń określających implementację **środowiska rozproszonego przetwarzania** TINA-C (TINA-C DPE).

Architektura obliczeniowa TINA została opisana zgodnie z terminologią ODP *(Open Distributed Processing).*

Model ODP określa pięć tak zwanych punktów widzenia *(View-points)* systemu rozproszonego:

- punkt widzenia przedsiębiorstwa *(Enterprise Viewpoint),*
- informacyjny punkt widzenia *(Information Viewpoint),*
- obliczeniowy punkt widzenia *(Computation Viewpoint),*
- inżynierski punkt widzenia *(Engineering Viewpoint),*
- technologiczny punkt widzenia *(Technotogy Viewpoint).*



Rysunek 51 Wpływ "punktów widzenia" na system rozproszony

Punkt widzenia przedsiębiorstwa *(ang.Enterprise Viewpoint)* nie jest rozpatrywany w architekturze TINA. Głównym problemem rozwiązywanym w tej części specyfikacji ODP jest ustalenie założeń dotyczących nadzoru systemu *(policy statements).* Założenia te definiuje się za pomocą zbioru pewnych zasad. Zasady te określają, jakie akcje (działania) są dozwolone, jakie zabronione, a jakie obowiązkowe. Definiują też ograniczenia nakładane na system. Podają tak zwany szablon specyfikacji nadzoru *(Policy Specification Template*
Szablon taki składa się z pięciu atrybutów.

- **Tryb** *(modalify)* wyraża, czy dana działalność może lub czy musi być podejmowana.
- **Działanie** *(activity)* opisuje zbiór podejmowanych akcji.
- **Podmiot** *(subject)* określa, kto wykonuje daną akcję.
- **Cel** *(target)* określa jednostki, "na których" akcje są wykonywane.
- **Ograniczenia** *(constraints) są* nakładane na wykonywane działania.

Informacyjny punkt widzenia *(ang. Information Viewpoint)* określa dwie możliwości reprezentowania istniejących zasobów. Pierwszy, graficzny model informacyjny zasobów sieci został zaczerpnięty ze zorientowanej obiektowo techniki modelowania OMT. Wykorzystuje ona pojęcia klas obiektów, opisuje ich zachowanie oraz zależności panujące między nimi (asocjacje, agregacje itd.) za pomocą reprezentacji graficznej. Druga możliwość to reprezentowanie obiektów za pomocą notacji GDMO *(Guidlines for the Definition of Managed Objects* opisane w Zaleceniu ITU-T X.722). Zależności między klasami mogą być opisywane za pomocą modelu GRM *(General Relationship* Modę/opisanego w Zaleceniu ITU-T X.724).

Obliczeniowy punkt widzenia ang. *(Computation Viewpoint)* opisuje system rozproszony jako zbiór współpracujących ze sobą obiektów obliczeniowych CO *(computational objects) oraz* łączących je interfejsów. Obiekty CO mogą być łączone według ustalonych zasad w bloki konstrukcyjne *(Building Blocks),* które współpracują ze sobą dzięki zawieranym kontraktom *(Contracts).* Istnieją dwa typy interfejsów: strumieniowe *(stream) oraz* operacyjne *(operational).* Każdy z obiektów obliczeniowych zawiera zbiór interfejsów związanych z usługami oraz z zarządzaniem.

Inżynierski punkt widzenia *(ang. Engineering Viewpoint)* opisuje abstrakcyjną architekturę, która pozwala na implementację obiektów obliczeniowych CO. Obiekty obliczeniowe są odwzorowywane "jeden do jeden" w inżynierskie obiekty obliczeniowe *(Engineering Computational Objects).* Definiuje się również tzw. grona *(cluster)* stanowiące tu odpowiedniki komponentów BB *(building blocks)* z modelu obliczeniowego. Kapsuły

(capsuls) grupują grona i stanowią podzbiory węzłów *(nodes).* Węzły stanowią abstrakcyjny opis systemu obliczeniowego składającego się z kapsuł modelujących pojedyncze urządzenia wirtualne. Z kolei grona modelują współpracujące ze sobą grupy obiektów.

Technologiczny punkt widzenia *(ang. Technology Viewpoint)* opisuje sposób implementacji w rzeczywistym środowisku obiektu opisanego wcześniej z inżynierskiego punktu widzenia.

W architekturze TINA wykorzystuje się trzy koncepcje:

- •modelowania informacji,
- •modelowania obliczeniowego,
- •modelowania inżynierskiego.

Koncepcja modelowania informacji pozwala na specyfikację informacji. Specyfikacja taka opisuje strukturę informacji posiadanej i używanej przez system. Opierając się na tej koncepcji definiuje się obiekty odzwierciedlające zasoby sieci, relacje panujące między nimi oraz ograniczenia i inne zasady określające ich współpracę. Specyfikacja informacji skupia się tylko na jednostkach informacyjnych i relacjach panujących między nimi. Nie rozpatruje się tu problemów związanych z rozproszeniem sprzętowym systemu.

Koncepcja modelowania obliczeniowego pozwala na przygotowanie specyfikacji obliczeniowej. Specyfikacja taka opisuje rozproszoną aplikację telekomunikacyjną widzianą jako zbiór współdziałających ze sobą jednostek obliczeniowych. Interakcje między jednostkami obliczeniowymi opisuje się za pomocą:

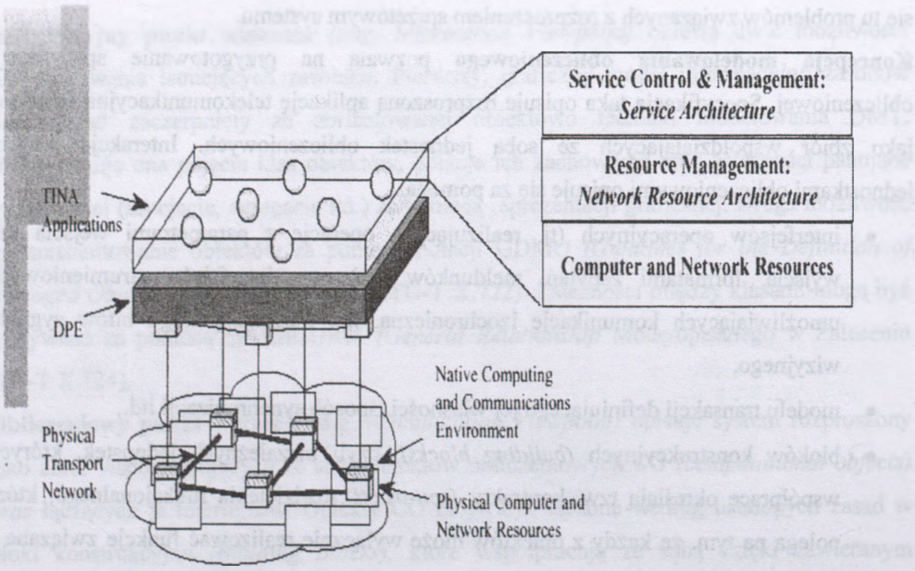
- interfejsów operacyjnych (tj. realizujących operacje z parametrami wejścia lub wyjścia, formatami zapytań, meldunków itp.) oraz interfejsów strumieniowych umożliwiających komunikację izochroniczną, np. transmisję ciągu bitów sygnału wizyjnego,
- modelu transakcji definiującego jej własności, sposób synchronizacji itd.,
- bloków konstrukcyjnych *(building blocks),* czyli niezależnych jednostek, których współpracę określają tzw. kontrakty *(con-tracts),*rozdzielenia funkcjonalnego, które polega na tym, że każdy z obiektów może wyłącznie realizować funkcje związane z obsługą interfejsu użytkownika, z zarządzaniem danymi wykorzystywanymi przez szereg obiektów bądź inne określone funkcje.

Architektura TINA opisuje dwa typy obiektów obliczeniowych, które wykonują usługi dla obiektów obliczeniowych (CO) realizujących daną aplikację. Są to tzw. serwery informacyjne *(trader servers)* i serwery meldunków.

Koncepcja modelowania inżynierskiego pokazuje metodykę tworzenia specyfikacji inżynierskiej. Specyfikacja ta pozwala na zrealizowanie koncepcji obliczeniowej. Budowa modelu inżynierskiego opiera się na trzech grupach jednostek inżynierskich zdefiniowanych

w ramach ODP, mianowicie na węzłach, kapsułach i gronach. Węzły przetwarzające dane są połączone ze sobą za pomocą tzw. sieci transportowej jądra *(kernel transport network).* Sieć ta jest logicznie rozdzielona od sieci używanej do izochronicznej transmisji informacji pomiędzy współpracującymi stacjami.

Model inżynierski definiuje również pewne pojęcia niezbędne do zarządzania rozproszonymi zasobami fizycznymi oraz lokalnymi zasobami sieci. Pojęcia te tworzą łącznie definicję **rozproszonego środowiska przetwarzania** DPE *(Distributed Processing Environment),* które pozwala na współpracę obiektów obliczeniowych. DPE składa się ze środowiska uruchomieniowego *(run-time DPE)* oraz zbioru narzędzi. Środowisko uruchomieniowe tworzą: jądra systemu rezydujące w każdym węźle obliczeniowym (odpowiedzialne za procedury komunikacyjne, składowanie danych) oraz serwery DPE, które umożliwiają między innymi realizację przezroczystości współbieżności procesów oraz przezroczystości lokalizacji procesów.



Rysunek 52 Elementy architektury TINA

Założenia architektury obliczeniowej TINA opierają się na dwóch wcześniejszych architekturach, tj. na architekturze OSCA zaprojektowanej w 1992 roku przez Bellcore oraz na architekturze CORBA zdefiniowanej przez OMG. Wspomnianą wyżej koncepcję bloków

konstrukcyjnych zaczerpnięto z opisu architektury OSCA. Definiowane w architekturze TINA bloki konstrukcyjne są odpowiednikami komponentów oprogramowania z architektury OSCA. Blok konstrukcyjny można porównać do kontenera zawierającego zbiór obiektów wraz z ich interfejsami. Sposoby komunikacji obiektów należących do jednego bloku z obiektami należącymi do innych bloków określają tzw. kontrakty.

Język wybrany do formalnego zapisu modelu obliczeniowego (w tym kontraktów i interfejsów) stanowi wzbogaconą wersję języka OMG I DL *(Object Management Group Interface Definition Language),* nazwaną ODL (język ten jest oparty na IDL, ale uzupełniony szablonami specyfikacji danych oraz interfejsów *zarówno* dla CO, jak i BB).

Model współpracy bloków konstrukcyjnych w środowisku rozproszonym i heterogenicznym zaczerpnięto z architektury CORBA *(Common Object Request Broker Architecture).* Model ten wykorzystuje mechanizm procedury RPC *(Remote Procedure Call).* Z kolei tryb przesyłania meldunków i wiadomości oraz zawierania transakcji jest wzorowany na protokole zarządzania CMIP standaryzowanym przez OSI.Na ostateczny kształt koncepcji architektury usługowej silny wpływ miała opracowana wcześniej architektura zaawansowanych sieci inteligentnych (AIN). Poza nią wykorzystano tu również wyniki badań w następujących dziedzinach: B-ISDN, ODP, OSI oraz programów badawczych RACE-ROSA i RACE-CASSIOPEIA.

Tina – architektura usługowa

Definicja usługi została zaczerpnięta z projektu architektury ROSA. Według niej usługa to zbiór możliwości oferowanych przez istniejącą bądź tworzoną sieć. Definiując usługę, TINA-C zwraca szczególną uwagę na pięciu udziałowców (abonent sieci, dostawca i zarządca usługi, operator sieci oraz sprzedawca usługi), którzy w różny sposób są zaangażowani w realizację usługi. Identyfikacja tych udziałowców jest podstawą do rozróżnienia na poziomie definicji usługi, kto i w jaki sposób jest zaangażowany w konkretną usługę.

Architektura usługi wyraźnie odróżnia więc funkcje związane z kontrolą konkretnej usługi od funkcji związanych z zarządzaniem zasobami sieci oraz od funkcji określonych w **uniwersalnym modelu komponentów** usług *{Universal Service Component* Model). Taka separacja, znana wcześniej w architekturze sieci inteligentnych, gdzie wyróżniano m.in. poziom komutacji usługi (SSP) i poziom kontroli usługi (SCP), ma kilka podstawowych zalet:

- niezależność rozwoju usługi od rozwoju zasobów sieci, co umożliwia w razie potrzeby szybką implementację nowych bądź modyfikację istniejących usług;
- niezależność usługi od konkretnej techniki komunikacji (przesyłanie obrazu może być realizowane zarówno w sieci ATM, jak i ISDN);
- możliwość zwiększenia efektywności zarządzania zasobami sieci.Zarówno kontrola usług, jak i zarządzanie zasobami, są modelowane za pomocą tej samej koncepcji opisanej przez architekturę logiczną.

Zadaniami stawianymi architekturze usługowej są:

- zdefiniowanie serwerów dedykowanych poszczególnym aplikacjom oraz ogólnych (generycznych) obiektów potrzebnych do tworzenia konkretnych usług,
- określenie zasad, według których powinny być używane serwery i obiekty.

Architektura usługowa wprowadza dodatkowe, w stosunku do architektury logicznej, ograniczenia wobec systemu rozproszonego. Usługi są zdefiniowane za pomocą kompletnych komponentów (modułów), stanowiących identyfikowalne części każdej tworzonej usługi.W modelowaniu usług korzysta się z modelu USCM.
Według jego założeń, każdy komponent usługi składa się z wielu obiektów określających rozmaite aspekty tego komponentu, takie jak:

- wykorzystanie *{usage}* komponentu - określa ono interfejs użytkownika związany z usługą;
- własności *{substance)* komponentu - określają one sposób współpracy z innymi, zewnętrznymi zasobami sieci oraz z pozostałymi usługami;
- zarządzanie *[management)* - definiuje ono wymagania oraz techniki umożliwiające zarządzanie usługą;
- jądro *(kernel)* - identyfikuje ono typ usługi oraz określa jej naturę niezależnie od tego, jak i za pomocą jakiej technologii jest ona implementowana oraz zarządzana.

Prowadzone w ramach konsorcjum TINA prace w dziedzinie zarządzania zasobami mają na celu określenie, w jaki sposób zasoby istniejące fizycznie mogą być zarządzane. Prace skupiają się wokół czterech kierunków badań:

- zarządzania usługą,
- zarządzania zasobami sieci,
- zarządzania DPE *(Distributed Processing Environment),*

- zarządzania zasobami multimedialnymi.

Ogólny model zarządzania zasobami został zaczerpnięty z systemu zarządzania OSI oraz TMN. Ze standardów OSI zaczerpnięto m.in. klasyczny podział na pięć obszarów zarządzania, zaś ze standardu TMN podział na warstwy zarządzania (warstwa zarządzania usługą, siecią oraz elementem i warstwa elementu sieci)

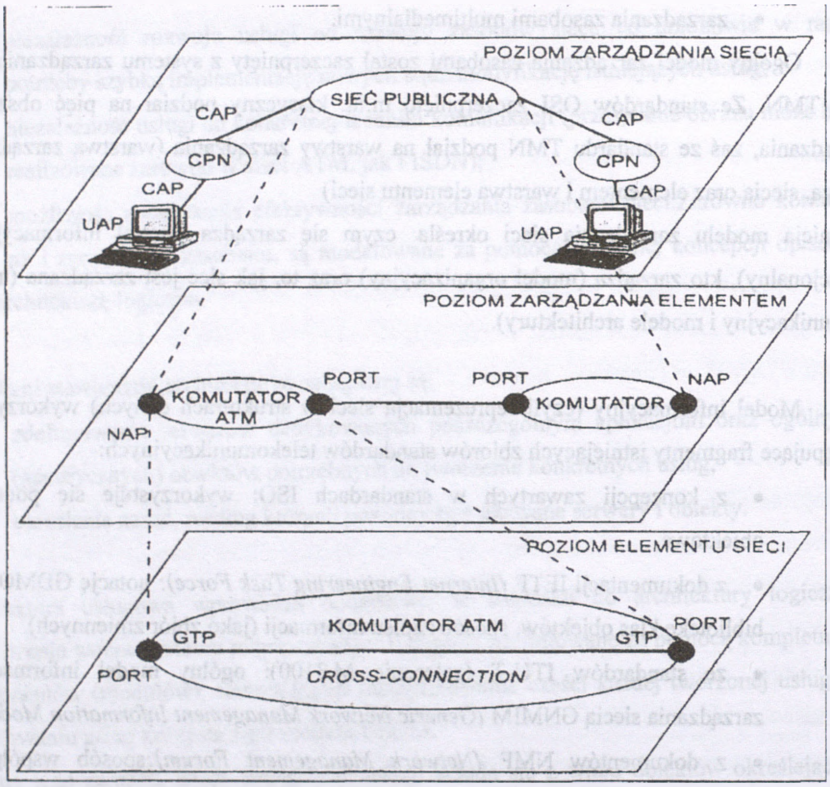
Definicja modelu zarządzania sieci określa: czym się zarządza (model informacyjny i funkcjonalny), kto zarządza (model organizacyjny) oraz to, jak sieć jest zarządzana (model komunikacyjny i modele architektury).

Model informacyjny (czyli reprezentacja sieci w strukturach danych) wykorzystuje następujące fragmenty istniejących zbiorów standardów telekomunikacyjnych:

- z koncepcji zawartych w standardach ISO: wykorzystuje się podejście obiektowe,
- z dokumentacji IETF *(Internet Engineering Task Force):* notację GDMO oraz bibliotekę klas obiektów, sposób zapisu informacji (jako zbiór zmiennych).
- ze standardów ITU-T (zalecenie M.3100): ogólny model informacyjny zarządzania siecią GNMIM *(Generic Network Management Information Model),*
- z dokumentów NMF *{Network Management Forum}:*sposób współpracy między modelami informacyjnymi OSI i Internetu.

Model informacyjny TINA-GNMIM jest więc oparty na Zaleceniu ITU-T M.3100 uzupełnionym modelem informacyjnym zarządzania usługami *(Service Management Information Model) oraz* modelem informacyjnym zasobów obliczeniowych *(Computing Resources Information Model).*Specyfikacja modelu informacyjnego zarządzanych zasobów sieci *(Network Resource Information Model) zawiera* wspólne klasy obiektów używanych przez wszystkie usługi i aplikacje zarządzania w sieci konstruowanej zgodnie z koncepcją TINA. Specyfikacja informacji może opisywać różne typy usług, np. usługi związane z publiczną siecią telefoniczną, ISDN, multime-diami i jest ona całkowicie niezależna od niższych poziomów warstw komutacyjnej i transmisyjnej (SDH, ATM).

Zgodnie z hierarchią poziomów zarządzania przejętą z TMN model informacyjny zarządzania składa się z pięciu warstw. W warstwie zarządzania usługą zasoby są opisywane za pomocą grafów połączeń *(Connection Graph),* które określają tryb współpracy obiektów obliczeniowych (graf połączeń logicznych) bądź fizycznych terminali (graf połączeń fizycznych). Warstwa zarządzania siecią i warstwa zarządzania elementem są opisywane przez **model informacyjny zarządzanych zasobów** *(Network Resource Information Model).* Model ten przypomina koncepcję sieci inteligentnej.



Rysunek 53 Architektura zarządzania - model informacyjny

Sieć jest postrzegana jako zbiór punktów (bloków) realizujących konkretne funkcje, przyłączonych do zarządzanych sieci prywatnych i publicznych.

W warstwie wyższej (zarządzanie siecią) są to:

- punkt dostępu użytkownika UAP *(User Access, Point),* punkt dostępu klienta CAP (Customer Access Point),
- sieć wewnętrzna (zakładowa) klienta CPN *(Customer Premises Network),* wirtualny punkt dostępu do sieci publicznej VAP (Virtual Acces Point).

W warstwie niższej (zarządzania elementem) są to:

- punkt dostępu do sieci NAP *(Network Acces Point)* i
- punkty dostępu do urządzeń komutacyjnych, czyli porty komutatorów SAP *(Switch Access Point).* Model funkcjonalny stosowany w architekturze

TINA wykorzystuje te same dziedziny funkcjonalne zarządzania, które spotyka się w modelu OSI oraz w modelu TMN (konfiguracja, wydajność, uszkodzenia, taryfy, bezpieczeństwo).

Dodatkową dziedziną wyodrębnioną w TINA jest dziedzina funkcjonalna zarządzania połączeniami *(Connection Management Functional Area),* w obszarze której definiuje się trzy typy obiektów obliczeniowych:

- CSM *(Communication Session Manager)* - zarządca sesji komunikacji umożliwia zestawienie, utrzymanie i rozłączanie połączeń logicznych interfejsów między obiektami obliczeniowymi, a nie do fizycznych urządzeń sieci);CC *(Connection Coordinator)* - koordynator połączeń jest obiektem obliczeniowym odpowiedzialnym za zestawianie połączeń między punktami końcowymi sieci mającymi swój adres; zawiera on oprócz adresów, również dane dotyczące samego połączenia (np. parametry jakościowe), jednak nie jest związany z samą techniką komutacji ani transmisji;
- CP *(Connection Performer)* - zarządca połączeń zarządza wydzieloną podsiecią oraz umożliwia tworzenie połączeń między punktami końcowymi zarządzanej podsieci; obiekty te są związane z poziomem zarządzania, gdzie są używane oraz z technikami transmisyjną i komutacyjną stosowanymi w zarządzanej sieci.

W architekturze TINA wykorzystano też niektóre doświadczenia NMF *(Network Management Forum)* wprowadzając dodatkowe funkcje zarządzania systemami SMF (Sysrem *Management Function).*Model organizacyjny jest opisem jednostek związanych z zarządzaniem, ich roli, położenia oraz panujących między nimi relacji.

Model komunikacyjny stanowiący opis wymiany informacji między jednostkami zarządzanymi został zaczerpnięty z wcześniej istniejących standardów. W szczególności przejęto następujące modele architektur (architektur rozumianych jako opis struktur zarządzanych jednostek i ich interfejsów):

- z modelu ISO - zarządzanie protokołami, poziomami oraz systemami,
- z zaleceń ITU - model TMN (architektura informacyjna, funkcjonalna i fizyczna, bloki funkcjonalne, punkty odniesienia),
- z dokumentów NMF - model jednostek CME *(Conformant Management Entities),* które mogą współpracować przez interfejs Q3.

Porównanie modelu TMN z architekturą TINA można w uproszczeniu przedstawić:

w architekturze TINA każdy blok funkcjonalny TMN jest przedstawiony za pomocą jednego lub więcej obiektów obliczeniowych, a punkt odniesienia TMN za pomocą jednego lub więcej interfejsów operacyjnych.

Model TINA jest równoważny części modelu (pogrubione linie) modelu TMN. Przykładowy blok OSF (TMN) w architekturze TINA jest modelowany za pomocą dwóch obiektów obliczeniowych C01 i C02. Równoważnikiem punktu odniesienia q3 są dwa interfejsy obliczeniowe łączące dwa bloki przedstawione w prawej części.

Środowisko DPE tworzone w ramach architektury TINA musi mieć następujące cechy:

- umożliwiać wszelkie wzajemne akcje między wszystkimi obiektami TINA-C,
- gwarantować współpracę rozproszonych aplikacji,
- być niezależne od specyficznych ograniczeń poszczególnych systemów komputerowych,
- definiować interfejsy API dla rozproszonych aplikacji,
- upowszechniać wielokrotne używanie *(software reuse)* jednego oprogramowania przez korzystanie z techniki zorientowanej obiektowo (to samo modułowe oprogramowanie może być używane po modyfikacjach w wielu aplikacjach),
- upowszechniać cechę przenośności oprogramowania *(portability),* zapewniać realizację rozproszonych aplikacji telekomunikacyjnych.Podczas tworzenia oprogramowania architektury TINA używa się dwóch narzędzi programistycznych:
- język TINA-C IDL *(Interface Definition Language),* w którym określono m.in. szablony obiektów i interfejsów.
- język TPL (TI-*NA-C Preprocesor Language),* stanowiący rozszerzenie języka C++, gdzie własności języka zorientowanego obiektowo uzupełniono własnościami rozproszenia.

Programy napisane w TPL są oceniane przez preprocesor TPL i podawane jako kod C++. Środowiskiem, w którym jest uruchamiane oprogramowanie jest DPE, umożliwiające współpracę oraz zarządzanie obiektami obliczeniowymi.

W środowisku tym wyróżnia się trzy typy serwerów:

- serwer konfiguracyjny oferujący zbiór usług niezbędnych do zarządzania systemem,
- serwer meldunków umożliwiający obiektom wysyłanie i odbieranie meldunków,
- serwer informacyjny *(trader server),* który administruje informacjami dotyczącymi oferowanych usług i dostępnych interfejsów oraz pełni rolę

mediatora i informatora (podobnie jak żółte strony w książce telefonicznej), zawierającego niezbędne dane do wymiany informacji między dwoma agentami.

Informacje dotyczące zarządzanych zasobów są przechowywane w dwóch typach baz danych *(repository):* w bazach danych specyfikacji *(Specification Repository),* gdzie przechowuje się szablony interfejsów, obiektów, komponentów zapisane w notacji TINA-C IDL, niezbędne do funkcjonowania serwerów konfiguracyjnego i informacyjnego oraz w bazach danych implementacji *(Implementation Repository)* przechowującej informacje związane z implementacją oprogramowania.

Literatura

Publikacje książkowe i periodyczne

1. Andrukiewicz E. -*„Zarządzanie zabezpieczeniem systemu informacyjnego"*, Prace IŁ 108/97
2. E.Bilski, I. Dubielewicz – „Model Odniesienia dla Współdziałania Systemów Otwartych – tom I" , Wydawnictwo Politechniki Wrocławskiej, Wrocław 1991r.
3. E.Bilski, I. Dubielewicz – „Model Odniesienia dla Współdziałania Systemów Otwartych – tom II", ISBN 83-7085-019 -7 Wydawnictwo Politechniki Wrocławskiej, Wrocław 1993r.
4. Bromirski M. Florek J. – „Zarządzanie Sieciami Telekomunikacyjnymi", Instytut Łączności Warszawa – Miedzeszyn, czerwiec 2002 r.
5. Caeli W., Longley D., Shain M.- *"Information Security Handboo"k.* Macmillan Press, Londyn (Wlk. Brytania), 1994
6. Czarnecki P., A.Jajszczyk, J.Lubacz – „Standardy Zarządzania Sieciami – OSI,/NM, TMN" Wydawnictwo EFP, Poznań 1996 r.
7. Gilbert L: - *"Guide for Selecting Automated Risk Analysis Tools."* Special Publication 500-174. Gaithersburg, MD: National Institute for Standards and Technology, October 1989Lubacz J.,
8. Huk R., ZmysłowskI D. - "A Concept of an Integrated System of Military Telecommunications Network Management" RCMCIS, Zegrze 2000.
9. KołodzińskI E., Huk R., Zmysłowski D.:- „Wykorzystanie technologii internetowych w systemach dowodzenia, kierowania i zarządzania. Perspektywy, szanse i zagrożenia" . IX Konferencja naukowa „Automatyzacja Dowodzenia", Jurata 2001.
10. Krull A. R.: - "GSSP *(Generally Accepted System System Security Principles): A Trip to Abilane?* "Computers & Security, Vol. 15 No. 7, 1996
11. Ostrowski P. – „Model Przestrzeni Zarządzania Telekomunikacyjnego Przedsiębiorstwa Operatorskiego" – Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne
12. Ozier W.: -"Issues *in Quantitive Versus Qualitative Risk Analysis"*. DataPro 6055, McGraw-Hill, Inc, March, 1994
13. Pavlou G.– "Telecommunications Management Network – A Novel Approach Towards its Architecture and Realisation Through Object-Oriented Software Platforms", University College London 1998 r.
14. Raman L.G. – "Fundamentals of Telecommunications Network Management", ISBN 0-7803-3466-3, IEEE Press, New York 1999 r.
15. Udupa D. K. – "TMN – Telecommunications Management Network", ISBN 0-07-065815-3, McGrawHill –2000-r.
16. Szczypiorski K. "Ochrona informacji w zarządzaniu sieciami telekomunikacyjnymi" KST, Bydgoszcz 1998 r.
17. Zmysłowski D. - „The Concept of a Simulation Model of a Computer System of Assisting a Local Network of the Military Communications Centre" RCMCIS, Zegrze 2000.
18. Zmysłowski D. - „Technologie programowe w zarządzaniu systemami telekomunikacyjnymi" Instytut Łączności Warszawa – Miedzeszyn, czerwiec 2002 r.

Normy i inne akty prawne

19. BS 7799 : 1995 *Code of Practice for Information Security Management.* BSI, 1995
20. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and free movement of such data
21. Ustawa z dn. 29 sierpnia 1997r. o ochronie danych osobowych, Dz. U. Nr 133, poz. 883
22. Ustawa o ochronie informacji niejawnych – Dz. U. Nr.11, poz 95 z dnia 22 stycznia 1999 rRozporządzenie Prezesa Rady Ministrów w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych - Dz. U. Nr. 18, 162 z dnia 25 lutego 1999 r.PN-T-20001-2:1992 (PN-92/T-2001/02) Systemy przetwarzania informacji – Współdziałanie systemów otwartych (OSI) – Podstawowy Model Odniesienia – Architektura zabezpieczeń.
25. PN-I-02000: 1998 Technika informatyczna - Zabezpieczenia w systemach informatycznych - Terminologia.
26. PN-ISO 9160:1997 Przetwarzanie informacji – Szyfrowanie danych – Wymagania dotyczące współpracy w warstwie fizycznej.
27. PN-ISO/IEC 9796-1:1997 Technika informatyczna – Techniki zabezpieczeń – Schemat podpisu cyfrowego z odtwarzaniem wiadomości.
28. PN-ISO/IEC 9797:1996 Technika informatyczna – Techniki zabezpieczeń – Mechanizm integralności danych wykorzystujący kryptograficzną funkcję kontroli z algorytmem szyfrowania blokowego.

29. PN-ISO/IEC 9798-3:1996 Technika informatyczna – Techniki zabezpieczeń – Mechanizmy uwierzytelniania podmiotów – Uwierzytelnianie podmiotów z wykorzystaniem algorytmu klucza publicznego..
30. ISO/IEC TR 13335-1 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych - Pojęcia i modele bezpieczeństwa systemów informatycznych.
31. ISO/IEC TR 13335-2 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Zarządzanie i planowanie zabezpieczeń systemów.
32. ISO/IEC TR 13335-4 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Wytyczne podstawowe.
33. ISO/IEC TR 13335-5 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Zastosowanie usług i mechanizmów zabezpieczania systemów.
34. ISO/IEC 15408-3 Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczania systemów – Zapewnienie jakości systemów, produktów i komponentów.
35. ISO 7498
36. ITU – T zalecenia serii M.
37. IAB – RFC
38. Dokumentacja programu RACE

Dokumentacja firmowa

38. AIX NetView/6000", Networld styczeń 1995
39. "Bringing out the big guns", – Product Comparison: LanTimes – October 1998 r.
40. "Unicenter TNG – zarządzanie scentralizowane", Integrator nr 3-4 1999 r.
41. 3Com, *3Com Transcend - Transcend Network Management and Control Solutions* - Data Sheet
42. 3Com, *Transcend Management Software Transcend Central* - User Guide
43. 3Com, *Transcend Enterprise Manager* Release Notes
44. 3Com, *Transcend Management Software ATM and VLAN Management* - User Guide
45. **3Com, *Transcend Management Software Device View* - User Guide**
46. 3Com, *Transcend Management Software LANsentry* - Manager User Guide
47. 3Com, *Transcend Management Software Status View* - User Guide
48. 3Com, *Transcend Management Software* - Getting Started Guide
49. 3Com, *Transcend WorkGroup Manager* - Release Notes
50. Bronisław Piwowar, *Zintegrowane zarządzanie siecią komputerową Transcend,* Networld grudzień 1994
51. Computer Associates, *Unicenter TNG Total Enterprise Management* – Product Overview
52. Data Sheet - Cisco Info Center;
53. Data Sheet – Cisco IP Manager;
54. Data Sheet - Cisco Provisioning Center
55. Data Sheet - Cisco Service Management System;
56. Data Sheet - Cisco WAN Manager;
57. Data Sheet – Cisco WAN Service Administrator;
58. Data Sheet - Data Sheet -Cisco Netsys Connectivity Service Manager;
59. Data Sheet -Cisco Netsys Connectivity Service Manager;
60. Digital, *ClearVISN VLAN Manager* - Software Product Description
61. Digital, *ClearVISN* - Product Overview June 1996
62. IBM, *IBM Nways Manager for AIX* – Product Overview
63. IBM, *IBM Nways Manager for HP-UX*– Product Overview
64. IBM, *IBM Nways RouteSwitch Network Management Suite* – Product Overview
65. IBM: *IBM Nways Workgroup Manager for Windows NT* – Product Overview
66. Internet – www.cisco.com;
67. Internet – www.hp.com
68. Internet - www.sun.com
69. Internet: www.3com.com
70. Internet: www.alantec.com
71. Internet: www.cai.com.
72. Internet: www.digital.com
73. Internet: www.ibm.com
74. Internet: www.olicom.com
75. Olicom, *CLEARSIGHT Network Management System* – Product Overview
76. Olicom, *OLICOM SNMP APPLICATIONS* – Product Overvew
77. Product brief Hp openview Netmetrix site manager for Windows NT;
78. Product overview Solstice Enterprise Manager 3.0
79. Quick Start Guide HP NetMetrix/UX version 5.0

80. User Guide - User's Guide, Volume 2 HP NetMetrix/UX version 5.0;
81. White Paper - Cisco Internetwork Management – Information of products;
82. White paper - Managing Your Network with HP OpenView Network Node Manager;
83. White paper – Solstice Site Manager Solstice Domain Manager v 2.3
84. White paper - SolsticeEnterprise Manager 2.1