Naukowa i Akademicka Sieć Komputerowa

oraz

Telekomunikacja Polska S.A.

Materiały seminarium

MIEDZESZYN '96

Część I

22-24 maja 1996 r.

Naukowa i Akademicka Sieć Komputerowa

oraz

Telekomunikacja Polska S.A.

Materiały seminarium

MIEDZESZYN '96

Część I

22-24 maja 1996 r.

Rada Programowa:

Roman Adamiec
Maria Baranowska
Wojciech Hałka
Tomasz Hofmokl
Jarosław Kępkowicz
Maciej Kocięcki
Maciej Kozłowski (Przewodniczący)
Wiktor Krzanowski
Krzysztof Trzewik
Józef Zalewski

Prowadzący Seminarium:

Andrzej Zienkiewicz

Wstęp

Szóste z kolei seminarium NASK w Miedzeszynie już po raz drugi jest organizowane wspólnie z TP SA. W ciągu roku, który upłynął od poprzedniego seminarium, w polskich sieciach komputerowych nastąpiło wiele zmian. Warto wymienić kilka z nich:

- *NASK prawie dwukrotnie zwiększył liczbę węzłów na terenie całego kraju, docierając do mniejszych ośrodków.*
- *Liczba klientów NASK wzrosła blisko dwukrotnie, a ilość przesyłanych danych zwiększyła się dwunastokrotnie; wymusiło to zwiększenie przepustowości dzierżawionych przez NASK linii międzynarodowych do 5.5 Mbps.*
- *W sieci NASK powstała rozwinięta struktura węzłów Frame Relay, umożliwiająca tworzenie i eksploatację wydzielonych sieci korporacyjnych.*
- *Miejskie sieci komputerowe stopniowo otrzymują zezwolenia i koncesje telekomunikacyjne.*
- *Powstała ogólnopolska sieć do przesyłania danych Polpak-T. Telekomunikacja Polska SA zapowiedziała udostępnienie Internetu swoim abonentom.*
- *Rozpoczęło działalność kilkadziesiąt firm, specjalizujących się w internetowych usługach informacyjnych i dołączeniowych.*
- *Następuje intensywna komercjalizacja Internetu w Polsce.*

Rozwój polskiego Internetu nadal jest związany z wieloma dylematami, wśród których na pierwszy plan wysuwają się organizacyjne i ekonomiczne aspekty budowy sieci komputerowych oraz problemy bezpieczeństwa sieci i ochrony informacji. Zagadnieniom tym poświęcamy szczególnie wiele miejsca, zarówno w aspektach technicznych jak i prawnych.

Na tegorocznym seminarium nie zabraknie również nowych propozycji technicznych, a wśród nich zagadnień wykorzystania sieci telewizji kablowej jako multimedialnego środowiska dostępowego. Wreszcie, zgodnie z ugruntowaną tradycją, "Miedzeszyn" jest okazją do szerokiej wymiany poglądów i doświadczeń we wszystkich kwestiach nurtujących środowiska operatorów i użytkowników sieci komputerowych w Polsce.

Spis treści

Część I

Część II

RYNEK USŁUG INTERNETOWYCH W POLSCE

Andrzej Błaszczyk, Sławomir Dobaczewski, Maria Miller

UnivNet Sp. z o. o., Wałbrzyska 3/5, 02-739 Warszawa

1. Światowy i polski rynek usług internetowych

Analiza rynku brytyjskiego przeprowadzona przez IRB International wykazała, że w 1996 r. liczba angielskich użytkowników Internetu powinna podwoić się osiągając pod koniec roku wartość trzech milionów. Nie ma powodów przypuszczać, że w Polsce nie wystąpi podobna tendencja rosnąca, pomimo negatywnych uwarunkowań, o których niżej.

W okresie ostatniego półrocza samoistnie pojawiła się w polskich mediach agresywna reklama rozległej sieci komputerowej Internet. Stan ten przypomina okres intensywnej propagandy najpierw zastosowań informatyki, a następnie użyteczności komputerów osobistych. Aczkolwiek wówczas ani zastosowania informatyki, ani wreszcie zakup mikrokomputera typu PC niczego nie stanowił poza nieuzasadnionym wydatkiem, to po kilku latach pojawiły się rzeczywiste implementacje bez których obecnie nie można sobie wyobrazić funkcjonowania państwa w skali mikro i makro.

Podobnie jak wówczas, kiedy o nowoczesności organizacji świadczyło wyposażenie w techniczne środki informatyki, tak i teraz połączenie komputerowej instalacji lokalnej z siecią Internet albo pakietową siecią X.25 stanowi o randze i rozwoju firmy. Większość organizacji nie potrafi wykorzystać możliwości wynikających z usług wymienionych sieci, jednak jest przekonana o celowości przeznaczenia pewnych środków na dołączenie się do nich.

Wobec światowego rozwoju społeczeństw informatycznych stanowimy zacofaną enklawę, w której mniejszość populacji potrafi korzystać ze światowych zasobów informacyjnych, zaś świat tylko w małym stopniu ma dostęp do zasobów polskich. Ta luka zaczyna się powoli wypełniać. Trwająca reklama Internetu wywołała podaż pewnej liczby usługodawców oferujących połączenie do komputerowej sieci rozległej, najczęściej na niedostatecznym poziomie technicznym, za to po niewielkiej cenie.

Rozwój rynku usług internetowych w Polsce datuje się od niedawna. Przed rokiem 1995 polski Internet był niemal wyłącznie domeną naukowo-akademicką.

Rozwój rozległej sieci komputerowej determinujący postęp cywilizacyjny w kierunku społeczeństwa informacyjnego wymaga znacznych nakładów inwestycyjnych i nigdzie nie nastąpił bez ingerencji państwa.

W Polsce rolę państwowego sponsora spełnił w przeszłości KBN inicjując poprzez NASK przemiany kulturotwórcze, których nie sposób przecenić, ponieważ zapoczątkowane zostały w środowisku młodej i najbardziej wykształconej części populacji. Wydaje się, że ten okres mamy już za sobą i ani parlament, ani rząd nie uświadamiają sobie szkód, które nastąpią w ciągu 2-3 lat wobec praktykowania tezy, że nadszedł czas na całkowite samofinansowanie się rozległej sieci komputerowej. Na takie poglądy mogą sobie pozwolić społeczeństwa o istniejącym znacznym stopniu upowszechnienia korzystania z sieci, w których to społeczeństwach operator i usługodawca mogą liczyć na klientelę zapewniającą rentowność ich działalności. Ten stan jest jeszcze przed nami.

Obecnie działa na rynku czterdziestu kilku usługodawców; dalszych kilkanaście firm jest zainteresowanych świadczeniem usług internetowych.

Liczba linii telefonicznych do dyspozycji klientów jest jednym z istotnych parametrów oceny usługodawcy. Standardy zagranicznych usługodawców zakładają, że stosunek liczby użytkowników na jedną linię telefoniczną powinien wynosić 10.

Przyjmuje się zwykle, że stosunek ten jeśli jest nie większy niż 20, umożliwia on klientowi skorzystanie z usług również w porach większego obciążenia. Tylko kilku polskich usługodawców dysponuje równą lub większą niż 50 liczbą linii komutowanych, jednak biorąc pod uwagę niewielką na razie liczbę klientów można uznać, że w większości firm liczba użytkowników na 1 linię nie przekracza 20. Jednak w niedalekim czasie sytuacja ta może ulec zdecydowanej zmianie. Jak dotychczas wszędzie na świecie liczba użytkowników wzrastała lawinowo i tendencja ta powinna utrzymać się dalej.

Zdecydowana większość usługodawców działa na terenie Warszawy oraz w większych aglomeracjach takich jak Kraków, Łódź, Wrocław czy Gdańsk ale pojawiają się też (firmy czy też ich filie) w mniejszych miastach takich jak Cieszyn czy Łowicz.

Internet ma w Polsce wielu sympatyków i być może stanie się niedługo usługą tak zwykłą jak telefon jeśli pokonane zostaną systemowe ograniczenia na poziomie państwa. Na razie jednak większość usługodawców dopiero rozpoczyna działalność i tylko najwięksi mają powyżej 300 klientów, większość około 100, przy czym tylko u kilku usługodawców procent klientów prywatnych stanowi więcej niż 50. Niektórych czeka zawód z powodu niespełnionych nadziei na sukces ekonomiczny.

2. Usługi internetowe, a usługi bazodanowe

Sieciowych baz danych udostępnianych przez polskich usługodawców jest na razie niewiele, a wydaje się, że usługa ta może zadecydować w przyszłosci o powodzeniu firmy jak równiez o rozwoju sieci. Billy Gates, szef Microsoftu w swoim artykule opublikowanym w Asia Week porównał eksplozję zainteresowania Internetem do amerykańskiej Gorączki Złota z 1849 roku. Gates uważa, że łatwiej będzie odnieść sukces finansowy zajmując się rozpowszechnianiem informacji poprzez sieć niż wytwarzając urządzenia niezbędne do obsługi sieci. Zdecydowaną uwagę Gates zwraca na reklamę, która nie dość, że może być interaktywna, co otwiera przed producentami reklamy niespotykane dotąd możliwości, to jeszcze umożliwia łatwe sprawdzenie popularności i swojej pozycji na rynku.

Firmy wykorzystujące do przekazywania informacji handlowych usługę Internetu mogą stać się konkurencją dla central handlowych, a nawet targów międzynarodowych. Taką działalność prowadzi w Polsce od marca międzynarodowa sieć handlowa Internet Tradeline. Oprócz niej działa jeszcze kilka serwisów wymiany informacji handlowej - takie jak Barter Net czy Commerce-Net. Przedstawiciele Tradeline twierdzą, że dostępność jej usług na naszym rynku będzie miała wielkie znaczenie dla wielu średnich i małych polskich firm, gdyż otworzy im drogę do niedostępnego do tej pory rynku międzynarodowego.

3. Rynek operatorów sieci szkieletowych

Operatorów sieci szkieletowych w Polsce jest niewielu. Ich polityka cenowa ogranicza rozwój ekspansji sieci do mniejszych ośrodków w kraju; są w kraju miejscowości, w których dostawcy usług mogliby rozpocząć działalność, lecz zbyt wysokie koszty dzierżawy łączy stałych uniemożliwiają takie przedsięwzięcia. W tym przypadku należy również pamiętać o faktycznym monopolu TPSA będącej głównym dostawcą łączy telekomunikacyjnych. Wydaje się, że najlepszym rozwiązaniem byłoby zwiększenie liczby lokalnych dostawców usług, związanych z danym obszarem kraju i odejście operatorów sieci szkieletowych od świadczenia usług odbiorcom prywatnym (indywidualnym) oraz przeniesienie zainteresowania na mniejszych operatorów sieci, jeśli się pojawią.

Jak wszystkim dobrze wiadomo potentatem wśród operatorów sieci szkieletowych, ale i usługodawcą jest NASK, który - czego wielu sobie nie uświadamia - jest głównie organizatorem budowy i eksploatacji węzłów sieci; natomiast głównym stymulatorem cen jest dostawca łączy czyli TPSA. Jedynym, który mógłby obecnie zmienić ten stan rzeczy jest BPT TELBANK, ale tylko w zakresie łączy międzymiastowych. Jednak wobec braku oferty łączy dostępowych i wysokich cen nie może być konkurencyjny. Pewne nadzieje może budzić rozwój sieci linii światłowodowych TELENERGO w zakresie łączy międzymiastowych i możliwości telefonii GSM oraz telewizji kablowej w zakresie problemów sieci dostępowej.

Od niedawna można zauważyć, że jest przełamywany monopol na szybkie łącza do sieci rozległej Internet w ruchu międzynarodowym. Pojawiają się dostawcy usług oferujący, oprócz dostępu do sieci Internet poprzez łącza NASKu lub do sieci MAN, również wejście przy wykorzystaniu własnych łączy satelitarnych. Takich dostawców usług można niewątpliwie uznać za operatorów części sieci szkieletowej w związku z oferowaniem własnych łączy innym usługodawcom. Jest to początek korzystnej konkurencji na rynku operatorów sieci szkieletowej.

Wszystko, co powiedziano powyżej jest dalekie od nadziei na pojawienie się mechanizmów rynkowych wśród operatorów sieci szkieletowej.

4. Rynek dostawców usług

Poziom usług oferowanych przez usługodawców jest dość zróżnicowany.
Oceniając usługodawcę ze względu na jakość usług można się posłużyć takimi kryteriami jak: legalność działań usługodawcy, rodzaj i jakość sprzętu, typ zainstalowanych modemów, przepustowość łącza do sieci szkieletowej, rodzaj stosowanych łączy telefonicznych, liczba linii telefonicznych dla klientów, system bezpieczeństwa, dostęp do lokalnych baz danych, ceny oferowanych usług, opieka nad klientem.

Po wejściu w życie znowelizowanej ustawy o łączności uznającej Internet za sieć telekomunikacyjną, większość działań usługowych w Internecie wymaga uzyskania koncesji. Obecnie tylko kilkunastu usługodawców posiada zezwolenie Ministra Łączności (są też firmy, które posiadają licencję ale nie prowadzą jeszcze działalności w tym zakresie), większość złożyła wniosek o rejestrację i czeka na decyzję. Część firm działa w tej sytuacji na pograniczu prawa.

Dla wielu klientów ważna jest jakość połączenia ze światem. Do tej pory wszyscy usługodawcy korzystali z wyjścia na świat poprzez łącza NASKu (linia satelitarna 2 Mbps do Sztokholmu i linia naziemna 256 Kbps do Wiednia). Niestety od dłuższego czasu łącza te są mocno przeciążone. Sytuacja ta może się niedługo zmienić w związku z pojawieniem się firm, korzystających z niezależnych łącz miedzynarodowych (Sprint, SatNet i TPSA).

Duże zróżnicowanie występuje w oferowanych usługach i cenach. Usługodawcy stosują różne strategie, wprowadzają limity czasowe, limity dyskowe, oferują kilka różnych rodzajów dostępu, inne stawki dla firm, inne dla użytkowników indywidualnych. Kilku stosuje rozliczenie za ruch co związane jest z nowym cennikiem NASKu. Generalnie można jednak stwierdzić, że potencjalny klient ma możliwość wyboru i znalezienia tańszej oferty.

Szczególnie duże zróżnicowanie cen wiąże się z usługą www. Jest to w tej chwili usługa najbardziej atrakcyjna dla klientów i 'napędzająca' popyt na Internet. Niektóre ceny za samo utrzymywanie stron www wydają się zadziwiająco wysokie. Większość usługodawców oferuje możliwość umieszczenia własnej strony www czy też reklamę w ich stronach, natomiast niewielu usługodawców oferuje usługę graficznego opracowania wyglądu stron www.

Jedną z usług internetowych mało na razie wykorzystywaną przez polskich usługodawców są wirtualne sklepy, chociaż są już przykłady udostępniania tej usługi również w naszym kraju. Np. w

sieci Polska Online dostepny jest wirtualny sklep wydawnictwa Gutenberg-Print. W Krakowie duży sklep wirtualny uruchomiła Główna Księgarnia Naukowa, oferująca ok. 15 tys. pozycji.

Nowością na polskim rynku są też tzw. 'kawiarnie internetowe', czyli ogólnie dostępne lokale, wyposażone w terminale z dostępem do sieci, w których za niewielką opłatą (rzędu kilku zł za godzinę) każdy może skorzystać z usług internetowych w podstawowym zakresie, bez konieczności inwestowania we własny sprzęt, opłat abonamentowych itp.

W najbliższym czasie Telekomunikacja Polska S.A. uruchamia ogólnopolską sieć komputerową, która zapoczątkuje polską infostradę.

Węzły sieci TPSA znajdą się we wszystkich miastach wojewódzkich w Polsce. Na ten sam numer można będzie dzwonić w całym kraju. Przez pierwsze 3 miesiące można będzie wejść do Internetu za darmo, abonent będzie tylko płacił normalną stawkę za czas połaczenia telefonicznego. Po trzech miesiącach planowana jest opłata 'symboliczna' za dostęp do Internetu. TPSA na razie nie przewiduje prowadzenia bardziej rozwiniętych usług w rodzaju sprzedaży kont czy informacji, które to usługi dostarczane są przez internetowych usługodawców. Abonenci będą mogli oglądać strony www, korzystać z gopherów, baz danych, ale nie będą mogli np. wysłać poczty. W przyszłości jednak, kiedy TPSA rozwinie usługi może stać się konkurencją dla dzisiejszych czołowych usługodawców. Już teraz może to spowodować, że nieopłacalne stanie się dla usługodawców inwestowanie w urządzenia dostępowe, gdyż potencjalni abonenci będą mogli bez problemów wejść do sieci korzystając z usług TPSA.

Na opisanym przykładzie szczególnie jaskrawo widać groźną tendencję powszechnie występującą u operatorów sieci szkieletowej i firm, dla których głównym źródłem dochodu nie jest usługodawstwo w sieci Internet. Usługodawstwo stanowi dla nich działalność peryferyjną. Typowy usługodawca w sieci Internet stoi przed koniecznością znacznych inwestycji, opłaca szybko rosnące koszty dostępu do sieci szkieletowej, obserwuje wolno rosnący nabór klienteli - przy stabilizacji na rynku cen na usługi, które sam świadczy. Poziom tych cen ustalany jest poniżej kosztu przez firmy, które utrzymują się z innych źródeł. Jest to niezgodne z prawem w zakresie praktykowania nieuczciwej konkurecji.

Widać też wzrastające zainteresowanie rynkiem usług Internetowych ze strony dużych firm komputerowych w rodzaju Microsoft czy Optimus, które też zapewne będą się lokowały na rynku według opisanego wyżej scenariusza.

Rodzaj sprzętu u usługodawców jest dość zróżnicowany. Jako serwery wykorzystuje się zarówno komputery PC, jak i Sun (SPARC) a także VAX.

Wśród stosowanych ruterów zdecydowanie przeważa CISCO. Jeśli chodzi o modemy dla klientów to większość firm poleca modemy w standardzie V.34.

Problemy związane z liczbą linii telefonicznych a raczej z ich brakiem zależą oczywiście od umowy usługodawcy z TPSA. Ci dostawcy, którzy dysponują światłowodem są oczywiście w lepszej sytuacji, jednakże jest ich niewielu, dosłownie kilku.

Zdecydowanie ważnym kryterium określającym usługodawcę jest przepustowość łącza jakim usługodawca jest podłączony do sieci szkieletowej. Istotne jest przy tym faktyczne obciążenie sieci. Kilkunastu usługodawców podłaczonych jest do operatora z prędkością większą niż 64 kbps, przy czym są i tacy którzy podłączeni są z prędkości 2 Mbps a nawet 10 Mbps. Są też jednak i takie firmy, które podłączone są z prędkościa mniejszą niż 64 kbps.

Z pomiarów efektywnej przepustowości wynika, że efektywną przepustowość powyżej 64 kbps osiąga ok 1/3 usługodawców, natomiast ok. połowy nie osiąga przepustowości (efektywnej) powyżej 30 kbps, co w praktyce uniemożliwia klientom pełne korzystanie z usług Internetowych.

5. Próba oceny technicznej jakości usług

Z przeprowadzonego badania efektywności łączy, zobrazowanego wykresami: ***Efektywna przepustowość łącza, Podział dostawców wg. efektywnej przepustowości łącza do sieci szkieletowej***, zauważalny jest pewien podział dostawców.

Badanie efektywności przepustowości łączy przeprowadzono stosując komendę ping i porównując czas przesłania pakietów o rozmiarach 56 bajtów i 560 bajtów. Pomiary uśredniono dla 10 pakietów w trzech wybranych porach roboczego dnia marca br. tzn. w godzinach: 8-10, 12-16, 19-21. Wymienione pory dnia wybrano ze względu na przewidywane wyższe obciążenie łączy w godzinach 12-16 i niższe w godzinach porannych i wieczornych.

Badanie było kompletne i objęło 43 providerów, a wyniki uporządkowano wg wielkości efektywnej przepustowości poczynając od najmniejszej do największej. Efektywna przepustowość została wyliczona wg wzoru: $8[kb]/(t_{560}-t_{56})[s]$. Pomiary wyprowadzono z komputera skalar.univ.waw.pl. W związku z tym wyniki limitowane są przepustowością linii UnivNet-WARMAN - 128 kb/s. Dostawcy usług Internetowych zazwyczaj zapewniają prędkość dostępowa dla klienta 14,4-28,8 kbps, a więc przepustowość łącza pomiędzy usługodawcą a siecią WAN powinna dla zapewnienia komfortu pracy użytkownika wynosić co najmniej 64 kb/sek. Jak widać ok. 40% dostawców usług Internetowych nie osiąga tej granicy. Niskie pozycje niektórych firm w omawianej tabeli mogą częściowo wynikać z ich odległej od Warszawy lokalizacji. Jednocześnie wyniki wskazują na to, że łącza pomiędzy głównymi usługodawcami a NASK nie są przeciążone. Należy jednak przy tym pamiętać, że nie dotyczy to łączy wyjściowych z Polski na świat.

Wykres - ***Podział dostawców wg. średniego czasu odpowiedzi na krótkie pakiety ping*** - zawiera czasy odpowiedzi poszczególnych komputerów na krótkie pakiety ping (56 bajtów), uśrednione z 10 pakietów przesyłanych w 3 różnych porach dniach. Wyniki zostały uporządkowane wg uśrednionego czasu odpowiedzi w kolejności od najmniejszego do największego. Krótsze czasy świadczą o możliwości lepszej zdalnej pracy w trybie interakcyjnym dla użytkownika (im krótszy czas tym system znajduje się 'bliżej'). Oczywiście należy pamiętać, że dalsze pozycje niektórych firm pozawarszawskich wynikają z ich lokalizacji.

Pomiary transmisji FTP przeprowadzono w dzień powszedni z hosta na Politechnice Warszawskiej. Transmisję przeprowadzono w trzech różnych porach dnia na 6 jednakowych plikach. Otrzymane wyniki, które są średnią arytmetyczną sześciu pomiarów cząstkowych przedstawione zostały na wykresie: ***Dostawcy usług w sieci Internet w podziale wg. uzyskanych prędkości transmisji ftp***. Pomiary objęły tych dostawców usług w sieci Internet, którzy udostępniają anonimowe konto FTP (27). Na podstawie uzyskanych prędkości transmisji daje się zauważyć naturalny podział dostawców na trzy grupy ze względu na prędkość transmisji FTP: do 10 kB/s, od 10 -40 kB/s, powyżej 40 kB/s. Wyniki wskazują na to, że ponad 50 % dostawców nie osiąga prędkości transmisji powyżej 10 kB/s.

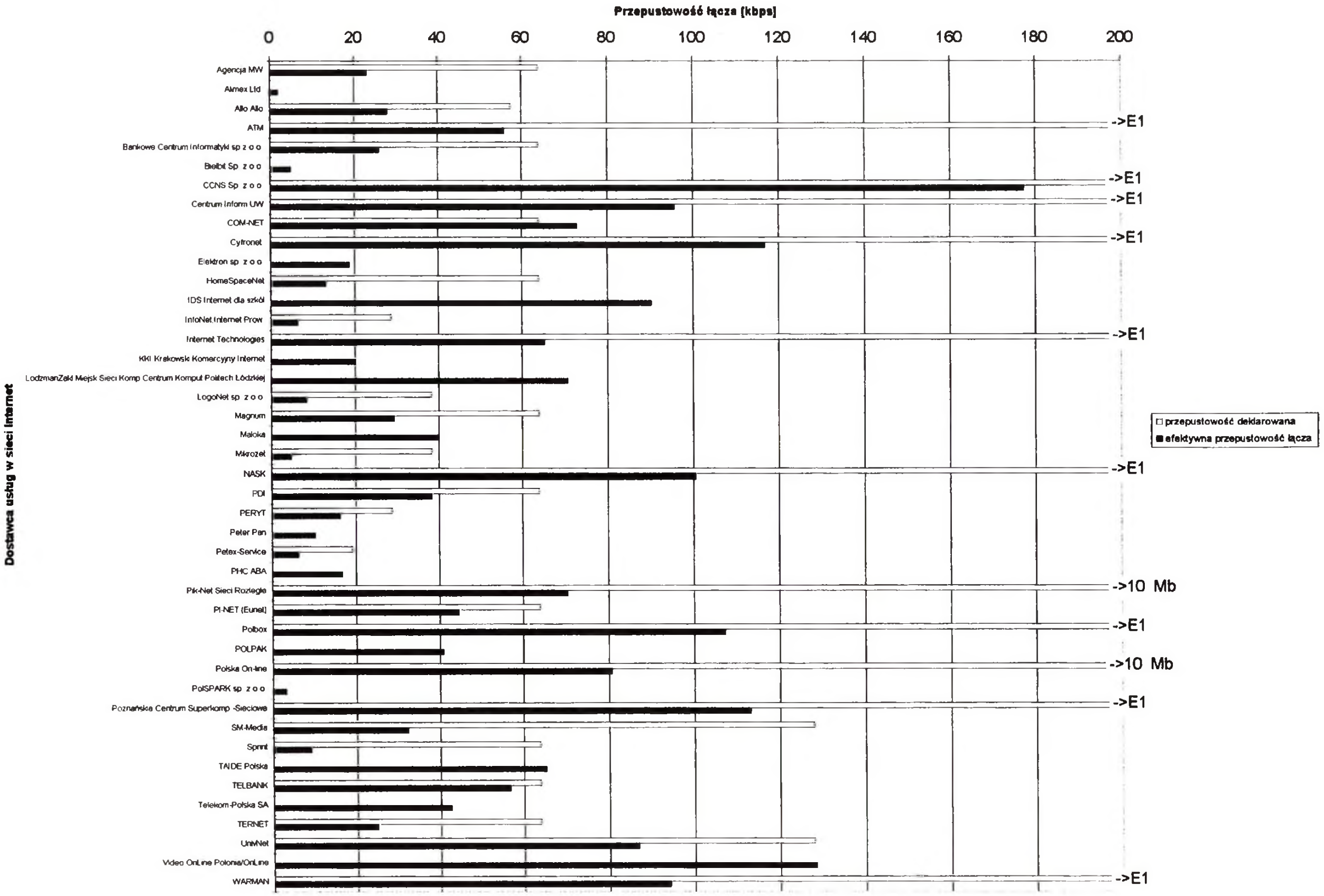
6. Odbiorcy usług

Idąc za czasopismem iWAY Magazine (march 1996), dostęp do sieci Internet można porównać do odkrywania tajemnic natury, tym samym można ją badać na różne sposoby:

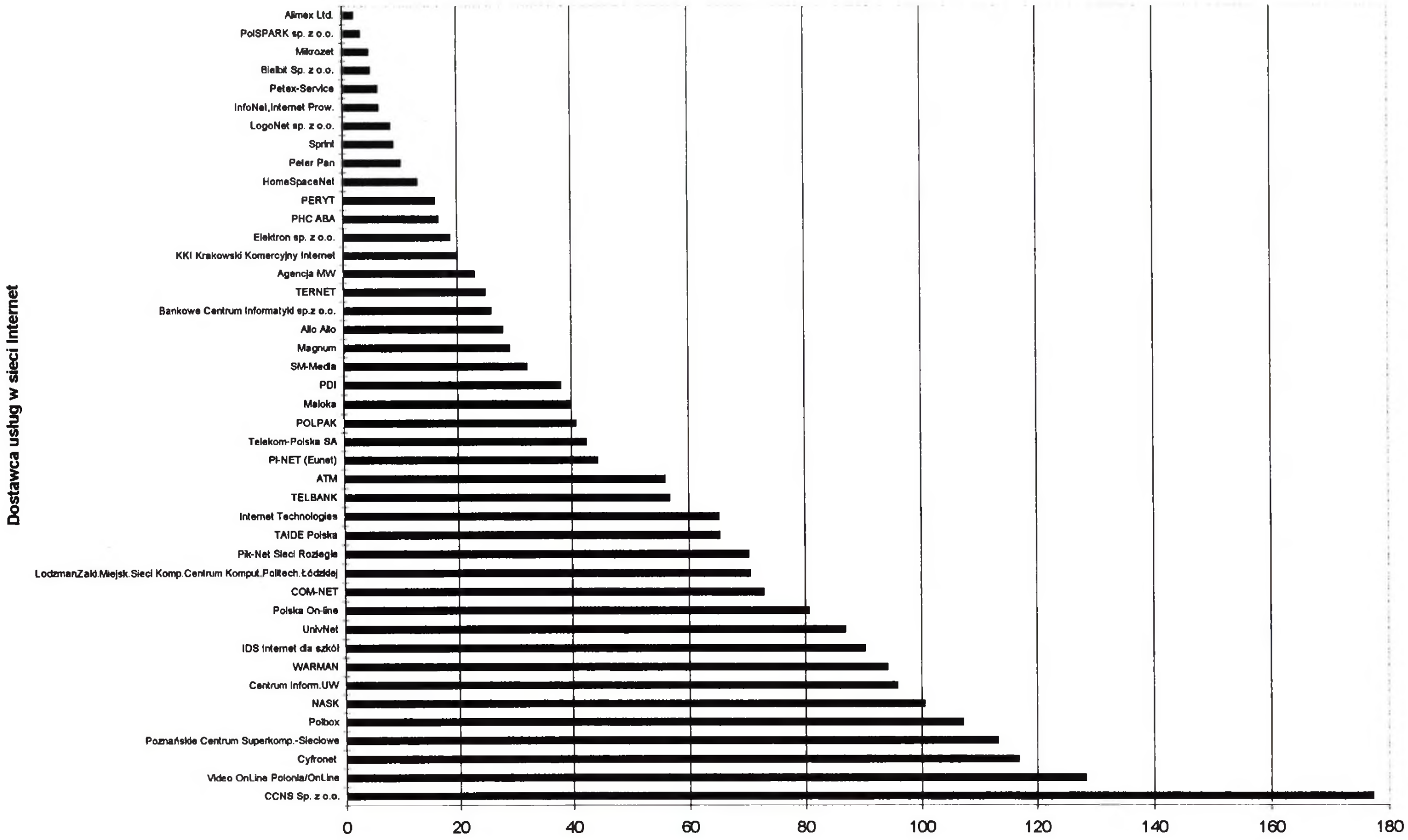
1) odwiedzić ogród zoologiczny;
2) wybrać się na safari w towarzystwie profesjonalnego przewodnika;
3) wylądować na spadochronie w środku dżungli i mieć przy sobie jedynie nóż

W Polsce mamy do czynienia raczej z tym ostatnim przypadkiem - klient często otrzymuje jakieś konto, a dalej musi się sam troszczyć o resztę, pomoc ze strony usługodawcy jest niezwykle kosztowna. Szkolenia są drogie - ok. 30-50 zł za godzinę, w związku z czym raczej niedostepne dla odbiorców indywidualnych. Niewielu krajowych dostawców wręcza klientowi specjalny pakiet

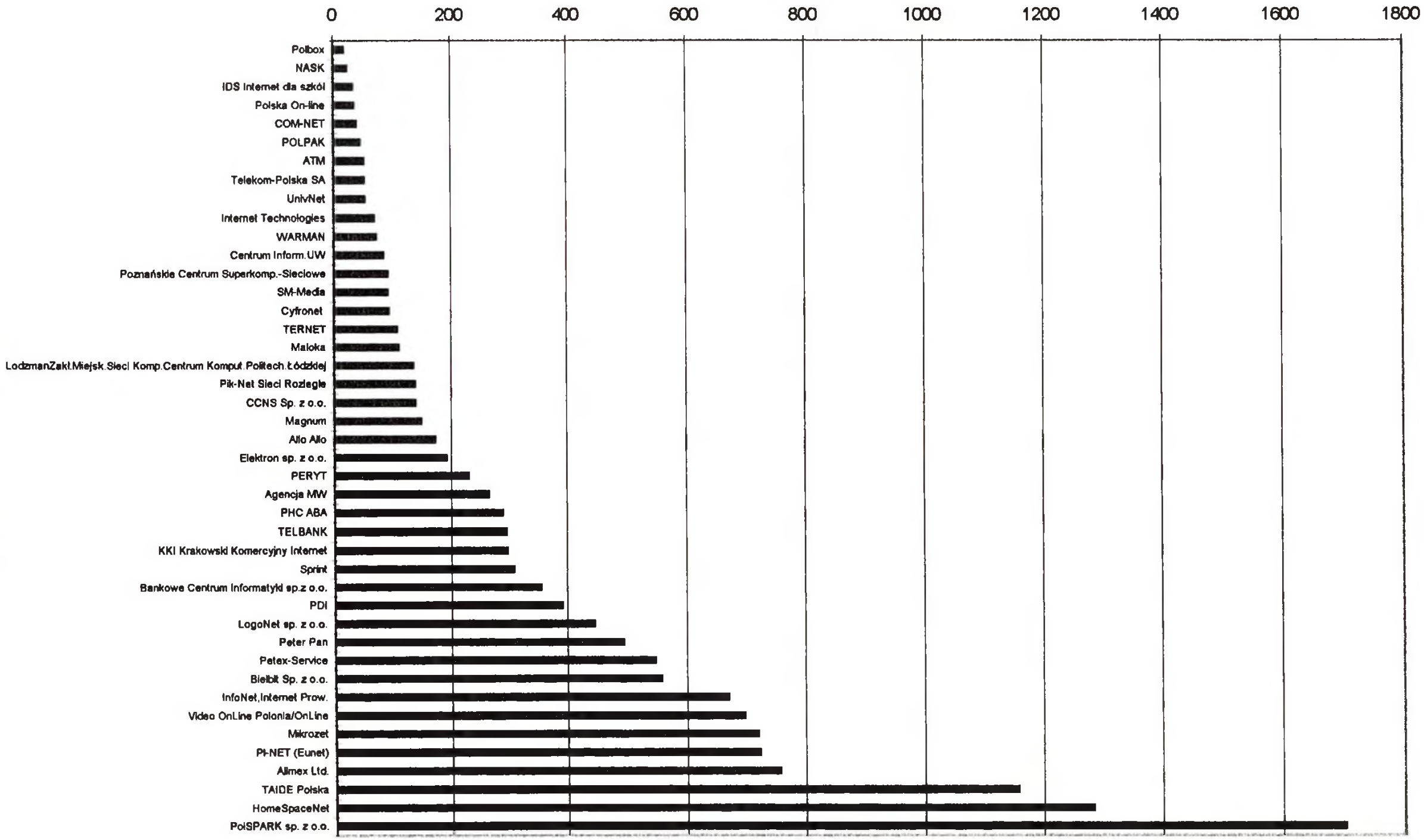
Efektywna przepustowość łącza (wykres liniowy)

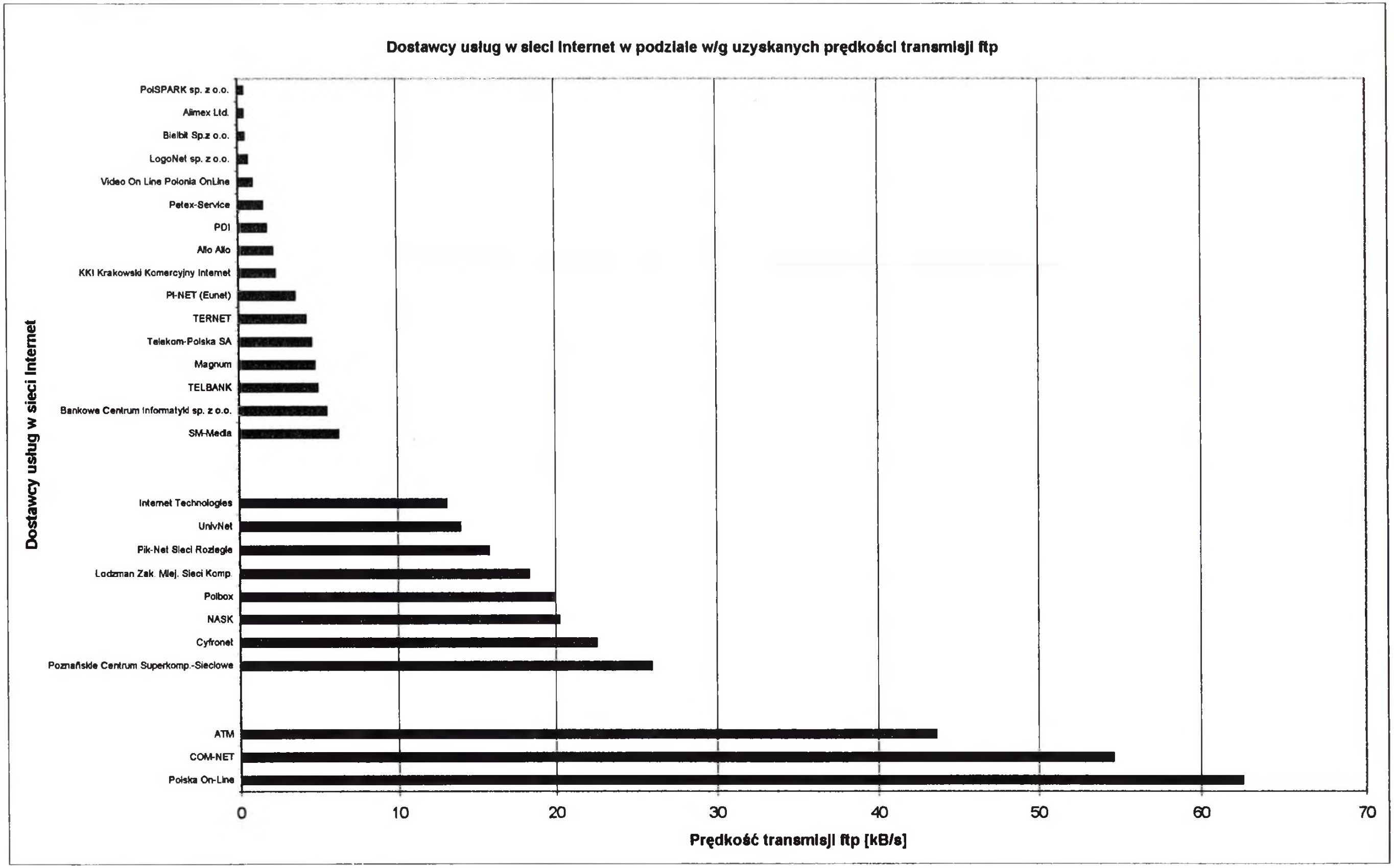


Podział dostawców wg. efektywnej przepustowości łącza do sieci szkieletowej



Podział dostawców wg. średniego czasu odpowiedzi na krótkie pakiety ping (56 bajtów)
czas [ms] (uśredniony z 3 pomiarów)




Dostawcy usług w sieci Internet w podziale w/g uzyskanych prędkości transmisji ftp
PolSPARK sp. z o.o.
Alimex Ltd.
Bielbit Sp.z o.o.
LogoNet sp. z o.o.
Video On Line Polonia OnLine
Petex-Service
PDI
Allo Allo
KKI Krakowski Komercyjny Internet
PI-NET (Eunet)
TERNET
Telekom-Polska SA
Magnum
TELBANK
Bankowe Centrum Informatyki sp. z o.o.
SM-Media
Internet Technologies
UnivNet
Pik-Net Sieci Rozlegle
Lodzman Zak. Miej. Sieci Komp.
Polbox
NASK
Cyfronet
Poznańskie Centrum Superkomp.-Sieciowe
ATM
COM-NET
Polska On-Line
Dostawcy usług w sieci Internet
0
10
20
30
40
50
60
70
Prędkość transmisji ftp [kB/s]

oprogramowania służący do podróżowania po stronach www czy też pomoc przy konfiguracji oprogramowania takiego jak Trumpet Winsock czy Netscape, a nie są to pakiety z którymi da sobie radę osoba niepewnie poruszająca się w środowisku Windows. Tacy odbiorcy też się zdarzają, a z czasem ich liczba będzie rosnąć w miarę jak Internet podbijać będzie najpierw firmy a potem ich pracowników.

Jak dotychczas na całym świecie liczba użytkowników sieci Internet wzrastała lawinowo, i nie ma powodu aby podobna sytuacja nie wystąpiła też w Polsce. Dostęp do Internetu jest obiektywnie tani, jednak na prywatną kieszeń nadal dość drogi, szczególnie jeśli chodzi o pełen dostęp do Internetu, nie tylko ograniczony do poczty elektronicznej.

Na rynku działa obecnie ponad czterdziestu usługodawców i potencjalny użytkownik ma możliwość wyboru. Ceny, jak również usługi są dość zróżnicowane, istnieje możliwość uzyskania pełnego konta już za około 30 zł, ale podobna usługa w innej firmie może kosztować też 150 zł. Tak więc, często również niektóre firmy decydują się na korzystanie tylko z poczty elektronicznej. Możliwość wyboru dostawcy dotyczy mieszkańców dużych miast, w których działa najwięcej firm. Należy przy tym pamiętać, że klient ponosi dodatkowo koszt połączenia telefonicznego, co jest czynnikiem ograniczajacym rozwój Internetu w Polsce. Przykładowo przy korzystaniu z Internetu przez godzinę dziennie miesięczny wydatek za telefon wyniesie w przybliżeniu 100 zł. Koszt ten będzie odpowiednio wyższy jeśli nie będzie to rozmowa lokalna, co zdecydowanie ogranicza szanse na korzystanie z Internetu dla mieszkańców małych miejscowości.

Szansą dla indywidualnych użytkowników Internetu może stać się sieć kablowa. W tym roku warszawska telewizja kablowa "Aster City" dysponująca siecią telekomunikacyjną docierającą do 144 tys. mieszkań (90 km światłowodów) zamierza zaoferować niektórym abonentom dostęp do Internetu. Przystosowanie sieci do komunikacji dwustronnej ma kosztować ok. 1% wartości sieci. Dostęp do Internetu poprzez kablową sieć TV będzie dla użytkowników indywidualnych dużo szybszy, wygodniejszy (przez modem kablowy można będzie przesłać od 4 do 10 mln bitów na sekundę) i , co najważniejsze, eliminujący konieczność dodatkowych opłat za połączenia telefoniczne.

Odrębnym problemem jest sprawa łączy do sieci szkieletowej, a przede wszystkim ich prędkości - wielu dostawców posługuje się wolnym łączami (poniżej 64 kbps), które na dłuższą mete nie będą satysfakcjonować użytkowników.

Wielu dostawców nie prowadzi monitorowania własnej instalacji sieciowej, czy też nie chroni się przed ewentualnymi skutkami awarii dublowanym dostępem do sieci szkieletowej, tak aby móc zapewnić ciągłość łączności. Pogarsza to sytuację klienta, który jest pozbawiany dostępu bez informacji o przyczynie; staje się on w ten sposób źródłem informacji dla usługodawcy - osobliwym testerem stanu użyteczności sieci.

METODY TARYFIKACJI I ICH SKUTKI

Andrzej Zienkiewicz
Naukowa i Akademicka Sieć Komputerowa
Marian Suskiewicz
Telekomunikacja Polska S.A.

1. Wprowadzenie

Teleinformatyka polska stoi przed wyborem modelu finansowania jej rozwoju. Jednym z tych modeli jest wprowadzenie odpowiedniego systemu odpłatności za korzystanie z Internetu, co z kolei jest warunkiem koniecznym dalszego utrzymania szybkiego rozwoju jego tempa. Internet , kiedyś sieć głównie wykorzystywana przez wojsko, następnie przekazana środowisku akademickiemu, służy obecnie znacznie szerszej grupie użytkowników. Korzysta z niej coraz więcej prywatnych osób, różne instytucje i przedsiębiorstwa. Wraz z postępującą komercjalizacją Internetu pojawiają się nowe usługi, a wiele firm chce robić interesy na nowym, wielkim rynku, który tworzy ponad 50 mln użytkowników sieci. Sieć Internet o zasięgu światowym wydaje się być wymarzonym środowiskiem do robienia interesów [1]. Funkcjonowanie jednak takiej sieci wymaga wielu nakładów finansowych, technicznych, ludzkich, itp. Koszty te powinny być rekompensowane dla operatorów i providerów usług, za udostępnianie tych możliwości dla prawie wszystkich chętnych do korzystania z nich. Niestety, Polska nie mogła uczestniczyć od samego początku w rozwoju światowego Internetu, podlegała restrykcjom nałożonym przez COCOM. Na szczęście jednak zmiana układu politycznego przyniosła możliwość zniesienia tych ograniczeń i stało się możliwe podłączenie naszego kraju do globalnej infrostrady, którego realizatorem był NASK. W wyniku prac Zespołu NASK, wypozażonego w pierwszym okresie z funduszy KBN, udało się stworzyć podwaliny sieci szkieletowej IP w Polsce . Jednak dalszy rozwój Internetu wymaga rozwiązania dwóch podstawowych problemów: pierwszy związany z ciągłymi brakami funduszy na rozwój sieci, drugi zaś to niedostosowane ustawodawstwo i prawodawstwo do obecnych wymogów w zakresie komputeryzacji szeroko rozumianej[2]. Po pierwszym okresie zaspokojenia największego głodu w krajowej infrastrukturze telekomunikacyjnej czas zacząć myśleć o telekomunikacji i teleinformatyce również w kategoriach ekonomii. Jednak klasyczne reguły analizy ekonomicznej stosowane w gospodarce rynkowej nadają się do wykorzystania w sektorze telekomunikacyjnym czy teleinformatycznym tylko w pewnym zakresie. Konkurencja powoduje, że spadają ceny. Operatorzy zaczynają się oskarżać o stosowanie dumpingu, czyli sprzedaży usług poniżej kosztów. Taki zarzut postawiono ostatnio firmie Deutsche Telekom, gdy zaproponowała redukcję taryf na usługi świadczone dla dużych firm [3]. Ten przykład wskazuje, że istnieją duże problemy i trudności w ocenie kosztów świadczonych usług teleinformatycznych. Poniżej zostaną

przedstawione niektóre ze stosowanych modeli taryfikacji usług i wyceny kosztów ich realizacji.

2. Tendencje w rozwoju i rozliczeniach usług sieci Internet

Internet stanowi potężne narzędzie komunikacji międzyludzkiej, z możliwości którego i związanymi z tym konsekwencjami do końca nie zdajemy sobie jeszcze sprawę.
Wobec wykładniczego wzrostu użytkowników systemu w Polsce i na świecie, coraz częściej pojawiają się opinie i wyrażana jest zarazem troska o to aby światowej sieci Internet nie zagroził całkowity paraliż spowodowany ogromnym wzrostem liczby jego użytkowników (aktualnie ponad 30 mln) oraz objętością przekazywanych informacji (30 Tbit miesięcznie, 1 Terabit = 10^6 Mbit).
Użytkownicy sieci coraz bardziej uskarżają się na spadek szybkości transmisji w sieci. Nowe zestawy protokołów World Wide Web umożliwiają funkcje interakcyjne, otrzymywanie zdjęć i rozbudowanej grafiki, a nawet dźwięku i obrazu, co istotnie przyczynia się do spowolnienia przepływności sieci.
Jak zauważył w swoim wystąpieniu prof. Tomasz Hofmokl podczas I Ogólnopolskiej Konferencji i Wystawy Promocyjnej "Internet w Polsce" (W-wa 21 - 22.09.95), ogólnoświatowym problemem jest wysoki poziom kosztów i niedostatek łączy międzykontynentalnych o dużej przepustowości. Regułą jest, że koszt dzierżawy linii cyfrowej rośnie liniowo wraz z jej przepływnością. Taka sytuacja nie sprzyja konstrukcji sieci szkieletowych o dużej przepływności i minimalizacji jednostkowych kosztów przesyłania jednego segmentu. Polska w tym względzie nie należy do wyjątku.
Na świecie podejmuje się już zdecydowane działania mające na celu przeciwdziałanie załamania się całego systemu. Przejawia się to głównie w procesie komercjalizacji i cięciach rządowych dotacji i subsydiów. Nawet tak bogate państwo i prekursor w tej dziedzinie jakim są St. Zjednoczone A.P., wycofało się już z subsydiowania sieci Internet. Dotychczas rząd amerykański przeznaczał rocznie 10 mln USD na pokrycie kosztów eksploatacji systemu. W 1994, w ramach prywatyzacji, pięć spółek telefonicznych takich jak Pacific Bell, Ameritech, Sprint, Metropolitan Fiber Systems oraz MCI przejęło czynności administrowania siecią na terenie USA. W rezultacie, ośrodki akademickie wnoszą obecnie opłaty za łączność na rzecz operatorów telekomunikacyjnych.
Dyskusja na forum światowej konferencji INET'95, na Hawajach potwierdziła tezę, że dotowanie i sponsorowanie na tym etapie rozwoju sieci straciło swoją rację bytu i prowadzi do systematycznej degradacji systemu wyrażającej się m.in. w:

- ograniczeniu możliwości elastycznego podwyższania sprawności i modernizacji sieci,
- rosnących opóźnieniach i utracie pakietów,
- braku możliwości zalogowania się w systemie,

• długim oczekiwaniu na kolejne kroki przy realizacji konkretnej funkcji typu telnet, ftp itd.
• wzroście liczby niezadowolonych użytkowników,
• groźbie zablokowania sieci.

Przy przesyłaniu dużych binarnych plików pocztą elektroniczną już znacznie wcześniej praktycznie zalecano aby :

• prosić o pomoc administratora systemu o informacje, czy taki plik wysyłany w normalnych godzinach pracy nie spowoduje przeciążenia systemu bądź utrudnienia komunikacji ze światem zewnętrznym,
• uzgadniać sesję z odbiorcą, który może używać powolnego połączenia z siecią lub posiadać bardzo ograniczoną przestrzeń dyskową,
• w miarę możności dzielić duże pliki na kilka mniejszych.

Odwołując się do rozwoju historycznego Internetu na świecie, możemy mówić zaledwie lub aż, o ponad 20 letniej przestrzeni czasowej (w przypadku Polski niecałe 6 lat). Na tarczy odmierzającej czas jest to niemalże cała epoka, biorąc pod uwagę dynamikę rozwoju Internetu. Jak inni wyobrażają sobie zmiany i tendencje w niedalekiej przyszłości, można powołać się na tezy prezentowane na tegorocznej majowej konferencji w Londynie (23-24.05.1995) poświęconej zagadnieniom Internetu.

O ile proces komercjalizacji będzie wymuszał określone zmiany w funkcjonowaniu Internetu, o tyle sam system będzie też zwrotnie oddziaływał na zdarzenia gospodarcze np.:

• projektowanie wyrobów, źródła finansowania i sama produkcja będzie podlegała fragmentaryzacji i geograficznemu rozproszeniu, przy czym :
- wiedza i umiejętności ludzkie będą "zasysane" (ogniskowane), a fizyczna produkcja będzie natomiast rozpraszana na obszary gospodarek o niskich kosztach produkcji,
- korporacje, firmy będą operować i zarządzać "wirtualnie" z tzw. podatkowych "rajów" (np. Andora, Luksemburg, Monako, Lichtenstein itd.),
• konsumenci będą mieli szerszy dostęp do zwiększonego zakresu produktów,
• operacje handlowe w czasie rzeczywistym i reakcje rynku na "nowości" będą natychmiast rejestrowane i będą informować sprzedawcę, umożliwiając mu reagowanie na poziom cen oraz na zmianę kanałów dystrybucji towarów. Taka sytuacja będzie również istotnie ułatwiała przewidywanie (zbliżone do rzeczywistego) popytu na towary i usługi, przez co ryzyko działalności gospodarczej ulegnie znacznej redukcji.
• użytkownicy Internetu dokonując płatności za pomocą "cyber-pieniędzy" mogą wywrzeć istotny wpływ (praktyczny dowód na "nieprzewidywalność" skutków sieci) na ograniczenie roli tradycyjnych systemów płatniczych, w tym płatności za pomocą kart kredytowych. Mogą również wywrzeć wpływ na normalny obieg pieniężny, na ilość gotówki w obrocie, gdy wirtualne transakcje zaczną zastępować tradycyjne. Stosując obopólną zgodę, sprzedający dobra za pośrednictwem sieci i kupujący korzystają z płatności bezgotówkowej. Naliczają oni sobie pewne kwoty, nierzadko kumulują je, oszczędzają, aby potem przeznaczyć je na inne zakupy lub usługi w sieci oferowane zupełnie przez kogoś innego.

• znaczenie hierarchicznego rynku tj. powiązania w układzie producent - hurtownik - detalista - konsument ulegnie radykalnemu zmniejszeniu, gdyż producent będzie w stałym kontakcie (w zależności od potrzeby) z konsumentem.

• zyski z marż handlowych zanikną, a ich redystrybucja dokona się na rzecz producenta i konsumenta.

Obecnie jesteśmy świadkami podejmowania na świecie określonych działań mających jednak na celu wprowadzenie pewnych ograniczeń w dostępie do informacji. W końcu dostrzeżono, że pełny liberalizm w tym względzie może okazać się również społecznie szkodliwy, szczególnie jeżeli chodzi o manipulowanie informacjami i rozpowszechnianie materiałów dotyczących seksu i przemocy. Oprócz intensywnego wdrażania systemów ochrony informacji w sieci, doskonalone są rozwiązania, które pozwolą użytkownikom "filtrować" zasoby światowej sieci Internet w taki sposób, aby wybierać jedne zakresy informacji i korzystać z nich, a blokować dostęp do innych.

W zakresie zjawisk społecznych, w ich aspekcie międzynarodowym, raport przygotowany przez pozarządową organizację Panos Institute (finansowaną przez kraje skandynawskie) ostrzega natomiast przed nowym rodzajem ubóstwa - ubóstwem informacyjnym zagrażającym krajom trzeciego świata. Przyczyną nowego zagrożenia są ograniczone możliwości dostępu do światowych sieci komputerowych, a także (relatywnie do indywidualnych dochodów) wysokie w krajach rozwijających się ceny komputerów, urządzeń peryferyjnych i usług telekomunikacyjnych. 70 proc. komputerów podłączonych do Internetu znajduje się w USA, podczas gdy dostęp do tej sieci posiada mniej niż 10 państw afrykańskich

W zakresie techniczno - organizacyjnym Internetu zachodzą różnorodne zmiany. Obserwuje się tendencję wykorzystywania programowych metod do sporządzania obrazu sieci. Interesujące rozwiązanie zastosowano w Grecji. Stworzono tam oprogramowanie na bazie okienek Unixowych, które oprócz gromadzenia, przetwarzania przesyłanych ilości danych, sporządzania statystyk i wykresów, wyłuskuje ruch międzynarodowy, generowany przez poszczególnych użytkowników. Na każdym urządzeniu, do którego dołączeni są użytkownicy, sporządzany jest tzw. accounting, czyli zliczana jest ilość pakietów w zależności od adresów input & output. Znając topologię sieci wewnątrz Grecji, można orientować się jaki jest ruch wewnętrzny, a jaki zewnętrzny dla każdego abonenta. Grecy liczą za ruch w obie strony, ale tylko za ruch międzynarodowy [4].

Oprogramowanie do sporządzania statystyk przesyłanych danych to skrypty (na każde łącze zapuszczany jest tzw. skrypt, badający interwały) w systemie Unix, które ściągają poprzez SMTP ilości przesyłanych bajtów. Statystyki te są uchwycone na każdym porcie sieci wewnętrznej, a także na każdym porcie Service Provider'a. Każdy port można taryfikować i każdego użytkownika można oddzielnie taryfikować z dokładnością do 1 bajta. Ilość przesłanych danych jest mierzalna w obu kierunkach. Oprogramowanie dodatkowo gromadzi wiele innych statystyk, np. typy błędów czy zagrożenia upadku linii. Każdy klient może ściągnąć statystyki do swojego portu. Dodatkowo więksi

użytkownicy dołączeni liniami synchronicznymi (z reguły mają u siebie profesjonalne routery) mogą ściągać statystyki bezpośrednio ze swojego urządzenia.

3. Modele taryfikacji usług telekomunikacyjnych

W istniejących sieciach telekomunikacyjnych stosowane są rozmaite metody taryfikacji abonentów. Ze względów historycznych, najbardziej zaawansowane systemy rozliczania stosowane są w publicznych sieciach telefonicznych. Szczegółowe zasady rozliczania zależą od operatorów sieci. Zalecenia i normy organizacji międzynarodowych przedstawiają jedynie ogólne zasady prowadzenia rozliczania. Zgodnie z tymi zaleceniami taryfikacja określa usługi i zdarzenia podlegające rozliczaniu, definiuje jednostki pomiaru stopnia ich realizacji oraz przypisuje tym jednostkom wskaźniki opłat. Taryfikacja usług jest ograniczona techniczną możliwością ich pomiaru. Możliwości pomiaru wyznaczają granice dokładności taryfikacji [5].
W typowych sieciach telekomunikacyjnych opłaty naliczane przez operatorów sieci można podzielić na kilka grup:
- opłaty za dostęp do sieci,
- opłaty za korzystanie z oferowanych usług,
- opłaty dodatkowe (np. kary lub opłaty za priorytet w przesyłaniu informacji).
Tworząc system rozliczeniowy należy zwrócić uwagę na odpowiednią proporcję między składnikami opłat, aby np. opłaty za dostęp do sieci nie przewyższały opłat za korzystanie z usług.
Rachunki (faktury) mogą zawierać różne informacje zależne od rodzaju danych gromadzonych przez operatora, o dostępie do usług przez abonentów.

Jako główne elementy kosztów jakie ponoszą operatorzy - dostarczający usług internetowych zostały wymienione takie składniki jak:

- koszty linii międzynarodowych oraz krajowych,
- sprzęt (amortyzacja),
- personel, administracja,
-elementy dodatkowe (utrzymywanie serwerów, składki na organizacje międzynarodowe).

W stosunku do abonenta można sobie wyobrazić kilka modeli cennikowych w/g np:

I. pasma dostępu,
II. czasu korzystania,
III. wielkości ruchu,
IV. odległości (cennik strefowy).

W modelu I abonent płaci stały ryczałt wynikający z prędkości z jaką jest dołączony. Jest to w tej chwili najczęściej spotykany model (również w USA). Taryfikowanie jest proste, narzuty administracyjne na obsługę taryfikacji małe - z drugiej strony nie ma bezpośredniego przełożenia pomiędzy

wykorzystaniem pasma przez abonenta a opłatami. W modelu tym, wzrastający ruch generowany przez już dołączonych abonentów, nie wiąże się ze wzrostem wpływów z tytułu opłat za korzystanie z sieci. Następuje też uśrednienie w całej masie abonentów (ci, którzy mało korzystają z sieci płacą za tych, którzy korzystają dużo).

Pewną modyfikacją tego modelu jest stosowanie opłat wynikających z uśrednionego ruchu w długich okresach czasowych. Model ten generalnie nie gwarantuje w zadawalającym czasie wzrostu środków na upgrade'y linii wraz ze wzrostem ruchu w sieci.

Model II jest możliwy do zastosowania jedynie w sieciach opartych o połączenia typu dial-up i na tym obszarze rynku zapewnia nadążanie za potrzebami.

W modelu III abonent płaci za ruch przychodzący do abonenta, wychodzący od abonenta lub całkowity ruch w obie strony . W obecnej chwili szacuje się że 80% ruchu w sieci Internet jest generowane przez odbiorcę informacji.

Model IV - opłaty strefowe (na wzór opłat stosowanych w telefonii), wymaga analizy pakietów w sieci Internet (bardzo kosztowne i kontrowersyjne) i jest niezbyt klarowny w środowisku klient-serwer, które dominuje w tej chwili w sieciach transmisji danych.

Praktyczne rozwiązania stosowane w poszczególnych krajach są wypadkową omówionych schematycznie modeli:
Stany Zjednoczone charakteryzują się najniższymi kosztami dzierżawy linii. Niestety w innych regionach łącznie z Europą sytuacja jest diametralnie różna. Tym bardziej ostro występują tam problemy z kosztami utrzymania linii. Skrajnym cytowanym przykładem są Wyspy Karaibskie. Na Barbados koszt godzinnej pracy w internecie wynosi 24 USD. W Stanach można już znaleźć okrojony serwis za tę samą sumę na miesiąc.
W innych krajach można dostrzec pewną regularność. Początek rozwoju sieci ogólnie a Internetu w szczególności łączy się z poparciem organizacji rządowych. W miarę rozwoju sieci dotacje muszą rosnąć jeżeli sieć ma się rozwijać lub trzeba znaleźć inne rozwiązanie. Takim rozwiązaniem może być przechodzenie na samofinansowanie się sieci akademickich. W miarę "dojrzewania" sieci udział bezpośredni Państwa w finansowaniu działalności sieciowej maleje i sami użytkownicy utrzymują sieć. Takie rozwiązanie przyjęto w Chile, gdzie rząd jest przeciwny bezpośredniemu subsydiowaniu sieci dla nauki i szkolnictwa wyższego. Agencja FONDEF subsydiująca sieć postawiła termin dwuletni na przejście do systemu pełnego samofinansowania Z tego powodu REUNA (sieć komputerowa Uniwersytetów chilijskich) od stycznia 1994 buduje taki system włączając do sieci uniwersyteckich użytkowników spoza tego środowiska. Staje się przez to siecią komercyjną. Dla placówek naukowych i uniwersytetów oznacza to tylko, że sieci są zasilane

poprzez te placówki a nie bezpośrednio. Pozwala to lepiej zdyscyplinować użytkowników. Oznacza to także, że opłata za sieć jest coraz bardziej związana ze stopniem jej wykorzystania. Opłatę tę ponosi bądź użytkownik końcowy bądź instytucja, która go zatrudnia. W tym modelu nie musi maleć pomoc Państwa dla korzystających z sieci, tylko inna jest zasada dystrybucji środków.

W praktyce na świecie wdrożono kilka modeli obciążania użytkownika.

Komercyjny Internet w Rosji obciąża użytkownika za całkowity ruch jaki jest generowany na styku z użytkownikiem. Oznacza to, że abonent RELCOMu płaci za ruch wychodzący jak i przychodzący.

Podobny przykład taryfikacji znajdujemy w Nowej Zelandii. Uruchomienie usługi informacyjnej w tym systemie wiąże się z ponoszeniem wydatków poprzez usługodawcę za korzystanie z serwisu przez użytkowników. Nie nadaje się wobec tego do tworzenia np. niekomercyjnych serwerów WWW.

W Australii użytkownik płaci tylko za ruch przychodzący. Podstawowy ruch jest generowany przez ściąganie do siebie dużych zbiorów, czy to za pośrednictwem WWW, czy też FTP. System taki nie hamuje tworzenia serwerów informacyjnych.

System stosowany do 1995 roku w Polsce polegał na odpłatności za przepływność portu, do którego dołączony jest użytkownik. Jest to najpowszechniejszy system i najprostszy do stosowania. Tam, gdzie większość użytkowników jest centralnie finansowana nie odgrywa roli dyscyplinującej. W miarę "zatykania" się łącza pojawia się żądanie zwiększenia przepływności, na które nie ma pokrycia w środkach finansowych.

W Chile przyjęto system monitorujący ruch i taryfikujący użytkownika w zależności od klasy do której zostanie zaliczony.

W rozliczeniach pomiędzy operatorami (dostawcami IP) panuje na świecie zasada, iż operator "mniejszy" płaci "większemu" za dołączenie z odpowiednią prędkością oraz routing (możliwość połączenia z całym światem lub wybranym regionem). Równi sobie operatorzy w ogóle rezygnują z rozliczania się pomiędzy sobą lub rozliczają się na podstawie specyficznych umów dwustronnych. W praktyce jest tak, że wszyscy mający połączenie ze Stanami Zjednoczonymi płacą za dołączenie do amerykańskiego Internetu (opłaty za pasmo oraz za routing, czyli trasowanie pakietów w sieci).
Najbardziej popularną metodą taryfikacji usług Internetowych stosowaną przez wielu usługodawców (ang. service provider) jest ustalenie dwóch rodzajów opłat: opłaty jednorazowej i opłaty pobieranej zwykle co miesiąc.
Opłata jednorazowa nosi nazwę opłaty wstępnej, instalacyjnej lub administracyjnej jest pobierana od abonenta jednorazowo przy abonowaniu usługi dostępu do sieci Internet. Opłata ta przede wszystkim związana jest z kosztami administracyjnymi założenia konta oraz pokrywa koszt udostępnienia

portu. Część usługodawców, szczególnie świadczących usługi za granicą, rezygnuje z ustalenia dla swoich abonentów opłat jednorazowych.
Drugą opłatą ustalaną przez usługodawcę jest opłata abonamentowa, pobierana od abonenta zazwyczaj co miesiąc. Są usługodawcy ustalający stawki roczne. Usługodawca określa, co w ramach abonamentu otrzymuje klient; określa liczbę godzin korzystania z usług internetowych, rodzaj dostępu do sieci INTERNET, rodzaj usług i systemów informacyjnych dostępnych dla klienta. Pozwala to usługodawcy zróżnicować opłatę abonamentową, w zależności od wybranej przez klienta opcji.
Klienci komercyjni są zainteresowani opłatami za faktycznie zrealizowane usługi i stopień wykorzystania zasobów sieci, a nie stałe opłaty ryczałtowe. Dlatego nowoczesne sieci teleinformatyczne są wyposażone w sprzęt i oprogramowanie umożliwiające taryfikację abonentów. Urządzenia sieciowe prowadzą bezpośredni pomiar ruchu generowanego przez abonentów, co pozwala na dokładne wyznaczenie opłat.
W sieci Internet podstawowy sprzęt pracuje na poziomie bezpołączeniowego protokołu IP. Pomiar ruchu na poziomie transmisji datagramowej ogranicza jakość i wiarygodność pomiaru, a ponadto może powodować szereg błędów i nadużyć. W sieci Internet pomiar ruchu wykonywany jest przez zewnętrzne oprogramowanie pomiarowe, szacujące wielkość ruchu. Najnowsze jednak generacje routerów są wyposażone w wewnętrzne oprogramowanie pomiaru ruchu, dzięki czemu rozliczanie abonentów można prowadzić na podstawie danych generowanych przez routery dostępowe sieci szkieletowej [5].

4. Analiza wykorzystania sieci NASK w I kwartale 1996 roku

4.1 Analiza stosowania cennika NASK w I kwartale 1996 r

Treść	Styczeń		Luty		Marzec	
	Ilość	%	Ilość	%	Ilość	%
1. Ogółem abonenci	464		517		548	
2. Abonenci rozliczani	463		513		548	
3. Abonenci, których zmiana cennika z 1.01.96 dotyczy	225	100	247	100	268	100
W tym:						
4. Abonenci, którzy w wyniku zmiany cennika płacą mniej	144	64	168	68	168	63
5. Abonenci mieszczący się w bezpłatnym limicie ruchu	121	54	129	52	117	44

6. Abonenci objęci ograniczenim płatności do czterokrotnej opłaty wg. poprzedniego cennik	**18**	**8**	**15**	**6**	**28**	**8**
7. Abonenci, dla których wariant cennika z opłatą za pasmo jest opłacalny	**12**	**5**	**13**	**5**	**22**	**8**
8. W tym ponad 10% opłaty	**10**	**4**	**12**	**5**	**18**	**7**

4.2 Analiza ruchu w I kwartale 1996

Kwartał	Styczeń	Luty	Marzec
1. Ruch całkowity w MB 4.002.374	**1.234.973**	**1.181.821**	**1.585.580**
2. Ruch zagraniczny w MB 1.664.326	**377.176**	**440.083**	**847.067**
3. Ruch krajowy w MB 1.751.559	**598.541**	**574.238**	**578.780**
4. Ruch lokalny w MB 586.489	**259.256**	**167.500**	**159.733**

Jak z powyższych zestawień wynika stosowany cennik spełnia oczekiwania nie wywołując negatywnych skutków oraz zapewniając korzystne warunki rozwoju zwłaszcza dla małych (początkujących) abonentów. Z analizy oraz danych tutaj niepublikowanych wynika konieczność odrębnego rozwiązania abonamentów dla wiekich operatorów co w przeważającej części świata jest rozwiązywane indywidualnie.

5. Dylematy rzeczywistej taryfikacji

W tej części referatu zajmiemy się doświadczeniami z opracowywania i wdrażania systemów taryfikacji abonentów sieci Internet. W ostatnich miesiącach sprawa była szeroko komentowana w różnego rodzaju środkach masowego przekazu jednak bez koniecznego w tym przypadku głębszego zbadania problemów. Całą historia opracowania pozornie racjonalnego cennika opłat z marca 1995 roku oraz wpadka ekonomiczna wywołana jego stosowaniem przy gwałtownym wzroście ruchu może być dobrym materiałem dla unikania podobnych sytuacji. Poniższe rozważania nie

dotyczą lub tylko w małej części dotyczą dzierżawy kanałów logicznych w sieci Frame Relay i ATM.

5 .1 Cele taryfikacji

Podstawowymi celami taryfikacji w sieci NASK są :
- identyfikacja użytkowników sieci,
- rejestrowanie używania zasobów sieci,
- rozliczanie kosztów i obliczanie opłat.

W sieci Internet, która stanowi ostatnie ogniwo dostępu do większości abonentów, nie istnieje określony związek pomiędzy adresem a lokalizacją abonenta. W numerze telefonicznym, podobnie jak w adresie sieci X.25, prosta analiza numeru telefonu czy adresu abonenta pozwala na określenie kraju, regionu, miasta, centrali komutacyjnej i wreszcie linii abonenckiej. W sieci Internet ciąg cyfr adresu nic nie znaczy, dwie sąsiednie klasy adresowe mogą być przydzielone użytkownikom w innych częściach świata. Trwające ostatnio porządkowanie, mające na celu odciążenie router'ów, nie zmieni zasadniczo istniejącej sytuacji. Adresowanie domenowe i związany z nimi system Name Serwerów, zawierający pozory uporządkowania, nie zmienia sytuacji z dwóch powodów. Po pierwsze korzystanie z Name Serwerów ma znaczenie tylko w chwili poszukiwania adresu służącego do routingu i nie jest w ogóle konieczne - jest to tylko udogodnienie. Po drugie nie ma przeszkód, aby obsługiwać dowolny adres z dowolnego Name Serwera.
W takiej sytuacji tylko rejestracja działania użytkowników sieci pozwala na określenie kto i ile z niej korzysta. Rejestracja jest również konieczna za względu na mnogość operatorów oraz mnożące się samodzielne drogi połączeń, co grozi niekontrolowanym świadczeniem usług przez sieci pośredniczące. Rejestracja działania użytkowników ma również znaczenie dla szeroko pojętego bezpieczeństwa sieci i jej abonentów.

Racjonalne gospodarowanie siecią i jej modyfikacje wymagają znajomości stopnia wykorzystania jej elementów ogólnie i w rozłożeniu czasowym. Istotne jest przy tym, kto z sieci korzysta i jaka jest formalna konieczność zapewnienia odpowiedniego standardu usług. Dokładna rejestracja pomaga w określeniu czasu i miejsc wpływających na obniżenie jakości pracy sieci, które często leżą poza zasięgiem bezpośredniego działania operatora.
Wreszcie ostatnim celem taryfikacji jest ustalenie opłat, którymi należy obciążyć abonentów niezależnie od sposobu pokrywania należności. System opłat zwłaszcza związanych z ruchem pozwala na prowadzenie elastycznej polityki cenowej oraz gromadzenia środków na konieczne modyfikacje sieci bez czasochłonnego planowania, które ze względu na swój cykl zupełnie nie nadaje się do finansowania zmian.

5.2 Typu abonentów sieci

W dyskusjach, zwłaszcza w mediach masowego dostępu, operuje się najczęściej ogólnikami typu "społeczność informatyczna", "środowisko naukowe" itp. Nie istnieje nic konkretnie zdefiniowanego w ramach poprzednio wymienionych pojęć, jak i nie da się ustalić rozsądnego wymiaru potrzeb generowanych przez zbiorowości tak źle określone. We wszystkich tego typu zbiorowościach występują abonenci sieci zasadniczo różni w zakresie możliwości jak i potrzeb korzystania z sieci. Z naszych

doświadczeń wynika konieczność podziału abonentów na klasy, które nie są rozłączne, to znaczy, że jedne abonent może należeć do więcej niż jednej klasy.

a) Pierwszą, najliczniejszą grupę abonentów stanowią teraz i w przyszłości abonenci, którzy chcą mieć tylko możliwość czasowego dostępu do sieci, bez angażowania dodatkowych środków łączności. Są to obecnie posiadacze telefonów, a pewnie w niedalekiej przyszłości abonenci sieci telewizji kablowej. Zasadnicze opłaty są przez nich ponoszone na rzecz operatorów zapewniających podstawową łączność telefoniczną czy w przyszłości TVK. Występuje tu pokusa ograniczenia wszelkich dodatkowych form rejestracji i taryfikacji tych abonentów. Uważamy, że jest to podejście błędne, ponieważ naraża operatora i innych abonentów sieci na szkody spowodowane przez użytkownika bez żadnej możliwości regresu. A ogólnie wiadomo, że "okazja czyni złodzieja". Z tego powodu uważamy, że abonenci tego rodzaju powinni być rejestrowani nawet , jeśli podstawowe opłaty za łączność są wystarczające na pokrycie kosztów ich działania w sieci. Abonenci tego rodzaju nie posiadają stałego adresu w sieci, przydziela się im adres na czas działania. Ten sam adres w następnym połączeniu może posiadać inny abonent sieci.

b) Drugą liczną grupę abonentów tworzą użytkownicy również chwilowo dołączeni do sieci, jednak korzystający ze stałych zasobów sieci. Abonenci z poprzedniej grupy, nie posiadający stałego adresu, nie mogli odbierać do siebie adresowanych przekazów informacji. Ta grupa korzystając z kont na komputerach różnych operatorów sieci, tzw. skrzynek pocztowych, może odbierać do siebie adresowaną pocztę, może inicjować przesłanie zbiorów informacji, może wreszcie gromadzić zbiory informacji na komputerach usługodawców. Adres tego rodzaju abonenta składa się z adresu serwera, na którym jest obsługiwany oraz z nazwy konta, które na tym serwerze posiada.

c) Trzecią nieliczną grupę abonentów stanowią posiadacze sieci komputerowych łączący się poprzez telefony publiczne. Grupa ta w miarę rozwoju ISDN może stawać się coraz liczniejszą. Jej istnienie wymaga angażowania dodatkowych środków operatora, koniecznych dla obsługi adresu abonenta w czasie, kiedy ten jest odłączony od sieci. Abonenci tego rodzaju posiadają stały adres Internetowy, który w czasie odłączenia sieci nie jest bezpośrednio dostępny.

d) Czwartą grupę stanowią abonenci na stałe dołączeni do sieci, korzystający z niej dla potrzeb własnych. Posiadają oni własną klasę adresową i są stale dostępni w sieci, przez cały rok i przez całą dobę. Ich aktywność w sieci jest stosunkowo nie wielka, często porównywalna z aktywnością abonentów dołączanych do sieci czasowo.

e) Piątą grupę stanowią abonenci świadczący usługi osobom trzecim na podstawie koncesji lub w zakresie usług niekoncesjonowanych. Ta grupa abonentów operuje ograniczoną grupą klas adresowych, najczęściej świadczy usługi użytkownikom łączącym się przez telefon lub przez sieć.

f) Wreszcie grupę ostatnią tworzą wielcy operatorzy sieci komputerowych. Zaliczają się do niej operatorzy sieci miejskich (MAN), inni operatorzy publicznie jak TP SA, TELBANK, ATM, jak i operatorzy wewnętrznych sieci uczelnianych na przykład Politechniki Warszawskiej, czy Zgrupowania Ochota. Obciążenie sieci przez nich generowane różni się kilkaset do przeszło tysiąca razu od obciążenie generowanego

przez innych abonentów sieci. Posiadają oni własny AS (znany w całej sieci światowej wydzielony zbiór klas adresowych) lub określony zasób klas adresowych, z których przydzielają adresy własnym abonentom. Podstawy prawne działania tych abonentów są różne: posiadana koncesja lub zezwolenie telekomunikacyjne, działają w ramach sieci wewnętrznej lub wydzielonej lub wreszcie nie posiadają legalnej podstawy działania.

5.3 Typy taryfikacji

Różni abonenci sieci wymagają różnego typu taryfikacji. Omówimy je kolejno. Nie zakładamy, że wyczerpiemy wszystkie możliwości lub choćby znane nam przykłady stosowania taryfikacji na całym świecie.

A) Najprostszy typ taryfikacji związany jest z czasem przyłączenia do sieci. Ten typ taryfikacji sprawdza się wtedy, kiedy możliwości pracy w sieci są ograniczone przez warunki techniczne połączenia. Taryfikacja czasu jest powszechnie stosowana w sieciach publicznych i sieciach komputerowych dołączanych przez komutowaną sieć publiczną. Najczęściej stosowana jest opłata abonamentowa za określony czas pracy w sieci gwarantująca opłacalność usługi nawet przy znikomym czasie pracy oraz dodatkowa, najczęściej wyższa opłata za dodatkowy czas pracy. Ta zwiększona opłata stanowi zaporę przed nadmiernym obciążaniem sieci.

B) Drugi typ taryfikacji jest związany z wykorzystywanymi zasobami sieci. Mamy tu na myśli kilka różnych typów zasobów. Sama idea taryfikacji jest prosta jednak w przypadku Internetu może rodzić poważne negatywne skutki, jak miało to miejsce w przypadku NASK w 1995 roku.
Internet pracuje w trybie transmisji bezpołączeniowej. Oznacza to, że poszczególne pakiety informacji przekazywane są do sieci, która nie kontroluje kanału przesyłania, sekwencji nadawania i odbioru oraz zajętości kanału tramnsmisji, który nie jest zestawiany. W takiej sytuacji łatwo dochodzi do przepełnień kolejek informacji na portach wejściowych urządzeń sieciowych i w efekcie gubienia pakietów.
Zabezpieczeniem jest ograniczone średnie obciążanie sieci (do trzeciej części przepustowości) tak, aby występowało niskie prawdopodobieństwo chwilowych przeciążeń. Tylko taka sieć zapewnia wystarczający standard obsługi, zwłaszcza przy typowej dla sieci pracy interaktywnej, kiedy tylko czasowo ściąga lub nadaje się większe bloki informacji bez długiego oczekiwania na wynik. Jednak udostępnianie takich kanałów abonentowi grozi załamaniem pracy sieci, jeżeli nie jest ona przystosowana do przyjmowania dużego ruchu w każdym swoim elemencie, również na najdroższych łączach międzynarodowych. Wobec tego taryfikacja za zasoby, czyli pasmo musi być droga, tak aby starczyło na utrzymanie nadmiarowej sieci oraz musi być prowadzona reglamentacja dołączania abonentów stosownie do przepustowości całego systemu sieciowego.
Wariantem dla taryfikacji za zasoby jest wydzielanie części sieci oraz zawieranie indywidualnych umów na eksploatację wydzielonych zasobów. Oczywiście tego rodzaju procedura musi być ograniczona i może dotyczyć niewielkiego grona abonentów.

C) Wreszcie można taryfikować ruch przesyłany w sieci. Jest to najbardziej naturalny sposób wiążący opłaty z wykorzystaniem sieci, która w swojej istocie zajmuje się wyłącznie przesyłaniem informacji. Tego rodzaju taryfikacja wymaga wprowadzenie

opłaty abonamentowej gwarantującej opłacalność przyłączenie oraz dodatkowej opłaty za ruch ponad limit przewidziany w abonamencie. Przy tego rodzaju taryfikacji istnieje najłatwiejszy sposób na dostosowywanie ceny do kosztów, które w przypadku rosnącego ruchu spadają w odniesieniu do jednostki przesyłanej informacji.

5.4 Tabela możliwości taryfikacji

Niżej przedstawiamy tabelaryczne zestawienie sensownych typów taryfikacji dla różnych typów abonentów. W tabeli zastosujemy oznaczenia klas abonentów i typów taryfikacji użytych w poprzednich akapitach.

Typ abonenta/Typ Taryfikacji	A	B	C
a	++		
b	++	++	
c	++	++	
d		+	++
e		+	++
f		++	++

W tabeli zaznaczyliśmy plusem rozsądne sposoby taryfikacji, dwoma plusami szczególnie przydatne w świetle dotychczasowych doświadczeń.
Na zakończenie chcielibyśmy ostrzec przed kilkoma nieprawidłowościami w popularnych rozumowaniach. Panuje przekonanie, że zakup pasma jest rozsądniejszy niż opłata za ruch. Na przykładzie operatorów zagranicznych można wykazać, że czysta opłata za niekontrolowane pasmo jest kilkakrotnie wyższa niż za pasmo przeliczeniowe, czyli za ruch (pasmo obliczane jako średnia ruchu). Popularna jest ostatnio praktyka taniego sprzedawania pasma ruchu, poprzez dopuszczanie zbyt dużej ilości abonentów lub taniego sprzedawania kanałów transmisji bez gwarantowanej przepustowości. Postępowanie takie prowadzi do silnie promocyjnego zaniżania ceny. W niedługim czasie albo jakość usług dramatycznie spadnie na skutek przeciążenia łącza lub zajdzie konieczność podniesienia opłat ze zjawiskami, obserwowanymi na przykładzie zmiany cennika NASK. Nikt nie będzie skłonny zauważyć, że wzrost opłaty jest związany ze zwiększonym ruchem, zauważony będzie wyłącznie wzrost opłat określony jako wzrost cen.

6. Podsumowanie

Przedstawione powyżej rozważania wykazują, że problem taryfikacji i wyceny usług sieci Internet może być na wiele sposobów rozwiązywany. Wybór najlepszego modelu płatności nie jest sprawą łatwą, ponieważ musi uwzględniać wiele czynników wpływających na jego kształt. Ponadto niezmierne ważne są skutki jakie powoduje dany model w rozwoju powszechnych usług teleinformatycznych.

Wspomniane wyżej rozwiązanie greckie jest o tyle interesujące, że odpowiednio przystosowane do warunków polskich, może w przyszłości istotnie przyczynić się do oddalenia groźby blokady sieci. Przyszły cennik mógłby zawierać dodatkowo jeszcze dwie pozycje, nazywając je umownie "tryb pracy on-line" i "tryb pracy off-line" (w odniesieniu do ruchu międzynarodowego). Ci spośród użytkowników, którzy nie musieliby pilnie korzystać z zasobów sieci znajdujących się poza granicami Polski lub nie odczuwaliby potrzeby interaktywnej pracy w międzynarodowych relacjach płaciliby mniej. Natomiast operator udostępniłby w swojej sieci cash-servery i mirror-servery, które aktualizowałyby zbiory z kilkunastogodzinnym opóźnieniem. W ten sposób można (o ile jest to technicznie możliwe i finansowo opłacalne) istotnie odciążyć łącza międzynarodowe.

Model płatności za ruch przychodzący powoduje, że abonenci będą zobowiązani płacić za nadaną do nich pocztę, co w wielu przypadkach można uznać za wadę, ponieważ abonent może być przypadkowo zarzucony niepotrzebną informacją. Model ten został bardzo ostro skrytykowany przez szerokie grono abonentów sieci Internet w Polsce [6]. Zaletą jednak tego modelu jest nieograniczanie dostępu do baz danych. W przypadku usługi WWW płaci ten, kto ściąga informację.

Wycena usług internetowych jest złożonym i trudnym przedsięwzięciem z powodu braku jednoznaczności, kto właściwie ma płacić za ruch i przesyłaną informację.

Z jednej strony można by przyjąć, że płaci ten, który wysyła informację w sieć, bo korzysta z medium transportowego, tak jak to się dzieje z naszymi paczkami na tradycyjnej poczcie.

Z drugiej strony zaś jesteśmy właściwie zainteresowani jedynie pozyskiwaniem informacji ze światowych baz danych. W takiej sytuacji powinniśmy płacić za ruch przychodzący. Sytuacja się komplikuje, ponieważ możemy być zarzuceni niepotrzebną nam informacją pochodzącą od firm reklamowych, złośliwością innych abonentów lub też popełnimy błąd w technice posługiwania się systemem. Nie ma mechanizmów obronnych w sieci przed napływem takiej informacji.

Wprowadzenie jednolitego ryczałtu za korzystanie z sieci Internet (usług internetowych) będzie z kolei niesprawiedliwe, bo nie każdy w tym samym stopniu korzysta z sieci. Użytkownicy posiadają bowiem różny stopień wtajemniczenia w posługiwaniu się narzędziami (programami wspomagającymi).

Inny postulat pod adresem operatora sieci Internet mówi o zróżnicowaniu opłat od pory dnia, inna powinna być opłata w godzinach szczytu a inna w czasie najmniejszego obciążenia.

Dotychczasowy model finansowania oparty na dotacjach i sponsoringu praktycznie traci rację bytu w sytuacji wycofywania się KBN z przydzielania coraz to większych nakładów finansowych na rozwój teleinformatyki i sieci komputerowych.

Opłaty za pasmo dołączenia - dobre w początkowym okresie istnienia sieci, źle rokują na przyszłość z powodu drastycznego wzrostu ruchu. Opłaty za ruch

oznaczają stabilizację sytuacji dla wszystkich użytkowników i dostawcy (operatora), lecz wymagają zakupu specjalnego oprzyrządowania do monitorowania i taryfikacji ruchu w sieci.
Skorelowanie wysokości opłat z wielkością przesyłanego ruchu, powinno poprawić drożność sieci i na pewien okres odsunąć groźbę zablokowania możliwości przesyłowych. Nawet doraźny zakup kolejnych łączy nie rozwiązuje generalnego problemu jakim jest dyscyplinowanie klientów, ponieważ powstają nowe aplikacje, które w krótkim czasie wyczerpią nowe możliwości przesyłowe sieci. Powyższe przedsięwzięcia organizacyjno - techniczne powinny usprawnić obsługę klientów oraz uwiarygodnić operatora sieci, jako podmiotu działającego w interesie swoich abonentów. Niezbędnym jest również uzupełnienie wyposażenia sieci w elementy podwyższające bezpieczeństwo przesyłanych danych między abonentami sieci. Przyszłość polskiej informatyzacji zależny również od powszechnego zrozumienia przez całą społeczność internetową w Polsce potrzeby racjonalnego sposobu korzystania z zasobów sieci Internet. Im bardziej struktury opłat będą oddalone od faktycznych kosztów dostarczenia usługi, tym bardziej skrzywione będą relacje ekonomiczne również w innych działach gospodarki całego kraju.

Literatura:

1. Wichniewicz Darek : Biznes i pieniądze w Internecie, ComputerWord nr 36,10/1995r.
2. Młynarski Krzysztof: Internet w Polsce - rozwój czy zastój, Software 7/95r.
3. Piotrowski Andrzej: Telekomunikacja - koszty i opłaty, Telekom Forum, 3/95r.
4. NASK, Praca zbiorowa: Analiza cen i usług internetowych w Polsce, listopad 1995r.
5. Machowski Bogusław : Taryfikacja w sieciach pakietowych, materiały konferencji "POLMAN'96", Ośrodek Wydawnictw Naukowych, Poznań 1996r.
6. Uhlig Maciej , Car Marek : Ratujmy Polski Internet, Warszawa, TIM 12/95.

KOMPLEKSOWA OBSŁUUGA DUŻYCH UŻYTWNIKÓW SYSTEMÓW INFORMATYCZNYCH

Jerzy Goraziński

Inter-Net Polska Sp. z o.o. Warszawa

Rynek technologii informatycznych (IT) podobnie jak telekomunikacja i związany z nią przemysł są najbardziej dynamicznie rozwijającymi się sektorami gospodarki ostatnich lat na całym świecie. Teleinformatyka stanowi i będzie stanowić w XXI wieku podobne zaplecze technologiczne dla światowych rynków jak „para i elektryczność" w XIX wieku.

Rozwój zasobów telekomunikacyjnych związany z ogromnymi nakładami inwestycyjnymi, rośnie relatywnie znacznie wolniej niż niezwykle elastyczny i mający w ostatnich dwóch latach charakter „eksplozji" rozwój IT. Dodatkowym czynnikiem stymulującym rozwój IT jest jego „rynkowość" - lub w bezpośrednim tłumaczeniu z angielskiego „rynkowe zorientowanie" proponowanych rozwiązań.

Jeżeli spojrzymy na rynek telekomunikacyjny,nie będzie trudno zauważyć, że jest on tradycyjnie opanowany przez znane - ogromne korporacje o ponadnarodowych powiązaniach i niezwykle silnych tradycjach monopolistycznych. Korporacje te mają łatwy dostęp do kapitału, posiadają szeroką bazę wśród użytkowników i dobre zaplecze techniczne. Są też nękane wszystkimi bez wyjątku tradycyjnymi przypadłościami zbyt wielkich przedsiębiorstw.

Na rynku IT sytuacja jest odwrotna - nadal znaczny procent stanowią firmy, które swoje pochodzenie wywodzą raczej z „garażu w Kalifornii" niż z zasobnych kont bankowych. Sektor IT wciąż jeszcze stara się „zapracować" na ulubioną „chorobę" telekomunikacji - manię wielkości. Nie to jednak stymuluje burzliwy rozwój IT. Podstawowym czynnikiem sukcesu jest dobry, niezwykle zaawansowany technologicznie produkt i odważna polityka marketingowa.

Teoretycy produkcji i teoretycy marketingu stwierdzą w tym miejscu, że to są właśnie rady jakich udzielają swoim klientom. To prawda,ale jak zwykle nie do końca.

Czym na rynku IT jest dobry produkt ? Odpowiedź również i tu nie zdziwi teoretyków. Dobry jest ten produkt, który zadowala klienta. W tym miejscu kończą się jednak proste pytania, odpowiedzi i rozwiązania - bo czy Państwo, jako klienci IT, jesteście w pełni zadowoleni z edytora, którym się posługujecie? A czy brak wideokonferencji w Waszym komputerze, rozmiary i ciężar monitora nie bywają uciążliwe? Jak widać, osiągnięcie zadowolenia u Klienta to trudna i niewdzięczna praca.

Żeby jednak uchronić managerów telekomunikacji i IT od dalszych stresów, a ich klientów od narzekań, chcę zaproponować rozwiązanie, które łączy wysoką funkcjonalność z ekonomiczną efektywnością. Zacznę jednak od zabawnego, moim zdaniem, porównania IT do przemysłu samochodowego. Gdyby obie dziedziny rozwijały się w tym samym tempie, nikt z nas nie zmieściłby się już do swojego samochodu, a zamiast praw jazdy konieczne byłyby licencje pilotów ponaddźwiękowych samolotów.

Rozwój sieci cyfrowych i technologie umożliwiające coraz powszechniejsze i łatwiejsze wykorzystywanie powstających możliwości cyfryzacji dźwięku i obrazu, technologie kompresji umożliwiające przesyłanie coraz większych zbiorów w sieciach w coraz krótszym czasie - wreszcie aplikacje potrafiące wykorzystać wspomniane nowoczesne rozwiązania, to tylko mały wycinek obrazujący rozwój i możliwości rynku IT.

Jeżeli dodamy do nich tempo zmian technologicznych na poziomie 3 - 6 miesięcy, wzrost liczby użytkowników rzędu 10% miesięcznie, otrzymamy obraz sytuacji, z którą muszą sobie poradzić użytkownicy.

Indywidualny użytkownik wciąż ma możliwość wyboru. Może zaryzykować i radząc się znajomych uznanych za autorytety, autorytetów uznających się za autorytety lub zawzięcie studiując liczne publikacje dziennikarzy, uznanych bądź uznających się za autorytety, dokonać wyboru i zakupić wymarzone produkty. Może też zrezygnować z zakupu. Czy jednak tę bądź podobną taktykę możemy zastosować planując rozwój firmy lub przedsiębiorstwa ? Sądzę, że nie.

Jaka więc jest alternatywa? Można oczywiście zrezygnować z wprowadzania technologii IT w przedsiębiorstwie, ale w kontekście rozwoju tej dziedziny i jej zastosowań jest to równoznaczne z uznaniem się za „firmę drugiej kategorii" - nie dlatego, że wszyscy już „mają" informatykę, ale dlatego, że podobnie jak przy wszystkich technologiach teleinformatycznych - ci którzy ich nie mają - tracą źródło informacji o sobie i dla siebie. Co nam więc pozostaje ? Sądzę, że we wszystkich tych sytuacjach odpowiedzią jest outsourcing.

Niektóre organizacje nigdy nie uznają outsourcingu za odpowiednie dla nich rozwiązanie. Rozważanie wszystkich „za i przeciw" jest w ich przypadku zupełnie nieskuteczne, a outsourcing pozostanie poza sferą dostrzeganą przez szefów tych firm.

Dlaczego tak się dzieje i jak należy rozumieć outsourcing w warunkach polskich?

Na początek warto pokusić się o próbę definicji. Definicji może być wiele, ale dwie z nich oddają moim zdaniem istotę zagadnienia.

Pierwsza mówi nieco żartobliwie, że outsourcing to takie rozwiązywanie złożonych problemów technicznych, technologicznych i organizacyjnych zlecanych przez klienta, które po zakończeniu kontraktu pozostawia uśmiech na jego twarzy.

Druga określa outsourcing jako współpracę dwóch wzajemnie uzupełniających się firm, której celem jest realizacja przez firmę outsourcingową kompleksu działań technicznych i organizacyjnych mających charakter wspomagający i obsługowy w zakresie, który umożliwi maksymalną koncentrację klienta na jego podstawowych zadaniach i działaniach. Wymiarami efektywności działań outsourcingowych są : obniżenie kosztów produkcji i wzrost sprzedaży.

Jak dowodzą badania przeprowadzone w USA na bazie listy „Fortune 1000", ponad 50% firm wymienionych na tej liście uznaje outsourcing za rozwiązanie, które należy rozważyć planując dalszą działalność. Jednak nie ocena samego outsourcingu w sferze IT jako metody działania jest istotna - ważne jest widzenie roli IT w zmienianiu sposobu funkcjonowania i wypracowaniu nowej pozycji firmy na rynku.

Jeżeli rola IT jest widziana przez firmę jako sposób poprawienia wydajności i efektywności jej działania - jako pomoc w osiągnięciu i utrzymaniu konkurencyjności na rynku - outsourcing w tym zakresie powinien stać się jedną z rozważanych metod planowania działalności firmy.

Duże znaczenie ma wybór firmy outsourcingowej. Im bliższa jest rynkowi, na którym planujemy działać - im bardziej wyspecjalizowana i posiadająca szeroki dostęp do fachowej kadry - im silniej uzależnia własny sukces od sukcesu wspólnego przedsięwzięcia, tym większe szanse na realizację określonych przez nas celów współpracy i zadowolenie zarówno partnerów jak klientów.

Wartość outsourcingu ma wiele wymiarów :

- poprawia wyniki ekonomiczne - zarówno przez obniżenie kosztów (efektywniejsze rozwiązania techniczne, technologiczne i organizacyjne, lepsze wykorzystanie funkcjonujących rozwiązań) jak przez kreowanie nowych źródeł dochodu (rozwój produktów i usług - poprzez koncentrację działań firmy na wytwarzanym produkcie postęp technologiczny jest szybszy i pojawiają się nowe rynki zbytu),
- usprawnia obsługę klienta - szersze i bliższe kontakty z klientem umożliwiają aktywną wymianę i wykorzystanie informacji (dzięki temu zarówno klient jak firma zyskują - klient lepszą, szybszą i dopasowaną do potrzeb obsługę, a firma wiedzę o odbiorze produktu na

rynku, jego użytkownikach oraz elementach, które należy usprawnić lub poprawić w produkcie i działaniu firmy).

- umożliwia wybór najnowocześniejszych - czasem unikalnych rozwiązań dopasowanych do potrzeb klienta - które będą realizowane przez zespoły, pracujące i zbierające doświadczenia w najbardziej zaawansowanych sektorach gospodarki.

Podjęcie decyzji, że outsourcing jest dobrym rozwiązaniem problemów, z którymi musi poradzić sobie firma, nie jest łatwe i wymaga odpowiedzi na wiele pytań. Są to jednak pytania, na które dobry manager powinien znaleźć odpowiedzi znacznie łatwiej, niż na te które mógłby napotkać próbując samodzielnie poruszać się po rynku IT.

Warto przytoczyć kilka przykładowych pytań :

- jaka część funkcjonowania firmy jest, a która nie jest kluczowym elementem działalności firmy i może stanowić obszar dla outsourcingu,
- czy wybrany partner posiada odpowiednie kompetencje i jest zainteresowany wspieraniem podstawowych działań naszej firmy,
- jak działając wspólnie na rynku uzyskać większą siłę i elastyczność tzn. osiągnąć dominującą pozycję na rynku - oferując produkty lepsze i bardziej poszukiwane,
- wreszcie jak produkować więcej i taniej wytwarzając równocześnie bardziej zaawansowane technologicznie produkty.

O ile uzasadnione wydają się zyski płynące z koncentrowania się przez firmy na ich podstawowej działalności, podejmowanie współpracy z wyspecjalizowanymi partnerami strategicznymi dla usprawnienia w obszarze IT nie jest już tak jednoznacznie oceniane.

Rozważając podjęcie ewentualnej współpracy warto uświadomić sobie i kierownictwu firmy najistotniejsze korzyści wynikające z takich porozumień - gdyż od tej świadomości może zależeć decyzja o skorzystaniu z oferty firmy outsourcingowej.

Pierwszy z nich to aspekt ludzki. Przystępując do działań związanych z wprowadzaniem nowoczesnych rozwiązań z zakresu IT, firmy i przedsiębiorstwa najczęściej nie posiadają kwalifikowanej kadry. Jej odpowiednie przygotowanie ze względów finansowych, konieczności posiadania doświadczenia i potrzeby stałego podnoszenia kwalifikacji nie jest możliwe w wymaganym czasie. W wymiarze finansowym, obniżenie kosztów związanych z nabywaniem kwalifikacji i podnoszeniem umiejętności przez pracowników zatrudnionych w służbach utrzymania i obsługi, znacznie obniża koszty wytworzenia podstawowego produktu firmy. Na rynku polskim bardziej niż na rynkach światowych odczuwalny jest brak wysoko kwalifikowanej, posiadającej odpowiednie doświadczenie kadry IT. Firmy outsourcingowe w obszarze IT mają tę przewagę, że dzięki specjalizacji mogą opierać się na wysoko kwalifikowanych specjalistach. Połączenie elastyczności w tworzeniu zespołów realizujących zadania i wysokich kwalifikacji pracowników zapewnia szybsze i tańsze rozwiązywanie zadań przez firmę outsourcingową zarówno w okresie wzmożonej aktywności jak w fazie zmniejszonego zapotrzebowania na działania w zakresie IT.

Kolejnym ważnym elementem jest zapewnienie dostępu do najnowocześniejszych technologii i rozwiązań IT. Firmy działające w zakresie outsourcingu podobnie jak firmy produkcyjne dążą do zaoferowania najnowocześniejszego produktu. Perspektywa jego wykorzystania przez kilku partnerów i posiadanie odpowiednich kontaktów wśród producentów umożliwia często zaoferowanie produktów, które dopiero znajdą się na rynku. Biorąc pod uwagę tempo rozwoju technologicznego tylko partnerska współpraca z firmą posiadającą odpowiednie doświadczenie, kontakty i wiedzę umożliwiają maksymalne wykorzystanie możliwości oferowanych przez technologie informatyczne pojawiające się na rynku.

Ten właśnie model działania staje się podstawą funkcjonowania firm outsourcingowych w obszarze IT. Preferowane zasady współpracy to partnerstwo i współzarządzanie w

odróżnieniu do dotychczasowego układu „klient - sprzedawca" czy „zarządzanie na bazie kontraktu managerskiego".

Podobnie jak zasady współpracy zmieniają się też również zasady rozliczeń. W miejsce tradycyjnej zasady rekompensaty pojawia się podział uzyskanych korzyści/oszczędności z tytułu wprowadzenia określonych rozwiązań. Tradycyjny sposób myślenia o partnerze przy realizacji zadań w formie outsourcingu zmienia się z „miły ale niekonieczny gdyż generuje dodatkowe koszty" na „wnoszący nowe wartości, uzupełniający i dający oszczędności". Jak widać outsourcing może stać się twórczy dla obu współpracujących stron. Budowane relacje mają stworzyć mieszaninę wzajemnie uzupełniającej się wiedzy i umiejętności, umożliwiając realizację korzystnej dla obu stron, wspólnie planowanej i realizowanej rynkowej strategii. Celem i obiektem tej współpracy jest klient i realizacja jego potrzeb. Zadowoleniu klienta, podporządkowana jest struktura współpracy i związane z jej realizacją umowy - zawierane pomiędzy firmami.

Tak jak forma powinna nadążać za funkcją - tak struktura kontraktu powinna oddawać cele współpracy. Już to ostatnie stwierdzenie obrazuje trudności jakie napotykają firmy outsourcingowe w Polsce. Trzeba podkreślić, że w równej mierze zachowania ludzi - przyzwyczajenia, stagnacja i chęć zachowania przywilejów - jak niedoskonałość prawa i systemu wymiaru sprawiedliwości odziedziczonego i utrzymywanego od lat praktycznie w niezmienionej formie (bądź tworzonego niefachowo i niespójnie) sprzyjają praktykom monopolistycznym, ograniczając działania wynikające z rachunku ekonomicznego i planowania, na rzecz pseudoekonomicznych manipulacji politycznych.

Outsourcing jest działaniem, które może być efektywnie realizowane przy zachowaniu równowagi pomiędzy obszarami bezpośrednio kontrolowanymi i przekazanymi do zarządzania firmie partnerskiej. Ważne są przy tym :

- znaczenie wytypowanego obszaru dla działania firmy,
- planowane rozwiązania techniczne i organizacyjne,
- oraz zasoby i umiejętności personelu.

Najczęściej przekazywanymi firmom outsourcingowym obszarami są infrastruktura i zarządzanie sieciami informatycznymi oraz billing. W obu wypadkach systemy stają się coraz bardziej rozbudowane, wymagające do obsługi specjalistycznych umiejętności, a konieczność stałego utrzymywania sprawności urządzeń przy jednoczesnej rozbudowie i rozwoju technologicznym stanowią obszar doskonale nadający się do zastosowania outsourcingu.

W Polsce i pozostałych krajach b.bloku socjalistycznego następuje gwałtowny rozwój technologii. Niestety dotychczasowe uwarunkowania - których wynikiem jest brak tradycji budowania elastycznych struktur, dopasowanych do zmiennych warunków w jakich będą funkcjonować na rynku, opóźnia szersze zastosowanie outsourcingu i ogranicza do niego zaufanie, podobnie jak do funkcjonowania bez własnego zaplecza magazynowego lub biura na bazie „open space shareing".

Biorąc pod uwagę wszystkie poprzednio omówione elementy związane z planowaniem wspólnych działań z partnerem działającym w obszarze IT należy pamiętać, że dla osiągnięcia sukcesu na rynku niezbędna jest prawidłowa organizacja, oraz właściwi ludzie i odpowiednio dobrana technologia. Ważne jest też przekonanie, że można i należy współpracować, a dla obu współpracujących stron outsourcing może być rozwiązaniem przynoszącym zarówno sukcesy jak korzyści ekonomiczne.

Dopiero w tak stworzonych ramach można określić rolę i zasady współpracy z firmą outsourcingową i oczekiwać, że będzie efektywnie wspierała dążenie do wspólnie określonych celów. Najważniejszym z nich powinno być spełnienie oczekiwań i potrzeb - naszych i klienta.

Warszawa, 29 kwietnia 1996

KONCESJE I ZEZWOLENIA TELEKOMUNIKACYJNE

Witold Busz

Ministerstwo Łączności, Departament Techniki i Rozwoju
Warszawa, ul. Chopina 1

Ustawowe definicje niektórych terminów

Międzynarodowa sieć telekomunikacyjna - sieć telekomunikacyjna, w której co najmniej jedno urządzenie telekomunikacyjne, z wyłączeniem urządzeń usytuowanych na sztucznych satelitach Ziemi, jest zainstalowane poza obszarem Polski;

usługa telekomunikacyjna - działalność gospodarcza polegająca na zapewnianiu przekazu informacji za pomocą sieci i linii telekomunikacyjnych;

sieć telekomunikacyjna użytku publicznego - sieć telekomunikacyjna służąca do świadczenia usług telekomunikacyjnych każdemu użytkownikowi na obszarze działania operatora tej sieci;

wydzielona sieć telekomunikacyjna - sieć służąca do świadczenia usług telekomunikacyjnych dla ograniczonego zbioru użytkowników;

wewnętrzna sieć telekomunikacyjna - sieć nie służąca do świadczenia usług telekomunikacyjnych;

usługa telekomunikacyjna o charakterze powszechnym - usługa telekomunikacyjna polegająca na zapewnianiu przekazu telefonicznego lub telegraficznego w sieci telekomunikacyjnej użytku publicznego;

operator - podmiot uprawniony do świadczenia usług telekomunikacyjnych na mocy ustawy lub koncesji albo działający na podstawie zezwolenia.

Wstęp

7 lipca 1995r. weszła w życie ustawa z dnia 12 maja 1995r. o zmianie ustawy o łączności oraz niektórych innych ustaw. Ustawa ta wprowadziła wiele istotnych zmian do ustawy z dnia 23 listopada 1990r. o łączności, a jednolity, obecnie obowiązujący, tekst ustawy o łączności został opublikowany w Dzienniku Ustaw z 1995r. Nr 117, poz. 564. Nowelizacja ustawy spowodowała wydanie przez Ministra Łączności kilkunastu nowych lub zmienionych rozporządzeń i zarządzeń. Zmiany wprowadzone w ustawie i w aktach wykonawczych do niej mają szczególne znaczenie dla przebiegu procesu wydawania dokumentów uprawniających do budowy infrastruktury telekomunikacyjnej i do świadczenia usług telekomunikacyjnych. Poniżej zostaną przedstawione obecne uregulowania prawne dotyczące wydawania tych dokumentów.

Podmioty wykonujące działalność w dziedzinie telekomunikacji

Zgodnie z art. 4 ustawy o łączności działalność w dziedzinie telekomunikacji wykonują:
1) Telekomunikacja Polska - Spółka Akcyjna,
2) jednostki organizacyjne MON i MSW - w zakresie własnych potrzeb zaspokajanych za pomocą własnych sieci telekomunikacyjnych,
3) jednostka organizacyjna MSZ - w zakresie potrzeb polskiej służby dyplomatyczno-konsularnej zaspokajanych za pomocą radiowej sieci telekomunikacyjnej,
4) jednostki organizacyjne MSW - w zakresie łączności rządowej, w porozumieniu z Ministrem Łączności,
5) podmioty, które otrzymały koncesję lub zezwolenie - w zakresie objętym koncesją lub zezwoleniem.

Z powyższego zapisu wynika, że jednostki określone w punktach 1 - 4 wykonują działalność w dziedzinie telekomunikacji na mocy ustawy, natomiast inne podmioty mogą działać w tej dziedzinie dopiero po uzyskaniu koncesji lub zezwolenia.

Koncesje i zezwolenia

Minister Łączności wydaje, w drodze decyzji administracyjnych, koncesje na świadczenie usług telekomunikacyjnych, natomiast Minister lub Państwowa Agencja Radiokomunikacyjna (w zakresie określonym przez Ministra) wydają zezwolenia na zakładanie i używanie urządzeń telekomunikacyjnych (a w tym - radiokomunikacyjnych urządzeń nadawczych i nadawczo-odbiorczych) i sieci telekomunikacyjnych.

Minister Łączności, wykonując upoważnienie ustawowe, wydał rozporządzenie, zgodnie z którym:
1) nie wymaga koncesji świadczenie usług telekomunikacyjnych:
   - za pomocą urządzeń końcowych, z wyjątkiem central abonenckich lub serwerów międzysieciowych,
   - w sieciach wydzielonych nie przekraczających obszaru jednego budynku lub wyodrębnionego zespołu budynków niemieszkalnych, zarządzanych przez jeden podmiot,
   - w sieciach wydzielonych znajdujących się w jednej miejscowości, w zakresie objętym działalnością tych sieci w dniu wejścia w życie rozporządzenia (2 listopada 1995r.),
   - w sieciach telewizji kablowej i odbioru zbiorowego, służących wyłącznie do rozprowadzania lub rozpowszechniania programów radiofonicznych lub telewizyjnych,
2) nie wymaga zezwolenia zakładanie i używanie:
   - telekomunikacyjnych urządzeń końcowych,
   - nadawczo - odbiorczych radiokomunikacyjnych urządzeń końcowych (abonenckich) pracujących w sieciach telekomunikacyjnych,
   - sieci wydzielonych (z wyłączeniem sieci radiokomunikacyjnych), w których świadczenie usług nie wymaga koncesji,
   - sieci wewnętrznych znajdujących się w jednej miejscowości lub służących wyłącznie do celów technologicznych albo do zarządzania, z wyłączeniem sieci radiokomunikacyjnych,
   - sieci telewizji kablowej i odbioru zbiorowego, służących wyłącznie do rozprowadzania lub rozpowszechniania programów radiofonicznych lub telewizyjnych, zainstalowanych w jednym budynku i posiadających nie więcej niż 250 gniazd abonenckich,
3) nie wymaga zezwolenia używanie wyłącznie na własne potrzeby urządzeń i sieci telekomunikacyjnych dzierżawionych od uprawnionych podmiotów.

Przetargi

Nowo wprowadzony do ustawy o łączności art. 14a zobowiązuje Ministra Łączności do przeprowadzania przetargów w celu wyboru podmiotów, którym wydane będą koncesje. Minister może odstąpić od przeprowadzenia przetargu jedynie w przypadkach określonych w ustawie, a w tym m.in. wówczas, gdy nie uważa za celowe ograniczanie liczby wydawanych koncesji na świadczenie danych usług na danym obszarze. Oznacza to praktycznie pozostawienie Ministrowi Łączności dużej swobody przy ustalaniu i realizowaniu polityki koncesjonowania, co dokładniej zostanie omówione w jednym z następnych rozdziałów referatu.

Za udostępnianie dokumentacji przetargowej Minister pobiera opłaty stanowiące dochód Skarbu Państwa.

Wydawanie oraz zawartość koncesji i zezwoleń

Koncesje i zezwolenia wydawane są na pisemny wniosek, który powinien zawierać: oznaczenie wnioskodawcy i jego siedziby, określenie przedmiotu i obszaru działalności oraz przewidywaną datę jej rozpoczęcia. Minister Łączności może ponadto zobowiązać wnioskodawcę do przedstawienia swego składu kapitałowego oraz dokumentów i informacji mogących uprawdopodobnić, że spełni on warunki, które będą określone w koncesji lub zezwoleniu.

Koncesja lub zezwolenie musi określać: osobę upoważnioną i jej siedzibę, przedmiot, zakres oraz obszar działalności objętej koncesją lub zezwoleniem, datę rozpoczęcia tej działalności oraz czas ważności wydanego dokumentu. Ponadto w koncesji lub zezwoleniu można, w miarę potrzeby, określić m.in. warunki wykonywania działalności (formy świadczenia usług, wymagania techniczne, rodzaj i rozmiar sieci telekomunikacyjnej), sposób wykonywania obowiązków na rzecz obronności i bezpieczeństwa państwa oraz podać skład kapitałowy osoby upoważnionej.

Za wydanie zezwolenia pobierana jest opłata skarbowa, która - w przypadku, gdy będąca przedmiotem zezwolenia sieć telekomunikacyjna jest wykorzystywana do prowadzenia działalności gospodarczej - wynosi obecnie 500 ZLN. Podmioty, które uzyskały zezwolenia uiszczają ponadto, określone w rozporządzeniu Ministra Łączności, roczne opłaty za używanie urządzeń i sieci będących przedmiotem zezwolenia.

Podmioty, które uzyskały koncesję, uiszczają jednorazowo lub ratalnie opłaty, które stanowią dochód Skarbu Państwa. Minister Łączności ustalił w rozporządzeniu wysokość tych opłat, która zależna jest od rodzaju świadczonych usług oraz obszaru działalności operatora. Minimalna opłata, dotycząca koncesji na świadczenie jednego rodzaju niepowszechnych usług telekomunikacyjnych przy wykorzystaniu sieci innych operatorów, wynosi 200 ECU. Obliczone, zgodnie z rozporządzeniem, opłaty za otrzymanie koncesji na świadczenie usług w sieci telefonicznej użytku publicznego, w przypadku wydania koncesji łącznie z zezwoleniem na zakładanie i używanie tej sieci, wynoszą dla obszaru województwa od 50 tys. do miliona ECU zależnie od liczby ludności, gęstości zaludnienia i gęstości telefonicznej w danym województwie, przy czym opłaty te mogą ulec zwiększeniu w razie udzielenia koncesji w drodze przetargu.

Ograniczenia w wydawaniu koncesji i zezwoleń

Zgodnie z art. 18 ustawy o łączności Minister Łączności ma obowiązek odmówić wydania koncesji lub zezwolenia m.in. wówczas, gdy:

- zagrażałoby to interesowi gospodarki narodowej, obronności lub bezpieczeństwu państwa albo dobrom osobistym obywateli,
- byłoby to sprzeczne z umowami międzynarodowymi, których Polska jest stroną,
- utworzenie sieci objętych zezwoleniem może spowodować niekorzystne skutki dla rozwoju danej usługi na określonym obszarze,
- wnioskodawcy lub podmiotowi w stosunku do którego wnioskodawca jest podmiotem zależnym, w okresie pięciu lat przed złożeniem wniosku, cofnięto koncesję lub zezwolenie,
- wnioskodawca nie daje rękojmi należytego wykonywania działalności,
- wybór podmiotu, któremu zostanie wydana koncesja, nastąpi drogą przetargu.

Nowelizacja ustawy o łączności znacznie poszerzyła możliwości wydawania decyzji odmownych w postępowaniu o przyznanie koncesji lub zezwolenia, co w szczególności odnosi się do oceny ekonomicznych i technicznych możliwości wykonywania działalności przez wnioskodawcę.

Z art. 16 ustawy o łączności wynika m.in., że:

- Telekomunikacja Polska SA ma monopol na świadczenie międzynarodowych usług telekomunikacyjnych o charakterze powszechnym i jest to jedyny monopol ustawowy posiadany przez TP SA,
- zezwolenia na zakładanie i używanie międzynarodowych sieci telekomunikacyjnych oraz urządzeń radiokomunikacyjnych do realizacji łączności o zasięgu przekraczającym granice Polski mogą otrzymać wyłącznie podmioty nie posiadające udziałów kapitału zagranicznego,
- koncesję na świadczenie: usług przewodowego rozprowadzania i rozpowszechniania programów radiofonicznych i telewizyjnych oraz wszelkich usług w sieciach telekomunikacyjnych przekraczających obszar telefonicznej strefy numeracyjnej (sieciach międzywojewódzkich), usług międzynarodowych niepowszechnych i usług w sieciach telefonii komórkowej, a także zezwolenie na zakładanie i używanie ww. sieci, mogą otrzymać tylko podmioty, w których udział kapitału zagranicznego oraz udział głosów podmiotów zagranicznych w zgromadzeniu wspólników lub walnym zgromadzeniu nie przekracza 49%, a ponadto członkami zarządu spółki i rady nadzorczej są w większości obywatele polscy zamieszkali w Polsce.

W pozostałych, nie wymienionych wyżej przypadkach, ustawa umożliwia wydawanie koncesji i zezwoleń bez żadnych ograniczeń dla kapitału zagranicznego. Dotyczy to w szczególności koncesji na świadczenie usług w wewnątrzstrefowych sieciach telefonicznych oraz zezwoleń na zakładanie i używanie takich sieci, a także koncesji na świadczenie usług niepowszechnych o zasięgu ogólnopolskim.

Cofanie koncesji i zezwoleń

Minister Łączności cofa koncesję lub zezwolenie jeżeli:

- działalność jest wykonywana w sposób sprzeczny z ustawą, warunkami określonymi w koncesji lub zezwoleniu lub zagraża obronności albo bezpieczeństwu państwa,
- podmiot w sposób uporczywy uchyla się od uiszczania opłat przewidzianych w ustawie,
- podmiot nie wykonuje decyzji organu kontrolnego, dotyczącej nieprawidłowości w działaniu,
- nastąpiły zmiany struktury kapitałowej podmiotu z naruszeniem art. 19a ustawy o łączności,
- podjęto decyzję o likwidacji podmiotu posiadającego koncesję lub zezwolenie.

Minister Łączności może cofnąć koncesję lub zezwolenie jeżeli:

- podmiot nie rozpoczął działalności w oznaczonym terminie,

- ogłoszono upadłość podmiotu,
- nastąpiło przejęcie bezpośredniej lub pośredniej kontroli nad działalnością objętą koncesją lub zezwoleniem przez inną osobę.

Polityka udzielania koncesji i zezwoleń

Minister Łączności przyjął politykę w zakresie udzielania koncesji na świadczenie usług telekomunikacyjnych oraz zezwoleń na zakładanie i używanie urządzeń i sieci telekomunikacyjnych związanych z prowadzeniem działalności gospodarczej w dziedzinie telekomunikacji. Polityka ta została określona w kilku dokumentach rządowych zaakceptowanych przez Radę Ministrów. Podstawowe kierunki tej polityki są następujące:

- infrastruktura międzynarodowej sieci telefonicznej i telegraficznej będzie należała do TP SA i nie będą udzielane zezwolenia na zakładanie i używanie tej sieci;
- dominującym operatorem międzystrefowej sieci telefonicznej i usług telefonicznych w niej świadczonych będzie do końca 1999r. TP SA. Zezwolenia w powyższym zakresie będą udzielane w absolutnie wyjątkowych przypadkach tylko wówczas, gdy TP SA nie będzie w stanie w odpowiednio krótkim terminie dołączyć do swej sieci międzymiastowej sieci wewnątrzstrefowych innych operatorów;
- koncesje na świadczenie usług w sieciach telefonicznych użytku publicznego będą wydawane wraz z zezwoleniem na zakładanie i używanie tych sieci i będą obejmowały obszary docelowych stref numeracyjnych czyli województw w obecnym podziale administracyjnym kraju. W sieciach wewnątrzstrefowych powinni działać dwaj operatorzy tzn. TP SA i operator niezależny od TP SA. Wybór niezależnych operatorów tych sieci nastąpi w drodze przetargów;
- liczba koncesji na świadczenie usług niepowszechnych nie będzie ograniczana, a więc koncesje te będą wydawane bez przetargów, z wyjątkiem przypadków, gdy przyznanie koncesji jest związane z przyznaniem numeru sieci międzynarodowej lub przydziałem częstotliwości.

Koncesje i zezwolenia w dziedzinie teleinformatyki

Do 7 lipca ub.r., to znaczy do wejścia w życie ostatniej nowelizacji ustawy o łączności, Minister Łączności wydał 13 zezwoleń na świadczenie usługi polegającej na zapewnieniu użytkownikom sieci telekomunikacyjnych dostępu do sieci Internet (przed nowelizacją ustawy nie były wydawane koncesje i na świadczenie usług telekomunikacyjnych Minister Łączności wydawał zezwolenia).

Do końca kwietnia br. wydane zostały 44 koncesje na świadczenie usługi dostępu do sieci Internet za pośrednictwem sieci telekomunikacyjnych innych operatorów oraz 2 koncesje wraz z zezwoleniami dla operatorów sieci MAN we Wrocławiu i Krakowie. W najbliższym czasie zostanie wydanych dalszych kilkadziesiąt koncesji dla operatorów sieci Internet, zgodnie ze złożonymi w Ministerstwie Łączności wnioskami, a okres postępowania administracyjnego w sprawie wydania koncesji będzie, dla wnioskodawców spełniających wymogi ustawowe, ograniczony do minimum. Koncesje dla operatorów sieci Internet zawierają minimalną liczbę zobowiązań, a opłata koncesyjna wynosi w tym przypadku 200 ECU. Zgodnie z wcześniej omówioną polityką wydawania koncesji, Minister Łączności będzie udzielał koncesji w tym zakresie wszystkim wniskodawcom spełniającym wymagania określone w ustawie o łączności.

W najbliższym czasie zostaną również wydane koncesje wraz z zezwoleniami dla operatorów sieci MAN i także w tym obszarze nie przewiduje się ograniczania konkurencji.

WPŁYW PRACY PRZY MONITORACH EKRANOWYCH NA ZDROWIE LUDZKIE

Ryszard Pachecka

Wstęp

Powszechne stosowanie komputerów rodzi pytanie czy praca przy urządzeniach komputerowych, głównie przy monitorach ekranowych jest bezpieczna. W ostatnich kilkunastu latach ukazało się wiele opracowań na ten temat. Problem ten rozpatrywany jest w dwóch aspektach:
1. Wpływ czynników fizycznych związanych z pracującym urządzeniem komputerowym, głównie monitorem ekranowym na zdrowie ludzkie.
2. Wpływ obciążenia pracą przy monitorach ekranowych na stan zdrowia operatorów.

Emisja promieniowania przez monitory ekranowe

Monitory ekranowe działają na następujących układach:
1. Monitor ekranowy katodowy (kineskopowy) (ME-K) zawierający lampę katodową
2. Monitor płasko-ekranowy z układem ciekłych kryształów (ME-CK)
3. Monitor płasko-ekranowy z układem plazmowym (ME-P)
4. Monitor płasko-ekranowy z układem elektro-luminescencyjnym (ME-EL)

Monitory ekranowe katodowe (ME-K) stanowią, jak dotąd, większość wytwarzanych i stosowanych współcześnie monitorów ekranowych. Ze względu na swoją budowę i funkcję mogą być powodem zagrożeń fizycznych, jako że są źródłem:
- statycznych pól elektromagnetycznych o krańcowo małej częstotliwości
- pól magnetycznych o bardzo małej częstotliwości
- pola elektrostatycznego
- promieniowania X
- promieniowania widzialnego
- promieniowania nadfioletowego
- promieniowania podczerwonego
- tętnienia światła
- ultradźwięków
- polifenoli chlorowanych

Z badań Zakładu Zagrożeń Fizycznych Instutu Medycyny Pracy w Łodzi wynika, że natężenie czynników fizycznych w otoczeniu monitorów ekranowych nie przekraczają norm dopuszczalnych dla ogółu ludności, a często są niższe, co uwidacznia tabela zaczerpnięta z pracy Benneta.

Typ promieniowania	Promieniowanie emitowane przez monitory
gamma i rentgenowskie	0,06 wartości uznanej za bezpieczną
ultrafioletowe	0,001 wartości uznanej za bezpieczną
widzialne	0,001 wartości uznanej za bezpieczną
podczerwone	0,001 wartości uznanej za bezpieczną
mikrofalowe	0,000000000001 wartości uznanej za bezpieczną

Mikroklimat

Monitor ekranowy, jak i sam operator przy nim pracujący wytwarzają ciepło. Ilość ciepła wzrasta w miarę liczby pracujących urządzeń i osób w pomieszczeniu. Sytuacja taka bywa powodem instalowania urządzeń klimatyzacyjnych. Klimatyzacja w tych urządzeniach zmniejsza ciepło, ale powodować może przeciągi, źle tolerowane przez niektórych pracowników. Należy unikać szybkości powietrza wyższej od 0,1 m/sek. Uciążliwością pracy w pomieszczeniach, w których znajdują się monitory ekranowe jest zbyt suche powietrze. Jest ono odczuwane, jako bardziej suche, gdy jest w ruchu (klimatyzacja), niż gdy jest nieruchome. Wilgotność względna powietrza w tychże pomieszczeniach powinna wynosić 40-60 %.

Aspekty zdrowotne pracy przy monitorach ekranowych

Sformułowanie „praca przy monitorach" jest określeniem uproszczonym. Z praktyki wiadomo, że praca ta bywa bardzo różnorodna. Można wyróżnić dwa główne jej typy:
1. Wprowadzanie danych
2. Praca w dialogu z komputerem.

Przy pierwszym typie pracy dość ściśle jest określona pozycja ciała (siedząca), w tym tułowia, głowy i szyi. Jedna lub obydwie ręce są głównie na klawiaturze. Wzrok jest ufiksowany na dokumencie i z rzadka zatrzymuje się na ekranie. Praca jest monotonna. Obciążone są przede wszystkim: kręgosłup, mięśnie szyi i łopatek, a ponadto mięśnie kończyn górnych. Obciążony jest również narząd wzroku. Obciążenie wzroku jest spowodowane bardziej złą czytelnością dokumentów niż ekranem. Pomimo monotonii pracy, stawiane są wysokie wymagania w zakresie umiejętności przystosowania i oncentracji.

Przy pracy typu dialogowego urządzenie jest używane do wprowadzania danych i uzyskiwania danych. Wzrok jest bardziej intensywnie skierowany na urządzenie, a praca na klawiaturze jest bardziej ograniczona niż przy wyłącznym wprowadzaniu danych.Ponadto są zawsze do wykonania prace pomocnicze, jak wyszukiwanie danych w teczkach itp. lub uzyskiwanie informacji telefonicznych. Praca jest urozmaicona, wymaga umiejętności koncentracji, przystosowania i redagowania. Obciążenie wzroku związane z obserwacją ekranu jest większe niż przy wprowadzaniu danych, natomiast obciążenie związane z wymuszoną pozycją ciała jest mniejsze.

Dolegliwości zgłaszane przez operatorów monitorów ekranowych

Operatorzy monitorów ekranowych zgłaszają różne dolegliwości. Można je ująć w następujące grupy:
1. Dolegliwości ze strony narządu wzroku
2. Dolegliwości mięśniowo-szkieletowe
3. Problemy dotyczące ciąży
4. Zmiany chorobowe w obrębie skóry
5. Aspekty psychologiczne.

Ad1. Wpływ pracy przy monitorach ekranowych na narząd wzroku

Zagadnienie to należy rozpatrzyć w dwóch aspektach:
1. zmęczenie wzroku jako zespół subiektywnych objawów
2. zmiany w funkcji wzroku, które można wykazać obiektywnie.

Do najczęściej zgłaszanych dolegliwości należy: zamazanie i migotanie obrazu, osłabienie ostrości wzroku, podwójne widzenie, światłowstręt, ból oczu. Zmęczenie wzroku może być spowodowane następującymi przyczynami:
- zmęczenie jednego lub większej liczby systemów kontroli tzn ośrodka akomodacji, wergencji, równowagi mięśni ocznych, ruchów sakkadowych i ruchów podążania, kontroli odruchów źrenicznych oraz częstości mrugania,
- zmęczenia elementów biorących udział w procesie widzenia poczynając od siatkówki, poprzez nerw wzrokowy, ciała kolankowe boczne do kory prążkowanej,
- wpływ stanu ogólnego napięcia emocjonalnego i wytężonego wysiłku w czasie pracy przy monitorze ekranowym.

Wśród czynników sprzyjających wystąpieniu uczucia zmęczenia wzroku wyróżnia się czynniki zewnętrzne i wewnętrzne.

Do czynników zewnętrznych zalicza się warunki pracy i charakterystykę monitora, a wśród nich: nieprawidłowe warunki oświetlenia ogólnego w polu pracy wzrokowej, pulsujące źródło światła, tętnienie oraz pozytywność lub negatywność ekranu, niewłaściwa odległość oczu od monitora, dokumentacji czy też klawiatury, zbyt duże kontrasty jaskrawości powierzchni w otoczeniu.

Do czynników wewnętrznych należą: osobnicze cechy układu wzrokowego, jak niemiarowość oczu, zaburzenia akomodacji i konwergencji, zaburzenia widzenia obuocznego, czynne lub przebyte choroby oczu. W badaniu okulistycznym stwierdzić można zaburzenia różnych funkcji wzroku i tak:
- obniżenie ostrości wzroku
- osłabienie akomodacji

- oddalenie punktu bliży konwergencji
- zaburzenie równowagi mięśni ocznych
- zmiany akomodacji i konwergencji zależne od lokalizacji punktu ciemnego
- zmiany w zakresie ruchów sakkadowych oczu
- zmniejszenie częstości mrugania
- zmniejszenie wrażliwości na barwy (tzw. efekt McCollough)
- obniżenie krytycznej częstości migotania

Badaniem okulistycznym najczęściej stwierdza się przemijającą miopizację, skłonność do ezoforii do bliży, osłabienie akomodacji i oddalenie punktu konwergencji. Niektórzy badacze sugerowali, że praca przy monitorach może powodować jaskrę, makulopatię i zapalenie tęczówki, jednak późniejsze badania nie potwierdziły tych sugestii. Rozważano również możliwości wpływu pracy przy monitorze na powstawanie zaćmy i nabytej krótkowzroczności. Badania Bergquista i Scitecha oraz dane przytoczone przez Bolesławskiego nie potwierdziły tych poglądów.

Znawcy zagadnienia podkreślają, że wysiłek wzrokowy podczas pracy przy komputerze jest tak duży, że operatorzy nie są w stanie skompensować małych wad refrakcji, podczas gdy wady te podczas pracy o innym charakterze mogą być w ogóle nie spostrzegane.

W Polsce nie ma sformułowanych zaleceń dotyczących badań okulistycznych u operatorów monitorów ekranowych, natomiast są podane warunki ergonomiczne tej pracy. Dolegliwości ze strony narządu wzroku zgłasza 10 - 77 % pracowników.

Dla ograniczenia obciążeń wzroku zalecane są regulaminowo przerwy w pracy przy monitorach ekranowych z częstością zależną od stopnia obciążenia umysłowego i obciążenia wzroku. Przy dużych obciążeniach przerwy powinny mieć miejsce co 1 godzinę i trwać powinny 15 minut, a przy obciążeniach mniejszych przerwy o czasie 15 minut powinny być organizowane co 2 godziny. W czasie takich przerw operatorzy powinni przebywać w wydzielonym pomieszczeniu rekreacyjnym, zapewniającym odnowę i wypoczynek dla wzroku (wystrój o łagodnych barwach zielonych lub seledynowych, łagodne oświetlenie, wietrzenie).

Ad 2. Wpływ pracy przy monitorach ekranowych na układ mięśniowo-szkieletowy.

Dolegliwości układu mięśniowo-szkieletowego stwierdza się w każdej grupie pracowników biurowych, ale najczęściej występują one u operatorów komputerów wprowadzających dane. Dolegliwości bólowe dotyczą głównie barku i szyi oraz kończyn górnych, a ponadto okolicy krzyżowej i ud. Ponadto występują bóle i skurcze oraz utrata czucia w palcach rąk i w nadgarstkach.

Objawy spondyloartropatii stwierdza się niemal 2-krotnie częściej wśród operatorów urządzeń komputerowych niż w grupie kontrolnej. Uważa się, że główną przyczyną obciążenia operatora monitora ekranowego jest jego własne ciało i obciążenie statyczne. Należy tu wymienić:

- pasywną siedzącą pozycję ciała
- wymuszoną postawę ciała
- częste, powtarzane ruchy

Po kilku latach pracy przy komputerze może rozwinąć się przewlekła postać tzw. zespołu RSI (Repetitive Strain Injury), a więc choroba rąk i przedramion przejawiająca się m.in. zapaleniem pochewek ścięgnistych nadgarstków, czy też wystąpieniem tzw. "łokcia tenisisty". Dla zapobiegania powstawaniu tego typu zmian, czy też zmniejszenia nasilenia objawów zaburzeń są wymienione wyżej przerwy w pracy.

Operatorzy monitorów nie posiadają raczej wiedzy o właściwym użytkowaniu urządzeń, jak i o związkach między warunkami pracy a dolegliwościami. Tu właśnie jest rola ergonomisty, który nie tylko powinien zaprojektować poprawnie stanowisko pracy, ale powinien spowodować, aby użytkownik był w stanie korzystać z niego w świadomy, ergonomiczny sposób.

Ad 3. Problemy dotyczące ciąży.

Ukazało się wiele prac dotyczących wpływu pracy kobiet ciężarnych przy monitorach ekranowych na płodność, przebieg ciąży, wagę urodzeniową noworodków oraz występowanie wad wrodzonych. Ponieważ w niektórych tego typu pracach wykonanych w pierwszej fazie zainteresowania tym problemem stwierdzono większą częstość poronień samoistnych wśród kobiet-operatorów monitorów

ekranowych, przyjęto wstępnie koncepcję, że czynnikiem decydującym jest tu wpływ oddziaływań fizycznych monitora ekranowego, szczególnie gdy praca przy monitorze ekranowym trwa dłużej niż 15-21 godzin tygodniowo. Jednak późniejsze prace nie potwierdziły tej koncepcji. Badacze tego zagadnienia doszli do wniosku, że za zwiększoną ilość poronień u kobiet ciężarnych, za przedłużony okres oczekiwania na zajście w ciążę oraz za większą częstość wad wrodzonych u noworodków, których matki obsługują monitory ekranowe jest odpowiedzialny stres psychologiczny. Istnieje więc pewnego stopnia rozbieżność poglądów na to zagadnienie.
Departament Inspekcji Sanitarnej Ministerstwa Zdrowia i Opieki Społecznej zajął w 1984r. stanowisko w sprawie kobiet ciężarnych pracujących przy monitorach ekranowych, w myśl którego nie należy zatrudniać kobiet ciężarnych bezpośrednio przy monitorach ekranowych w całym okresie ciąży, a w pomieszczeniach z pojedynczymi monitorami ekranowymi mogą być zatrudnione kobiety ciężarne na stanowiskach pracy usytuowanych w odległości 1,5-2 m od tychże monitorów.
Z danych opublikowanych przez Międzynarodową Organizację Pracy w 1994r. dotyczących wpływu pracy przy monitorach ekranowych na ryzyko poronień samoistnych i powstawanie wad wrodzonych, a opartych o analizę około 126 000 kobiet ciężarnych pracujących przy monitorach ekranowych, tylko w jednej analizowanej podgrupie stanowiącej 1,26 % całości analizowanego materiału stwierdzono zwiększoną liczbę poronień i tylko w jednej (innej) podgrupie stanowiącej 1,15 % całości analizowanego materiału stwierdzono większą liczbę wad wrodzonych u noworodków.
Tak więc, jakkolwiek wpływ pracy przy monitorze ekranowym na przebieg ciąży i powstawanie wad wrodzonych u noworodków jest nadal otwarty i wymaga dalszych badań, to raczej sam fakt pracy kobiet ciężarnych przy tychże urządzeniach nie ma istotnego znaczenia. Jeżeli ten wpływ istnieje, to wynika on raczej ze stresu związanego z pracą, a nie jest spowodowany fizycznym zagrożeniem wynikającym z obsługi monitora ekranowego.

Ad 4. Zmiany chorobowe dotyczące skóry.

U operatorów monitorów ekranowych występować mogą zmiany na skórze, głównie w obrębie skóry twarzy, wyrażające się zaczerwienieniem i / lub grudkową wysypką, u niektórych pracowników zmiany skórne mają charakter łojotokowy. Zmiany te nie mają specyficznego charakteru; na podstawie badań bioptycznych skóry nie wykazano, aby te, które występują u operatorów monitorów ekranowych różniły się od takichże zmian występujących u osób nie pracujących przy monitorach. Przyczyny zmian skórnych występujących u operatorów monitorów ekranowych mogą być następujące:
- pole elektrostatyczne w otoczeniu operatora
- rozmaite cząstki w powietrzu w otoczeniu monitora i operatora (alergeny kontaktowe)
- czynniki klimatyczne w pomieszczeniach (wysoka temperatura, obniżona wilgotność powietrza)
będące przyczyną fizjologicznych reakcji naczynioruchowych
- stres jako przyczyna reakcji skórnych
- wtórna reakcja do natężenia wzroku
Według współczesnej wiedzy zmiany skórne występujące u operatorów monitorów ekranowych nie mają jednak udowodnionego związku z fizycznymi wpływami monitora ekranowego na ich powstawanie.

Ad 5. Aspekty psychologiczne, w tym stres psychologiczny, związane z pracą przy monitorach ekranowych.

Każda praca łączy w sobie elementy wysiłku fizycznego i umysłowego. Odnosi się to również do osób pracujących przy monitorach ekranowych. Z wysiłkiem umysłowym wiąże się konieczność odbierania informacji i ich przetwarzania, a także podejmowanie decyzji. Z wysiłkiem umysłowym związane jest również napięcie emocjonalne wiążące się z koniecznością podejmowania decyzji i poczuciem odpowiedzialności. W każdej pracy wystąpić mogą czynniki powodujące wzrost napięcia emocjonalnego, takie jak presja czasu i konfliktowe sytuacje.
Wiadomo, że koszt fizjologiczny wysiłku fizycznego zależy od jego intensywności, ale też od osobniczych możliwości. Podobną zależność stwierdzono dla wysiłku umysłowego - im bardziej jest intensywna praca umysłowa, tym wyższy jest jej koszt fizjologiczny. Im praca umysłowa jest łatwiejsza do wykonania, tym jej koszt fizjologiczny jest niższy. W obu więc sytuacjach fizjologiczny koszt pracy jest uzależniony od relacji między wymaganiami pracy, a możliwościami jej realizacji.

Od początkowego okresu zastosowania komputerów (lata czterdzieste) większość wysiłków ludzkich była skoncentrowana na tworzeniu sprzętu komputerowego, zespolonych systemów informacyjnych i uniwersalnych języków programowania. Komputery są używane przez ludzi, a zatem czynnik ludzki powinien być brany pod uwagę nie tylko w zakresie projektowania systemów komputerowych, języków programowania, ale i w zakresie wpływów psychologicznych, które w związku z obsługą komputera się pojawiają. W związku z powyższym wyłaniają się liczne problemy. Jednym z nich jest "obsesyjne" używanie komputerów, szczególnie w procesach programowania.
Problem "komputerowego narkomana" wiąże się nie tylko z tym, że człowiek taki może się "odciąć" od innych ludzi, ale i z tym, że może on widzieć swoje interakcje z komputerem "jako bardziej możliwe do przyjęcia" niż interakcje z ludźmi. To "uzależnienie" od komputera ma nie tylko naturę uzależnienia psychologicznego, ale wiąże się również z deformacją poczucia czasu. Za tym "uzależnieniem" od komputera i deformacją poczucia czasu idzie izolacja społeczna.
Praca przy komputerze może być powodem występowania zaburzeń emocjonalnych, które mogą wyrażać się jako zaburzenia nastroju, czasem przejawiają się pod postacią zaburzeń psychosomatycznych, a niekiedy przyjmują formę ogólnego niezadowolenia z pracy i warunków pracy.
Źródła tego dyskomfortu tkwią w:
– fizycznych warunkach pracy przy komputerze
– złych programach nie uwzględniających właściwości intelektualnych i percepcyjnych człowieka
– sposobie projektowania zadania
– konieczności znacznej koncentracji uwagi i wytrwałości
– różnicy w czasie reagowania pomiędzy elektronicznym komputerem a systemem nerwowym człowieka
– monotonii i fragmentaryczności niektórych zadań roboczych
– niepartycypowaniu w decyzjach dotyczących własnej pracy
– abstrakcyjności pracy
– awariach technicznych urządzeń komputerowych, a nawet w obawie o awarie systemu
– czasie reakcji systemu
– ograniczeniu kontaktów między ludźmi
Z powyższych danych wynika, że praca przy komputerze wiąże się z obciążeniem psychicznym.
Obciążenie może być różne.
Wyróżnia się:
a. obciążenie przeciętne - proste wprowadzanie danych do pamięci komputera
b. obciążenie duże - weryfikacja danych komputerowych i ich korekta
c. obciążenie bardzo duże - opracowywanie programów z bezpośrednim użyciem monitora
d. przeciążenie - jednoczesna łączność z komputerem (weryfikacja danych i ich korekta) i bezpośredni lub telefoniczny kontakt z interesantami
Z obciążeniem psychicznym wiąże się uczucie zmęczenia. Można wyróżnić 3 jego typy:
1. Uczucie senności i przytępienia
2. Trudności koncentracji uwagi
3. Uczucie dyskomfortu psychicznego
Pierwszy typ zmęczenia nie jest związany z typem pracy. Drugi typ zmęczenia dominuje wśród pracowników umysłowych, trzeci zaś typ u pracowników fizycznych. Czynniki wywołujące zmęczenie są lepiej poznane niż jego mechanizm. W mechanizmie zmęczenia odgrywa rolę m.in. zwiększenie metabolizmu, statyczne napięcie mięśniowe, rodzaj i stopień zaangażowania grup mięśniowych, powtarzalność ruchów w pracy monotypowej, jak również cechy środowiska pracy.
Ocena zmęczenia pracą przysparza wiele problemów, a dobór właściwych metod tej oceny budzi wiele wątpliwości i jest przedmiotem dyskusji. Poza metodami psychologicznymi stosowane są metody polegające na badaniu zużycia tlenu, pomiarze częstości akcji serca, pomiarze ciśnienia tętniczego, badaniu elektromyograficznym. Z obciążeniem psychicznym wiąże się występowanie chorób, w etiopatogenezie których czynnik emocjonalny odgrywa istotną rolę. Są to choroby z kręgu chorób psychosomatycznych. Wymienić tu należy: nadciśnienie tętnicze, chorobę niedokrwienną serca z jej szczególnym etapem, jakim jest zawał serca, zaburzenia rytmu serca, zaburzenia czynności przewodu pokarmowego, a przede wszystkim wrzód trawienny, głównie wrzód dwunastnicy, a ponadto zespół jelita drażliwego.
Literatura (83 pozycje): u autora.

ZASADY WSPÓŁPRACY I ROZLICZEŃ MIĘDZY OPERATORAMI TELEKOMUNIKACYJNYMI

Jerzy Gospodarek

Katedra Prawa Gospodarczego, Szkoła Główna Handlowa
02-554 Warszawa, Al. Niepodległości 162

1. Uwagi ogólne

Budowa i używanie sieci komputerowych oraz świadczenie usług w tych sieciach wymaga spojrzenia z punktu widzenia obowiązującego prawa na zasady współpracy i rozliczeń operatorów sieci komputerowych z innymi operatorami telekomunikacyjnymi. Podstawy tej współpracy są przesądzone ustaleniami ustawy z dnia 23 listopada 1990 r. o łączności, znowelizowanej w 1995 r. /tekst jednolity Dz. U. z 1995 r. Nr 117, poz. 564/. Drugim aktem normatywnym wymagającym uwzględnienia w tej analizie jest rozporządzenie Ministra Łączności z dnia 26 października 1995 r. w sprawie ogólnych warunków przyłączania sieci telekomunikacyjnych oraz zasad rozliczeń /Dz. U. Nr 127, poz. 608/, dalej powoływane jako rozporządzenie w sprawie o.w.p. Jest to akt o charakterze wykonawczym, wydany na podstawie art. 38 ust. 2 wymienionej ustawy. Inny charakter mają dwie decyzje Ministra Łączności z dnia 2 kwietnia 1996 r.: decyzja nr 8 w sprawie ustalania szczegółowych warunków współpracy i rozliczeń między operatorami telekomunikacyjnymi lub użytkownikami sieci oraz decyzja nr 9 w sprawie trybu rozpatrywania wniosków o ustalenie warunków współpracy i rozliczeń pomiędzy operatorami telekomunikacyjnymi lub użytkownikami sieci telekomunikacyjnych. Decyzje te powoływane dalej jako decyzja nr 8 i decyzja nr 9 podlegają opublikowaniu w Dzienniku Urzędowym Ministerstwa Łączności, co w chwili pisania tego referatu jeszcze nie zostało zrealizowane.

Należy zauważyć, że wymienione akty prawne wprowadzają ustalenia odnoszące się do wszystkich operatorów telekomunikacyjnych i nie przewidujące jakichś specjalnych rozwiązań prawnych dla operatorów sieci komputerowych. Wydaje się, że jest kwestią najbliższego czasu wprowadzenie do obowiązującego prawa pewnych specyficznych regulacji odnoszących się tylko do operatorów sieci komputerowych oraz usług świadczonych w tych sieciach. Może to nastąpić w przyszłej ustawie o telekomunikacji, nad której projektem prace w Ministerstwie Łączności już się rozpoczęły zgodnie z rezolucją Sejmu z dnia 21 kwietnia 1995 r. w sprawie rozwoju rynku usług telekomunikacyjnych /Mon. Pol. Nr 23, poz. 272/. Rezolucja ta podkreśliła znaczenie telekomunikacyjnych usług dodanych oraz potrzebę roztrzygnięcia zasad koordynacji rozwoju telekomunikacji, w tym teleinformatyki i usług multimedialnych, w opracowanym przez rząd dokumencie "Polityka rozwoju telekomunikacji". Dokument ten właśnie został przesłany do Sejmu i jego ustalenia są przedmiotem odrębnego referatu.

Przyszła ustawa o telekomunikacji nie ma jeszcze dokładnie wyznaczonego zakresu. Zgłaszane są różne propozycje założeń do tych nowych regulacji ustawowych.1/ Nie powinno w nich zabraknąć specyficznej problematyki sieci komputerowych oraz usług multimedialnych.

2. Umowy jako podstawa współpracy i rozliczeń między operatorami telekomunikacyjnymi

Zgodnie z art. 38 ust. 3 ustawy o łączności warunki współpracy między operatorami są ustalane w drodze umów. Zawarcie tych umów przez operatorów następuje na zasadach ustalonych w prawie cywilnym. Jedną z tych zasad jest swoboda umów. Zgodnie z art. 353 kodeksu cywilnego strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości /naturze/ stosunku, ustawie ani zasadom współżycia społecznego. W szczególności umowa nie może więc być sprzeczna z bezwzględnie obowiązującymi normami prawnymi. Tego rodzaju normy dominują w ustawie o łączności oraz wydanych na jej podstawie aktach wykonawczych.

Wśród warunków ustalanych w analizowanej umowie o współpracy między operatorami ustawa o łączności w art. 38 ust. 3 wymienia warunki przyłączenia ich sieci oraz szczegółowe warunki rozliczeń. Nie są to oczwiście jedyne kwestie, które mogą być objęte taką mową. Powinna ona ponadto określać m.in. zasady współdziałania stron w zakresie niezbędnej przebudowy sieci w związku z przyłączeniem oraz warunki współpracy w zakresie przekazywania informacji związanych z wykonywaniem danej umowy.2/

Kwestii treści umowy o współpracy między operatorami dotyczy wyżej powołana decyzja nr 8. Jako podstawa prawna wydania tej decyzji został powołany art. 4 ust. 1 pkt 3 ustawy z dnia 1 grudnia 1989 r. o utworzeniu urzędu Ministra Łączności /Dz. U. Nr 67, poz. 408 ze zmianami/. Stanowi to - delikatnie mówiąc - nieporozumienie, jako że wskazany przepis kompetencyjny mówi o wykonywaniu zadań przez Ministra Łączności w szczególności przez "tworzenie warunków oraz inicjowanie przdsięwzięć ekonomiczno-finansowych, organizacyjnych i technicznych w celu zapewnienia sprawnego funkcjonowania systemów łączności telekomunikacyjnej i pocztowej, a także ich nowoczesnego rozwoju dla efektywnej obsługi gospodarki i społeczeństwa". Są to sformułowania prawne ustalające ogólne warunki przyłączania sieci telekomunikacyjnych oraz zasady rozliczeń mają nadany w omawianym rozporządzeniu charakter bezwzględnie obowiązujący. Jedynie w kwestii obowiązków związanych z doprowadzeniem linii łączących sieć użytku publicznego do innych sieci telekomunikacyjnych oraz z rozbudową istniejącej sieci telekomunikacyjnej użytku publicznego niezbędną dla wnioskowanego przyłączenia innej sieci par. 4 ust. 6 tego rozporządzenia dopuszcza umowne uzgodnienie przez operatorów innych warunków niż normatywnie ustalone tym aktem. W tym więc zakresie można mówić o dyspozytywnym charakterze norm analizowanego aktu wykonawczego ale też nie bez zastrzeżeń, skoro takie ustalenia umowne nie mogą naruszać bliżej nie określonych przepisów prawa ani pogarszać - również nie sprecyzowanych - możliwości korzystania z usług telekomunikacyjnych przez abonentów połączonych sieci. Trudno oprzeć się wrażeniu, że są to zastrzeżenia uczynione na pokaz.

3. Charakter i zakres ustaleń rozporządzenia w sprawie o.w.p.

Analizowane rozporządzenie odnosi się tylko do sytuacji przyłączenia sieci telekomunikacyjnej do sieci telekomunikacyjnej użytku publicznego. Akt ten nie obejmuje natomiast przypadków przyłączania sieci telekomunikacyjnej do sieci wydzielonej czy wewnętrznej. Takie rozwiązanie wynika z ustalenia art. 38 ust. 1 ustawy o łączności, które zobowiązuje tylko operatorów sieci telekomunikacyjnych użytku publicznego do dokonania przyłączenia do swojej sieci każdej innej sieci telekomunikacyjnej wybudowanej zgodnie z przepisami. Zobowiązanie to nie obejmuje więc operatorów sieci wydzielonych i wewnętrznych.3/

Najważniejszą zasadą omawianego rozporządzenia jest ustalenie par. 3 ust. 1 o obowiązku zapewnienia przez operatora sieci telekomunikacyjnej użytku publicznego równoprawnych warunków przyłączania innych sieci. Powinno to wykluczać sytuacje preferencyjnego lub dyskryminującego traktowania w tym zakresie poszczególnych operatorów. Drugim wartym podkreślenia ustaleniem tego aktu normatywnego jest określenie w par. 4 ust. 1, jakie wymagania powinien spełniać wniosek uprawnionego podmiotu o przyłączenie jego sieci. Jeżeli będzie to wniosek pisemny zawierający dane techniczne dotyczące styku między sieciami, rodzajów usług i przewidywanego ruchu oraz propozycje co do wnioskowanego miejsca, sposobu i terminu przyłączenia sieci, to operator sieci telekomunikacyjnej użytku publicznego nie będzie mógł żądać żadnych innych dodatkowych dokumentów i informacji - poza dokumentem stwierdzającym uprawnienie podmiotu do prowadzenia działalności w dziedzinie telekomunikacji, o ile zresztą w danym wypadku takie uprawnienie jest wymagane.

Trzecią istotną sprawą jest nałożenie - w par. 4 ust. 2 rozporządzenia w sprawie o.w.p. - na operatora sieci telekomunikacyjnej użytku publicznego obowiązku ustosunkowania się do złożonego wniosku przez określenie miejsca i terminu przyłączenia, wymaganych parametrów technicznych oraz protokołów komunikacyjnych i synchronizacyjnych. Niestety,

niedotrzymanie tego terminu nie pociąga za sobą żadnych konsekwencji prawnych, co niewątpliwie jest słabym punktem analizowanego rozporządzenia.

Można mieć wątpliwości, czy na plus tego rozporządzenia trzeba zapisać odwołanie się w par. 4 ust. 3 w kwestii wyznaczania miejsca przyłączenia sieci do przesłanki racjonalności techniczno-ekonomicznej tworzonego układu sieci. To bowiem, co jest racjonalne od strony technicznej, wcale nie musi być tak samo ocenione od strony ekonomicznej, na odwrót zresztą też.

Tylko pozornie mniej wątpliwości wywołują ustalenia rozporządzenia w sprawie o.w.p. w kwestii rozliczeń między operatorami. Słuszna jest zawarta w par. 7 ust. 1 zasada równoprawnego traktowania w tym zakresie wszystkich podmiotów. To samo można powiedzieć o obowiązku wprowadzonym w par. 7 ust. 4 uznania jako podstawy rozliczeń wskazań urządzeń rejestrujących ruch telekomunikacyjny. Trudno jednak zaprzeczyć, że to wszystko nie wystarczy Ministrowi Łączności do obiektywnego rozstrzygnięcia sporu między operatorami, jeśli nie dają oni do porozumienia w sprawie sposobu ustalania wzajemnych należności. Trzeba tu zaznaczyć, że omawiane rozporządzenie w najmniejszym stopniu nie okazało się przydatne przy rozwiązywaniu problemów powstałych pod koniec ubiegłego roku w związku z nowym cennikiem usług INTERNETU świadczonych przez NASK, chociaż zgodnie z par. 1 tego aktu miał on określić zasady rozliczeń nie tylko między samymi operatorami, ale także między operatorami a użytkownikami sieci.4/

4. Zasady i tryb rozstrzygania przez Ministra Łączności sporów między operatorami w sprawie warunków współpracy i rozliczeń

Przeciągające się spory między TP S.A. a innymi operatorami co do warunków współpracy i rozliczeń skłoniły ustawodawcę do przyznania Ministrowi Łączności - w art. 38 ust. 4 znowelizowanej w 1995 r. ustawy o łączności - kompetencji do wydawania decyzji w tych sprawach. Taka decyzja administracyjna ma rodzić skutki cywilnoprawne i zastępować w całości lub w części umowę stron, jeśli negocjacje okażą się bezskuteczne. Skorzystanie przez Ministra Łączności z tych kompetencji typu sądowego jest uzależnione od złożenia w danej sprawie wniosku przez jedną ze stron sporu oraz upływu 3 miesięcy negocjacji liczonych od daty złożenia wniosku o przyłączenie do sieci telekomunikacyjnej użytku publicznego. 5/

Powyższe rozwiązanie prawne jest dalekie od doskonałości już choćby dlatego, że Minister Łączności jest zarazem reprezentantem Skarbu Państwa w TP S.A., która jest jedną ze stron w tego typu sporach. W pewnym stopniu zapobiegać preferowaniu interesów TP S.A. w tej sytuacji ma wymaganie art. 38 ust. 5 ustawy o łączności, by taka decyzja była wydana po zasięgnięciu opinii Prezesa Urzędu Antymonopolowego.6/ Choć opinia ta nie jest wiążąca, to ważne znaczenie ma tutaj możliwość wszczęcia przez Urząd Antymonopolowy postępowania antymonopolowego.7/

Ustawa o łączności nie określiła trybu składania i rozpatrywania przez Ministra Łączności wniosków o ustalenie warunków współpracy i rozliczeń między operatorami sieci telekomunikacyjnych. Sam wymieniony minister dokonał tych ustaleń w powołanej wyżej decyzji nr 9, a ściślej w załączniku do tej decyzji, która bez żadnego uzasadnienia powołuje jako swą podstawę cytowany już art. 4 ust. 1 pkt 3 ustawy o utworzeniu urzędu Ministra Łączności, jak również art. 38 ust. 4 ustawy o łączności. Ten ostatni przepis prawny także nie upoważnia Ministra Łączności do wydania tego typu aktu prawnego.

Inkryminowana decyzja nr 9 jest nie tylko pozbawiona podstawy prawnej, ale w istocie też zupełnie zbędna, gdyż załącznik do niej określa przede wszystkim wewnętrzny tryb postępowania w Ministerstwie Łączności przy rozpatrywaniu sporu co do warunków współpracy jak z innej epoki, a co więcej, nie upoważniają one Ministra Łączności do wydawania żadnych aktów prawnych. Świadomość tego stanu rzeczyspowodowała, że decyzji nr 8 został nadany charakter jedynie zalecenia i nie ma ona mocy powszechnie obowiązującej, choć powołuje się ponadto na swe powiązania z rozporządzeniem w sprawie o.w.p. Ustalenia zawarte w decyzji nr 8 powinny znaleźć się właśnie w tym rozporządzeniu i wtedy sytuacja

prawna byłaby zupełnie inna. W Ministerstwie Łączności mówi się o odpowiedniej zmianie wskazanego rozporządzenia, ale wymaga to uzgodnień międzyresortowych i musi potrwać.

Z powyższymi zastrzeżeniami podchodząc do zaleceń decyzji nr 8, należy zauważyć, że sprowadzają się one w większości do generalnie słusznych, trudnych do kwestionowania zasad, choć ich sformułowania nie zawsze są najszczęśliwsze. Można to powiedzieć o zaleceniach, by operatorzy:

- kierowali się dążeniem do zapewnienia wspólnych korzyści i należytych dochodów każdej ze stron z tytułu wspólnie realizowanych usług telekomunikacyjnych;
- uwzględniali wysokość nakładów inwestycyjnych już poniesionych i planowanych do poniesienia przez operatora sieci przyłączonej;
- opierali rozliczenia na dążeniu do zapewnienia operatorowi sieci przyłączanej zwrotu uzasadnionych kosztów oraz osiągnięcia uzasadnionego zysku;
- nie wiązali rozliczeń z wysokością pobieranych przez siebie opłat taryfowych;
- przymowali za podstawę rozliczeń wskazania urządzeń telekomunikacyjnych rejestrujących wspólnie realizowany ruch telekomunikacyjny.

Natomiast trudno zrozumieć, jakie wnioski Minister Łączności chciałby wyciągać z nieuwzględnienia zalecenia, by operatorzy ustanawiali stałych pełnomocników prowadzących negocjacje w sprawie umowy o współpracy i rozliczeniach. Niewątpliwie powołanie takich pełnomocników może ułatwić i przyspieszyć kontakty między zainteresowanymi stronami, ale tego typu kwestie techniczno-organizacyjne powinni dowolnie przesądzać sami operatorzy. Można to też powiedzieć o kolejnym zaleceniu decyzji nr 8, by operatorzy w dążeniu do zawarcia umowy o współpracy i rozliczeniach wykorzystywali "wszelkie dostępne środki i metody, w tym - opinie ekspertów lub arbitrów". Nie chodzi tutaj zapewne o opinie arbitrów lecz o powoływanie ich przez negocjujące strony w celu roztrzygnięcia spornych kwestii. Trudno także zaprzeczyć, iż raczej nigdy nie da się wykorzystać wszystkich dostępnych środków i metod, zwłaszcza że kolejna opinia czy ekspertyza może okazać się diametralnie różna od poprzedniej.

5. Wnioski końcowe

W świetle dokonanych analiz należy stwierdzić, że ustawowe regulacje problematyki zasad współpracy i rozliczeń między operatorami telekomunikacyjnymi są niepełne i nie mogą usatysfakcjonować. Z kolei rozporządzenie w sprawie o.w.p. pozbawione jest w większości ustaleń, które mogłyby być podstawą prawną rozstrzygania przez Ministra Łączności sporów co do warunków współpracy i rozliczeń między operatorami. Natomiast obydwie wyżej omówione decyzje Ministra Łączności nie zasługują nawet na podsumowanie, skoro w świetle obowiązujcego prawa nie mają one mocy prawnej.

Przypisy:

1/ Zob. J. Gospodarek: Ustawa o telekomunikacji. Propozycje podstawowych założeń do nowych regulacji ustawowych w dziedzinie telekomunikacji, TELEINFO nr 9/1996 r., s. 13.
2/ Zob. S. Piątek, L. Stępniak: Prawo telekomunikacyjne. Komentarz do ustawy o łączności, Warszawa 1995, s. 159.
3/ Tamże, s. 1.57.
4/ Por. Raport końcowy Zespołu Ekspertów KBN d/s Internetu w Polsce, Warszawa, styczeń 1996.
5/ Zob. S.Piątek, L. Stępniak: op.cit., s. 159.
6/ Zob. J. Gospodarek: Legal Grounds for Investment in Polish Telecommunications, Polish Investment Market, nr 3/1996, s. 14.
7/ S. Piątek, L. Stępniak: op. cit., s. 160 - 161.

OCHRONA PRAWNA DANYCH I SYSTEMÓW KOMPUTEROWYCH - - WYBRANE ZAGADNIENIA

mgr inż. Małgorzata Skórzewska-Amberg

Instytut Matematyki, Politechnika Warszawska, Plac Politechniki 1

I. Ochrona danych gromadzonych na nośnikach cyfrowych oraz ochrona obiegu informacji w systemie połączeń komputerowych jest realizowana środkami przede wszystkim o charakterze technicznym ale coraz częściej i na coraz większą skalę także środkami organizacyjnymi i prawem.

Szczególną rolę odgrywa ochrona danych i szeroko pojętych systemów komputerowych na gruncie prawa administracyjnego, cywilnego i karnego.

Funkcję ochronną pełni przede wszystkim prawo autorskie - ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych (Dz.U. Nr 24, poz. 83). Zgodnie z postanowieniami ratyfikowanego w 1994 roku Układu Europejskiego ustanawiającego stowarzyszenie między Rzecząpospolitą Polską z jednej strony a Wspólnotami Europejskimi i ich państwami członkowskimi z drugiej strony (Dz.U. z 1994 roku, Nr 11, poz. 38) Polska zobowiązała się do dalszego doskonalenia ochrony praw własności intelektualnej, przemysłowej i handlowej oraz przystąpienia do wielostronnych konwencji o ochronie tego rodzaju dóbr.

W pewnym stopniu rozwiązania prawa autorskiego uzupełniane są prawem o wynalazczości - ustawa z dnia 19 października 1972 roku oraz prawa o znakach towarowych - ustawa z dnia 31 stycznia 1985 roku.

Tam gdzie nadużycie przybiera postać przestępstwa stosowane jest prawo karne, zaś wywołane szkody mogą być dochodzone w oparciu o prawo cywilne.

Przedmiotem niniejszych rozważań są podstawowe rozwiązania w tym zakresie zawarte w Kodeksie karnym i Kodeksie cywilnym oraz uregulowania będące przedmiotem prac parlamentarnych w związku ze skierowaniem do Sejmu projektu nowego Kodeksu karnego.

II. Najwcześniej, bo w latach 1973-1974, sformułowano na gruncie europejskim zasady, które winny być stosowane w regulacjach prawnych dotyczących przechowywania informacji osobowych w elektronicznych bankach danych. Zasady te zostały zawarte w przygotowanych przez Komitet Ministrów Rady Europy rezolucjach o ochronie danych osobowych w sektorze prywatnym[1] (1973 rok) i sektorze publicznym[2] (1974 rok).

W 1981 roku Rada Europy przyjęła konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych o charakterze osobowym.

Dalsze prace nad problematyką przestępczości komputerowej doprowadziły do powołania, w 1985 roku, Komisji Ekspertów do spraw przestępczości komputerowej. Rezultatem prac Komisji był projekt zalecenia, przyjęty w 1989 roku, Komitetu Ministrów Rady Europy[3], dotyczący przestępstw związanych z użyciem komputera. Dokument ten zawiera wskazania legislacyjne dla rządów krajów członkowskich, dotyczące zmian ustawodawczych oraz zakresu kryminalizacji zachowań przestępczych z wykorzystaniem komputera. W efekcie sporów w łonie samej komisji "co do potrzeby posługiwania się represją karną wobec wszystkich zdefiniowanych form zachowań"[4], zachowania przestępne zostały skatalogowane na dwóch listach: pierwszej (tzw. lista minimalna), zawierającej wedle opinii Komitetu Ekspertów czyny wymagające kryminalizacji we wszystkich krajach członkow-

[1] Rezolucja Rady Europy (73)22
[2] Rezolucja Rady Europy (74)29
[3] Zalecenie Rady Europy R(89)9
[4] Przestępczość komputerowa, Poznań 1994 r., wyd. Towarzystwo Naukowe Organizacji i Kierownictwa "Dom Organizatora", TNOiK Toruń, s. 143

skich[5], a co za tym idzie ścisłej współpracy międzynarodowej pociągającej za sobą harmonizację ustawodawstw krajowych w zakresie ścigania przestępczości transgranicznej, oraz drugiej (tzw. lista fakultatywna), obejmującej zachowania o mniejszym stopniu szkodliwości i nie wymagające ścisłej współpracy międzynarodowej w zakresie ich ścigania i jurysdykcji[6].

Lista minimalna obejmuje następujące zachowania:

- oszustwo komputerowe,

  Oszustwo komputerowe dokonywane jest najczęściej w jednej z następujących form:
  - manipulacja danymi (*input manipulation*),
  - manipulacja programem (*software manipulation*),
  - manipulacja wynikiem (*output manipulation*).
- fałszerstwo komputerowe,
- niszczenie danych lub programów komputerowych,
- sabotaż komputerowy,

  Działania prowadzące najczęściej do sparaliżowania funkcjonowania systemu komputerowego przez wymazywanie lub wprowadzanie zmian w systemie danych albo przez fałszowanie jego działania.
- nieuprawnione wejście do systemu,
- nieuprawnione przechwycenie informacji - podsłuch komputerowy,
- bezprawne kopiowanie, rozpowszechnianie lub publikowanie programów komputerowych prawnie chronionych,
- bezprawne kopiowanie topografii półprzewodników[7].

Lista fakultatywna (opcjonalna) obejmuje natomiast:

- modyfikację danych lub programów komputerowych,
- szpiegostwo komputerowe (szpiegostwo przemysłowe obejmujące *hardware* i *software*),
- używanie komputera bez zezwolenia,
- używanie prawnie chronionego programu komputerowego bez upoważnienia.

W ostatnim czasie w wykonaniu decyzji Europejskiej Komisji do Spraw Problemów Przestępczości, podjęto prace nad przygotowaniem Europejskiej Konwencji w sprawie Przestępstw Komputerowych, regulującej "karnomaterialne, karnoprocesowe i międzynarodowe aspekty przestępstw popełnianych z wykorzystaniem komputerów"[8].

Na początku lat dziewięćdziesiątych Organizacja Narodów Zjednoczonych uznała nadużycia komputerowe za jedną z form przestępczości transgranicznej i jako takie stały się one przedmiotem badań prowadzonych z inicjatywy ONZ[9], a dotyczących przestępczości zorganizowanej. Jednym z efektów tych badań było stwierdzenie zaskująco niskiego poziomu ujawniania przestępstw przeciwko systemom komputerowym lub z wykorzystaniem komputera - rzędu od 1 do 5 %. Przyczyny takiego stanu rzeczy mogą być następujące:

- brak ogólnego porozumienia co do formalnoprawnej definicji zachowania przestępnego,
- brak ogólnego porozumienia co do typów zachowań, uznawanych za przestępne,
- brak specjalistów w dziedzinie przestępstw komputerowych w policji, prokuraturze i sądach,
- nierównowaga zdolności prawnej organów ścigania i wymiaru sprawiedliwości poszczególnych krajów, do podejmowania czynności procesowych związanych z dostępem do systemów komputerowych i zabezpieczeniem danych komputerowych jako materiału dowodowego,
- niedostosowanie w poszczególnych krajach przepisów proceduralnych, związanych ze ściganiem przestępstw komputerowych,

[5] Przestępczość komputerowa, j.w., s. 153
[6] Przestępczość komputerowa, j.w., s.153
[7] Przestępczość komputerowa, j.w., s. 144
[8] Przestępczość komputerowa, j.w., s.104
[9] rezolucja Rady Społeczno-Gospodarczej 1992/22

- brak umów ekstradycyjnych i o wzajemnej pomocy prawnej oraz zsynchronizowanego mechanizmu międzynarodowej współpracy w zakresie ścigania przestępstw komputerowych[10].

III. Na gruncie europejskim, krajem, w którym dokonano całościowej regulacji ustawowej spraw związanych z przestępczością komputerową, według wskazań Komisji Ekspertów Rady Europy, jest Francja[11].

Pojawienie się przestępczości komputerowej we Francji to połowa lat siedemdziesiątych, a więc okres kiedy nie tylko we Francji, ale również w innych krajach europejskich, nie istnieje odrębne ustawodawstwo regulujące kwestie przestępstw popełnianych z wykorzystaniem komputera. Dopiero w 1978 roku pojawił się pierwszy specjalistyczny akt prawny - ustawa "Informatyka i wolności". Ustawa ta zapewniając pierwszeństwo "ochronie ludzi przed informatyką" staje w obronie utrzymania wolności osobistych i ochrony życia prywatnego.

Ustawa stanowi przede wszystkim o ochronie danych osobowych, formułuje ściśle określone zasady dotyczace gromadzenia, rejestrowania, przechowywania i wykorzystywania informacji imiennych o osobach fizycznych, zakazując jednocześnie gromadzenia i przechowywania informacji mogących być podstawą jakiejkolwiek dyskryminacji, a więc na temat "rasy, przynależności politycznej, religijnej i związkowej, a także karalności". Zapewnia gwarancje prawne dla osób rejestrowanych, w postaci:

- prawa do sprzeciwu wobec przetwarzania dotyczących ich informacji,
- prawa do znajomości treści dotyczących ich informacji,
- prawa do prostowania informacji imiennych.

W celu zapewnienia kontroli i nadzoru nad wypełnianie postanowień ustawy, powołano jako organ kontrolny, niezależny urząd administracyjny z prawem wydawania rozporządzeń - Państwową Komisję Informatyki i Wolności.

Ustawa "Informatyka i wolności" nie tylko więc wprowadza zakaz tworzenia nielegalnych kartotek osobowych, ale stawia też warunki dotyczące automatycznego przetwarzania danych osobowych, przewidując w każdym wypadku dla takiego przetwarzania, albo wymóg zgłoszenia do Państwowej Komisji Informatyki i Wolności zamiaru przetwarzania danych osobowych (w sektorze prywatnym), albo wręcz konieczność wydania ustawy lub innego aktu prawnego na podstawie opinii Państwowej Komisji Informatyki i Wolności (w sektorze publicznym).

Kolejnym specjalistycznym aktem w dziedzinie *ius informationis* we Francji była ustawa z 1985 roku o ochronie praw autorskich. Ustawa precyzuje, że "osoba działająca na własny rachunek jest właścicielem praw do programu, który sama opracowała, natomiast prawa do programu opracowanego w trakcie wykonywania funkcji zawodowych należą - w braku odmiennego postanowienia - do pracodawcy". Okres ochrony autorskiej wynosi 50 lat.

Swoje miejsce w systemie prawa francuskiego mają również dyrektywy Unii Europejskiej (1991 rok) o ochronie prawnej programów komputerowych, szczególnie w zakresie definiowania nowego rodzaju przestępstw, a mianowicie:

- nieuprawnionego odtwarzania programu komputerowego,
- dekompilacji programu w celu jego przetłumaczenia, dostosowania lub poprawienia,
- wprowadzania programu do obrotu.

W 1988 roku powstała tzw. ustawa Godfraina o fałszerstwach komputerowych. Ustawa definiuje automatyczny system przetwarzania danych jako "zespół składający się z jednej lub więcej jednostek przetwarzania pamięci, oprogramowania, urządzeń wejścia-wyjścia lub łącz, które współ-

[10] Sławomir Redo, *Prevention and Control of Computer Related Crime from the United Nations Perspective*, Przestępczość komputerowa, j.w., s.75-76

[11] Marcel Vigouroux, *Przepisy prawne dotyczace przestępstw komputerowych we* Francji, Przestępczość komputerowa, j.w., s. 119-126

działają dla uzyskania określonego skutku, przy czym zespół ten chroniony jest urządzeniami zabezpieczającymi" i zapewnia ochronę tego systemu poprzez "zwalczanie nielegalnego dostępu do systemu oraz nielegalnego posiadania części, bądź całego systemu automatycznego przetwarzania danych", penalizuje sabotaż i oszustwo komputerowe, wprowadza pojęcie " porozumienia przestępczego w celu popełnienia oszustwa komputerowego". Przepisy tej ustawy zostały zmodyfikowane (głównie przez zaostrzenie represji) przez Kodeks własności intelektualnej z 1992 roku i ustawę z 1994 roku.

Powyższe przepisy zostały recypowane przez nowy kodeks karny z 1994 roku.

W Wielkiej Brytanii jednym z podstawowych aktów umożliwiających ściganie przestępstw dokonywanych z wykorzystaniem komputera jest Prawo o Ochronie Danych (*Data Protection Act*). Prawo o Ochronie Danych opiera się na następujących zasadach:

- informacje dotyczące danych osobowych będą pozyskiwane i przetwarzane uczciwie i zgodnie z prawem,
- dane osobowe będą przechowywane tylko w konkretnie określonych i zgodnych z prawem celach,
- dane osobiste przechowywane w określonym celu nie będą używane lub ujawniane w jakikolwiek sposób niezgodny z tym celem,
- dane osobiste przechowywane w określonym celu będą szczegółowe na tyle, na ile takich szczegółów wymaga cel, w jakim są przechowywane,
- dane osobiste będą dokładne oraz uaktualniane tam, gdzie jest to konieczne,
- każda osoba będzie miała:
  - prawo do poprawienia lub wymazania tych danych,
  - w odpowiednich okresach, bez nieuzasadnionego opóźnienia i nieodpłatnie prawo do informacji od każdego użytkownika danych, czy przechowuje on jej dane osobowe
  - w odpowiednich okresach, bez nieuzasadnionego opóźnienia i nieodpłatnie dostęp do każdego typu danych o sobie, przechowywanych przez firmy korzystające z własnych baz danych.

Zgodnie z tym prawem każdy posiadający np.: listy adresowe, powinien się zarejestrować, zaś każdy użytkownik tych danych, tzn. osoba sprawująca nadzór nad zawartością i wykorzystywaniem danych osobistych przechowywanych w systemie komputerowym, jest odpowiedzialny za ich zabezpieczenie i wprowadzenie środków gwarantujących kontrolę dostępu do bazy.

Użytkownicy baz danych winni także zabezpieczyć dostęp do budynków i pomieszczeń, w których znajdują się komputery, podjęte środki powinny także zabezpieczać przed kradzieżą, pożarem oraz inną klęską, powstała z przyczyn naturalnych[12].

Inną istotną ustawą jest prawo z 1990 roku o nadużyciach komputerowych. Ustawa ta wyróżnia trzy typy przestępstw popełnianych z wykorzystaniem komputera:

- niedozwolone wejście do systemu, w tym włamanie (orzekają Sądy Rozjemcze, najniższa karalność),
- niedozwolone wejście do systemu z zamiarem popełnienia na zlecenie przestępstwa w rodzaju oszustwa lub kradzieży, lub pomagania w wykonaniu takiego zlecenia (orzekają Sądy Koronne),
- dokonywanie niedozwolonych zmian w danych komputerowych, włączając użycie wirusów i bomb logicznych (orzekają Sądy Koronne)[13].

Ustawa o nadużyciach komputerowych jest pierwszym szczególnym aktem prawnym w Zjednoczonym Królestwie (jurysdykcja ustawy rozciąga się na teren całego Zjednoczonego Królestwa) skierowanym przeciwko przestępcom komputerowym, i jako taki wyznacza kierunek dalszych zmian ustawodawczych.

---

[12] *Prawo o ochronie* danych, opr. Przemysław Pawełczyk, Computerland, numer z 4 maja 1992 roku

[13] Noel Bończoszek, *Wykrywanie przestępstw komputerowych w Zjednoczonym Królestwie*, Przestępczość komputerowa, j.w., s. 107-108

IV. W systemie polskiego prawa brak jest odrębnych (za wyjątkiem prawa autorskiego) przepisów regulujących odpowiedzialność za szkody wyrządzone przez czyny przestępne, dokonywane z wykorzystaniem komputera. W tej sytuacji osoby za dokonanie takich czynów odpowiedzialne mogą być ukarane jedynie w oparciu o ogólne przepisy prawa.

1. Przepisy Kodeksu karnego powstały w czasie (1969 rok), gdy zagadnienia przestępczości związanej z systemami kompterowymi nie wymagały szczegółowej regulacji, stąd też brak przepisów odnoszących się wprost do tej sfery przestępczości. Brak odrębnej dyspozycji nie wyłącza jednak odpowiedzialności karnej.

W trakcie międzynarodowej konferencji naukowej na temat prawnych aspektów nadużyć popełnionych z wykorzystaniem nowoczesnych technologii przetwarzania informacji, która miała miejsce w 1994 roku w Polsce, podkreślono, że wśród nadużyć związanych z systemem komputerowym, które można określić mianem zachowań przestępnych, wyróżnia się przede wszystkim działania dotyczące:

- prawidłowego obiegu informacji komputerowej, tzn. czyny godzące bezpośrednio w oprogramowanie, system i przechowywane dane,
- uprawnień do programów komputerowych, tzn. naruszenia praw autorskich do programu komputerowego oraz związanych z tym praw pokrewnych (przestępne naruszanie praw autorów, producentów i użytkowników oprogramowania).

Obecnie, pod względem prawnym, wyróżnia się zachowania karalne, w których:

- informatyka jest narzędziem przestępstwa, czyny przestępne mają najczęściej charakter ekonomiczny (np.: oszustwa) lub osobowy (np.: nielegalne tworzenie kartotek osobowych),
- informatyka jest przedmiotem przestępstwa, np.: kradzież programów komputerowych[14].

W prawie karnym, zgodnie z art. 120 § 1 kk, przez czyn zabroniony rozumie się każde działanie lub zaniechanie o znamionach określonych w ustawie karnej. Podstawą odpowiedzialności karnej za czyn, określony jako zabroniony , jest wina sprawcy. Mówiąc o winie należy uwzględnić zarówno jej element obiektywny, obejmujący każde zachowanie się niezgodne z przepisami prawa, jak i subiektywny, czyli umyślność lub nieumyślność popełnionego czynu. Zaznaczyć przy tym trzeba, iż niezależnie od tego czy sprawca działał umyślnie, w zamiarze bezpośrednim (chce popełnić czyn zabroniony) lub ewentualnym (przewiduje możliwość popełnienia czynu zabronionego i na to się godzi), czy też wskutek lekkomyślności (przewiduje możliwość popełnienia czynu zabronionego lecz bezpodstawnie przypuszcza, że tego czynu uniknie) lub niedbalstwa (nie przewiduje możliwości popełnienia czynu zabronionego, choć powinien i mógł ją przewidzieć) wina pozostaje, kwestią otwartą jest natomiast jej stopień.

Odpowiedzialność karną można ponosić nie tylko za samo dokonanie czynu zabronionego np.: zniszczenie danych czy rozpowszechnianie wirusów, lecz także za współsprawstwo, pomocnictwo i podżeganie do tego rodzaju działań.

W określonych prawem sytuacjach mają zastosowanie przepisy dotyczące przestępstw przeciwko wolności (art. 172 kk), przestępstw przeciwko mieniu (art. 212 kk), przestępstw przeciwko tajemnicy państwowej i służbowej (art. 260 k.k) oraz przestępstw przeciwko dokumentom (art. 265-268 kk).

Przepis art 172 kk chroni tajemnicę korespondencji i wiadomości uzyskanych środkami telekomunikacji. Przestępstwo z art. 172 § 1 kk może być popełnione tylko przez działanie, tzn.:

- otwarcie zamkniętego pisma nie przeznaczonego dla sprawcy,
- ukrycie lub zniszczenie cudzej korespondencji zanim adresat się z nią zapoznał,
- przyłączenie się do przewodu służącego do podawania wiadomości,
- podstępne uzyskanie wiadomości nie przeznaczonej dla sprawcy, nadanej przy użyciu środków telekomunikacji.

[14] Przestępczość komputerowa, j.w., s.18

Otwarcie zamkniętego pisma, ukrycie lub zniszczenie korespondencji, muszą nastąpić zanim adresat zapoznał się z treścią korespondencji. Tylko wtedy działanie takie jest przestępstwem z art. 172 kk, działanie późniejsze może być występkiem z art. 268 kk.

Przestępstwo z art. 172 kk dokonuje się z chwilą, gdy sprawca dopuścił sie jednego z wyżej wymienionych działań, np.: otwarcia listu. Tak więc przyłączenie się do przewodu będzie przestępstwem popełnionym z chwilą takiego działania sprawcy.

Dla dokonania przestępstwa z art. 172 § 1 kk nie jest wymagane aby sprawca zapoznał się z treścią korenpondecji, rozmowy czy przesyłanych informacji.

Odpowiedzialność karna z art. 172 kk następuje, gdy sprawca działał umyślnie. Ściganie, za wyjątkiem czynu dotyczącego korespondencji lub wiadomości przeznaczonej dla instytucji państwowej lub społecznej (ściganie z oskarżenia publicznego) odbywa się z oskarżenia prywatnego.

Przepis art. 212 k.k chroni własność i posiadanie mienia przed zniszczeniem, uszkodzeniem lub uczynieniem niezdatnym do użytku. Niszczenie mienia polega na jego unicestwieniu, uszkodzenie zaś na takiej zmianie materii rzeczy, że nie może ona służyć celom, do których była przeznaczona. Czynienie mienia niezdatnym do użytku obejmuje takie przypadki, gdy mienie wprawdzie nie zostało zniszczone ani uszkodzone lecz pomimo tego stało się niezdatne do użytku.

W naszym przypadku mieniem będą oczywiście posiadane i przechowywane w systemie informacje, a także sprzęt - niejednokrotnie wielkiej wartości.

Przestępstwo z art. 212 kk dokonuje się z chwilą wywołania skutku, np.: zniszczenia sprzętu.

Odpowiedzialność karna z art. 212 kk następuje, gdy sprawca działał umyślnie, przy czym zgodnie z art. 212 § 3 kk, jeśli czyn nie dotyczy mienia społecznego, ściganie przestępstwa następuje na wniosek pokrzywdzonego.

Nieumyślność działania sprawcy powoduje wyłącznie odpowiedzialność cywilną.

Przepis art. 260 kk chroni tajemnicę państwową przed jej ujawnieniem osobom nieuprawnionym. Ujawnienie wiadomości stanowiącej tajemnicę państwową, to udostępnienie jej osobom nieuprawnionym, przy czym obojętny jest sposób jej ujawnienia. Może się to odbyć np.: za pomocą ustnej wypowiedzi np.: podanie hasła, jeśli takie jest zabezpieczenie dostępu w komputerze.

Tajemnicą jest to, o czym informacja (o czymkolwiek, o jakiejkolwiek okoliczności) nie powinna dojść do osób niepowołanych. Bez znaczenia jest czy mamy do czynienia z tajemnicą w znaczeniu materialnym (ze względu na treść i znaczenie) czy też tajemnicą w znaczeniu fromalnym (tzn. ze względu na wolę utajnienia wiadomości przez tych, którzy ją znają).

Przestępstwo z art. 260 kk zostaje dokonane z chwilą ujawnienia wiadomości, a więc z chwilą udostępnienia zapoznania się z nią przez osoby nieuprawnione. Przestępstwo może popełnić zarówno osoba uprawniona do posiadania tajnej informacji, przez ujawnienie jej wobec osób nieuprawnionych, jak i osoba nieuprawniona, która ujawniła wiadomość wobec siebie samego lub też innej osoby.

Odpowiedzialność karna sprawcy z art. 260 kk następuje gdy sprawca działał umyślnie. Nieumyślne ujawnienie tajemnicy państwowej spenalizowane jest jedynie w odniesieniu do osoby będącej pracownikiem instytucji państwowej lub społecznej "jako jedynego uprawnionego nosiciela takiej tajemnicy" (art. 260 § 3 kk).

Przepisy dotyczące przestępstw przeciwko dokumentom chronią pewność oborotu (a nie same dokumenty), która opiera się na zaufaniu do dokumentu. Zamach na dobro prawne związane z dokumentem może polegać na:

- fałszerstwie dokumentu (materialnym - art. 265 kk "kto w celu użycia za autentyczny podrabia lub przerabia dokument albo takiego dokumentu używa" lub intelektualnym: bezpośrednim - art. 266 lub pośrednim - art 267 kk),
- zniszczeniu, uszkodzeniu itp. dokumentu (art. 268 k.k " kto niszczy, uszkadza, ukrywa lub usuwa dokument, którym nie ma prawa wyłącznie rozporządzać).

Odpowiedzialność karna z art. 265-268 następuje, gdy sprawca działał umyślnie, przy czym

przestępstwo z art. 266 kk jest przestępstwem indywidualnym, gdyż jego sprawcą może być tylko określona osoba (funkcjonariusz publiczny lub inna osoba upoważniona do wystawienia dokumentu).

Z punktu widzenia odpowiedzialności za czyn istotne jest ustalenie, czy sprawca dokonał czy też usiłował dokonać czynu zabronionego.

W myśl art. 11 kk za usiłowanie odpowiada sprawca, który w zamiarze popełnienia czynu zabronionego, zachowaniem swym zmierza bezpośrednio ku jego dokonaniu, które jednak nie następuje.

Problemem otwartym pozostaje ustalenie momentu dokonania czynu. O ile niewątpliwy wydaje się moment dokonania czynu w sytuacji np.: włamania się do sieci teleinformatycznej, czy też fizycznego uszkodzenia sprzętu, to już w sytuacji niszczenia informacji np.: przez wprowadzenie do systemu wirusa, ta chwila nie jest już tak jednoznaczna. W świetle obowiązującego prawa dokonanie czynu następuje w chwili uszkodzenia lub zniszczenia informacji, słuszny jednak wydaje się pogląd, aby w przyszłości, zgodnie z rozwiązaniem brytyjskim, karac już za samo naruszenie systemu (np.: przez włamanie lub wprowadzenie wirusa), tę właśnie chwilę przyjmując za moment dokonania czynu.

O usiłowaniu przestępstwa mówimy, gdy nie nastapiło jeszcze dokonanie wszystkich czynności niezbędnych do wywołania zamierzonego skutku, ale sprawca podjął już działania bezpośrednio zmierzające do dokonania tego czynu. Na przykład wprowadził wirusa do systemu, wirus zagnieździł się powodując powstanie programu - nosiciela, ale pomimo fizycznej obecności wirusa w systemie, informacje pozostały nie zmienione.

Nieistotne jest czy sprawca uświadamia sobie czy też nie, możność lub niemożność dokonania czynu ze względu na brak przedmiotu nadającego sie do dokonania lub ze względu na użycie środka nie nadającego się do wywołania zamierzonego skutku.

Jeżeli sprawca dąży do zniszczenia informacji za pomocą wirusa, ale nie uświadamia sobie, że sposób w jaki to czyni nie może doprowadzić do dokonania czynu (brak wirusa na dyskietce używanej do zakażenia, nieszkodliwość wirusa etc.) również ponosi odpowiedzialność za usiłowanie dokonania czynu zabronionego.

Za usiłowanie popełnienia przestępstwa wymierzana jest kara w granicach takich samych jak za dokonanie przestępstwa. Jeżeli usiłowanie jest nieudolne, sąd może nadzwyczjanie złagodzić karę lub też jej nie wymierzać.

Jeżeli sprawca zamierzał dokonać czynu zabronionego np.: wprowadzenia wirusa do systemu i w trakcie swego działania dobrowolnie odstąpił od tego zamiaru np.: poprzez zneutralizowanie wirusa przed jego zagnieżdżeniem, wówczas w myśl art. 13 § 1 kk nie ponosi kary, chyba że jego zachowanie, oprócz znamion nie podlegającego karze usiłowania jednego przestępstwa, wyczerpuje ponadto znamiona innego przestępstwa. Jeżeli z własnej woli usiłował zapobiec skutkowi przestępnemu i nie udało mu się (art. 13 § 2 kk), wówczas sąd może zastosować nadzwyczajne złagodzenie kary.

Przygotowanie, tzn. działanie sprawcy w celu popełnienia przestępstwa, polegające na gromadzeniu środków, informacji, sporządzaniu planów popełnienia przestepstwa etc., do popełnienia czynów określonych w art. 212, 172, 266-268 kk nie jest karalne. Karalne jest natomiast przygotowanie do przestępstwa z art. 261 § 1 tzn. do fałszerstwa dokumentów.

Zgodnie z art. 16 kk za sprawstwo, tzn. dokonanie czynu odpowiada nie tylko ten, kto dokonuje czynu sam lub z kimś innym, ale także ten, kto kieruje wykonaniem przez inną osobę czynu zabronionego.

Mamy tu do czynienia z dwoma różnymi pojęciami: współsprawstwa i sprawstwa pośredniego (sprawstwa kierowniczego).

Współsprawstwo ma miejsce wtedy, gdy czynu dokonują wspólnie dwie lub więcej osób, np.: poprzez podział zadań - część osób tworzy kod wirusa, część go wprowadza do systemu. Każdy ze współsprawców odpowiada za swój czyn tak jak sprawca indywidualny.

Jeżeli dwie lub więcej osób jednocześnie, ale niezależnie od siebie i bez świadomości tej jednoczesności, wprowadzi wirusa do systemu, mamy wówczas do czynienia z tzw. sprawstwem równoległym. Odpowiedzialność ponosi każdy ze sprawców tak jak sprawca indywidualny.

Ze sprawstwem pośrednim mamy do czynienia, gdy sprawca "używa" do popełnienia czynu pośrednika. Przykładem sprawstwa pośredniego może być następująca sytuacja: sprawca dąży do

wprowadzenia wirusa do systemu i urzeczywistnia swój cel dając zarażoną dyskietkę innej osobie, która, niekoniecznie świadoma zawartości dyskietki, wprowadza wirusa do systemu. Sprawca jest w tym wypadku sprawcą pośrednim i odpowiada karnie niezależnie od tego czy bezpośredni wykonawca także podlega takiej odpowiedzialności.

Jeżeli ktoś chce urzeczywistnić znamiona czynu zabronionego (uszkodzenie mienia przez wprowadzenie wirusa) przez wzbudzenie u innej osoby woli popełnienia tego czynu, to zgodnie z art. 18 § 1 kk jest podżegaczem. Niekiedy pewne zachowanie może zrodzić u sprawcy zamiar popełnienia przestępstwa (np.: opowiadanie o niewykrywalnym wirusie, o słabych zabezpieczeniach jakiegoś systemu), a mimo to nie stanowi podżegania, a więc nie rodzi odpowiedzialności karnej, jeżeli nie było podjęte z zamiarem nakłonienia do popełnienia czynu zabronionego.

Jeżeli ktoś chce aby inna osoba dokonała czynu zabronionego albo godzi się na to i ułatwia popełnienie tego czynu, to w myśl art. 18 § 2 kk odpowiada za pomocnictwo. Jeżeli jednak ktoś np.: udziela informacji na temat budowy i działania wirusów, dostarcza literatuty fachowej, i czyni to nie w zamiarze udzielenia sprawcy pomocy dokonania czynu zabronionego, nie jest on pomocnikiem sprawcy, natomiast zachowanie takie jest nieumyślnym przyczynieneim się do popełnienia przestępstwa i jako takie nie jest karane.

Pomocnictwo może być także zrealizowane przez zaniechanie np.: osoba która jest szczególnie zobowiązana do ochrony informacji zawartych w systemie nie zabezpiecza systemu w sposób w jaki zobowiązana jest to zrobić, również odpowiada za pomocnictwo.

Niezależnie od tego czy sprawca czynu zabronionego dokonał tego czynu lub czy nie ponosi za niego odpowiedzialności, podżegacz i pomocnik, zgodnie z art. 19 § 1 kk, odpowiadają w granicach swego zamiaru, tzn. jeżeli podżegacz lub pomocnik chcieli aby informacje zostały zniszczone, zaś sprawca wprawdzie usiłował popełnić czyn zabroniony i w tym celu wprowadził wirusa do systemu, ale zniszczył go zanim ten wyrządził szkodę, wówczas sprawca będzie odpowiadał w myśl art. 13 § 1 kk, ale podżegacz lub pomocnik będą odpowiadać tak, jakby sprawca dokonał czynu polegającego na zniszczeniu danych za pomocą wirusa.

Czasami bardzo trudno jest rozróżnić pomocnictwo od współsprawstwa, przy czym istotą sporu nierzadko są szczegóły. Mocno upraszczając można powiedzieć, że współsprawstwo zachodzi wtedy, gdy osoba działająca identyfikuje się z czynem, zaś pomocnictwo, gdy osoba, chcąc dopomóc do dokonania czynu zabronionego, uznaje go jednak za cudze przedsięwzięcie.

Zgodnie z art. 20 § 1 kk za podżeganie lub pomocnictwo wymierzana jest kara w granicach takich samych jak za dokonanie przestępstwa. Jeżeli nie usiłowano dokonać czynu zabronionego, to zgodnie z art. 20 § 2 kk sąd w stosunku do podżegacza lub pomocnika może zastosować nadzwyczajne złagodzenie kary lub też odstąpić od jej wymierzenia.

Jeżeli osoba, która podżegała lub pomagała w dokonaniu czynu zabronionego, dobrowolnie zapobiegnie dokonaniu czynu (art. 21 § 1 kk), wówczas nie podlega karze. Jeżeli zaś osoba ta usiłuje zapobiec dokonaniu czynu, ale jej się to nie udaje, wówczas sąd może zastosować nadzwyczajne złagodzenie kary (art. 21 § 2 kk).

Jeżeli ktoś nakłania inną osobę do popełnienia czynu zabronionego, po to, aby osoba ta poniosła odpowiedzialność karną (prowokacja), wówczas wobec osoby nakłaniającej, instytucja czynnego żalu nie ma zastosowania (art. 21 § 3 kk).

Karalność przestępstwa ustaje, jeżeli od czasu jego popełnienia upłynęło lat 20 - gdy czyn stanowi zbrodnię (dolna granica kary - 3 lata); 10 - gdy czyn stanowi występek zagrożony karą pozbawienia wolności przekraczającą lat 5; 5 - gdy chodzi o pozostałe występki. Zgodnie z art. 105 § 1 kk karalność czynu wyczerpującego znamiona przestępstwa, np.: z art. 212 & 1 kk, ustanie z upływem lat pięciu, a z art. 260 & 2 kk po upływie lat dziesięciu, natomiast gdy przestępstwo ścigane jest z oskarżenia prywatnego, jego karalność ustaje z upływem 3 miesięcy od czasu, gdy pokrzywdzony dowiedział się o osobie sprawcy przestępstwa, nie później jednak, niż z upływem 5 lat od czasu jego popełnienia. Ten przepis znajduje zastosowanie np.: w przypadku art. 172 kk, jeśli korespondencja lub wiadomość nie jest przeznaczona dla instytucji państwowej lub publicznej.

2. Trzeba jeszcze wymienić przewidujące odpowiedzialność karną przepisy prawa autorskiego - ustawa z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych. Artykuły od 115 do

119 tej ustawy regulują odpowiedzialność za przywłaszczenie autorstwa, rozpowszechnianie cudzego utworu bez nazwiska twórcy lub bez uprawnienia, utrwalanie bez uprawnienia lub wbrew jego warunkom oraz paserstwo przedmiotu będącego nośnikiem utworu, a także uniemożliwienie lub utrudnienie wykonywania prawa do kontroli korzystania z utworu.

V. Nowe typy przestępstw związanych z rozwojem nowoczesnej techniki cyfrowej zawiera projekt Kodeksu karnego, przygotowany przez Komisję do Spraw Reformy Prawa Karnego.

Projekt ten został przyjęty przez Rząd i skierowany pod obrady Parlamentu. Obecnie po pierwszym czytaniu w Sejmie, projekt jest przedmiotem prac specjalnie powołanej Komisji Nadzwyczajnej.

Przepisy dotyczące przestępczości komputerowej, oprócz przepisów w zbliżonej fromie istniejących obecnie, rozmieszczone zostały w kilku rozdziałach projektu, zależnie od przedmiotu ochrony, m.in.: w rozdziale dotyczącym przestępstw przeciwko ochronie informacji (art. 269-271 projektu), przestępstw przeciwko wiarygodności dokumentów (art. 272, 278 projektu) czy przestępstw przeciwko mieniu (art. 287 projektu).

Przedmiotem ochrony tajemnicy (w tym tajemnicy korespondencji) jest wyraźnie wymienione bezprawne pozyskiwanie informacji uzyskane przez przełamanie elektronicznego, magnetycznego lub innego szczególnego zabezpieczenia wiadomości. Ochrony tej dotyczy także przepis "typizujący zachowanie polegające na zakładaniu lub posługiwaniu się urządzeniem podsłuchowym, wizualnym lub innym urządzeniem specjalnym w celu uzyskania cudzej informacji bez uprawnienia"[15] (art. 269,270).

W tym samym rozdziale projektu, art. 267 i 268 przewidują odpowiedzialność osób, które wbrew przepisom ujawniają cudzą tajemnicę, z którą zapoznały się podczas wykonywania obowiązków zawodowych, działalności publicznej, społecznej, gospodarczej lub naukowej. Przepis ten ma szczególne znaczenie w sytuacji, gdy większość danych opracowań i innych informacji dotyczących osoby lub jej działalności znajduje się w komputerowych bazach danych, a co za tym idzie wymaga szczególnej ochrony prawnej.

Odrębny typ przestępstwa dotyczy "zakłócenia lub uniemożliwienia gromadzenia lub przekazywania informacji o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowania administracji państwowej przez niszczenie zapisu informacji na nośniku komputerowym, ich uszkodzenia lub zmiany, niszczenie nośnika tej informacji lub jego wymianę albo też niszczenie urządzenia służącego automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji, które jest nazywane sabotażem komputerowym" (art. 271).

W przestępstwach przeciwko mieniu przewidziana jest odpowiedzialność karna osoby, która w celu osiągnięcia korzyści majątkowej przez ukształtowanie programu komputerowego, włączanie do pamięci komputera niewłaściwych lub niepełnych informacji albo przez inne oddziaływanie na przetwarzanie informacji wpływają na wynik opracowania i powodują szkodę majątkową innej osobie (art. 287) oraz dla osoby która niszczy, uszkadza lub czyni niezdatnym do użytku cudzy zapis magnetyczny lub elektroniczny lub bez upoważnienia zmienia jego treść (oszustwo komputerowe).

Art. 280 § 2 projektu, w tym samym rozdziale, w odniesieniu do tego, co potocznie nazywa się kradzieżą programu komputerowego, wprowadza nowy typ przestępstwa "zbliżony do kradzieży", jako że czyn taki "nie polega na zaborze rzeczy (informacja nie jest rzeczą)" ani też "zabór" nie pozbawia osoby uprawnionej dalszego dysponowania programem, zatem "chodzi tu nie tylko o uzyskanie programu od jego autora, a więc uzyskanie dyspozycji osobistymi prawami autorskimi, lecz raczej innej osoby uprawnionej, dysponującej materialnymi prawami związanymi z danym programem".

Również skierowany do Sejmu projekt Kodeksu postępowania karnego pośrednio dotyka sfery informatyki, mianowicie w przepisach rozdziału dotyczącego kontroli i utrwalania rozmów (art. 233-238 projektu).

Niekiedy w celu wykrycia, uzyskania dowodów lub zapobieżenia dokonaniu najpoważniejszych przestępstw konieczne jest zastosowanie podsłuchu telefonicznego. Działanie takie jest ściśle

[15] Uzasadnienie projektu Kodeksu karnego, skierowanego przez Rząd pod obrady Sejmu, s. 96 i następne

opisane i poddane szczególnym rygorom ze względu na jego ingerencję w "sferę osobistą człowieka i naruszenie prawnie chronionej tajemnicy komunikowania się"[16]. Projekt ogranicza dopuszczalność kontroli i utrwalania rozmów telefonicznych do enumeratywnie wyliczonych w art. 233 § 3 rodzajów przestępstw, zastrzega konieczność wszczęcia postępowania karnego w jednym z wymienionych przestępstw (art. 233 § 1), decyzję o dopuszczeniu podsłuchu (na wniosek prokuratora) pozostawiając sądowi (art. 233 § 1). Jedynie w wypadkach nie cierpiących zwłoki dopuszczona jest możliwość zastosowania kontroli wprost przez prokuratora, jednakże z obowiązkiem uzyskania w ciągu pięciu dni zatwierdzenia tej decyzji przez sąd (art. 233 § 2). Ustawowo ograniczone są także "krąg osób, w stosunku do których można tę kontrolę wprowadzić (art. 233 § 4) oraz czas jej trwania (art. 234)".

Art. 237 projektu, przewidując - na powyższych zasadach - dopuszczalność kontroli i utrwalania przy użyciu środków technicznych treści przekazów informacji innych niż rozmowy telefoniczne, przewiduje możliwość posługiwania się podsłuchem komputerowym w postępowaniu karnym.

VI. Nadużycia związane z użyciem komputerów mogą prowadzić również do wywołania szkody, co będzie powodowało odpowiedzialność cywilną.

W myśl art. 23 Kodeksu cywilnego, niezależnie od ochrony przewidzianej w innych przepisach, prawo cywilne chroni dobra osobiste człowieka, w szczególności zdrowie, wolność, cześć, nazwisko, tajemnicę korespondencji, twórczość naukową itd. Odpowiedzialność za szkodę powstałą w wyniku naruszenia dóbr osobistych uregulowana jest w art. 448 kc. W myśl tego przepisu w razie umyślnego naruszenia dóbr osobistych poszkodowany może żądać, niezależnie od środków potrzebnych do usunięcia skutków wyrządzonej szkody, ażeby jej sprawca uiścił pewną sumę pieniężną na rzecz Polskiego Czerwonego Krzyża. Zmiana Kodeksu cywilnego, uchwalona przez Sejm w ostatnim czasie, będąca jeszcze przedmiotem dalszych prac ustawodawczych, przewiduje rozszerzenie przesłanek tej odpowiedzialności (wprowadza obok umyślnego naruszenia dóbr także wywołane rażącym niedbalstwem), jak również możliwość przyznania świadczeń osobie pokrzywdzonej.

Rozważmy sytuację, gdy zostanie złamane zabezpieczenie wiadomości pozostawionej w komputerze dla określonego adresata (np. list w poczcie elektronicznej). Wiadomość taką można potraktować jako zamknięte pismo, a uzyskanie do niej dostępu przez osobę trzecią, zanim z jej treścią zapoznał się adresat, jako przestępstwo z art. 172 § 1 kk. W takim przypadku poszkodowany oprócz ukarania sprawcy zgodnie z przepisami art. 172 kk może domagać się odszkodowania w procesie cywilnym.

Przepisy art. 24 kc stanowią, że osoba, której dobro osobiste zostaje zagrożone bezprawnym cudzym działaniem może żądać zaprzestania tego działania, a jeżeli naruszenie zostało dokonane może żądać usunięcia jego skutków, dodatkowo zaś jeżeli wyrządzona została szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.

Zastanówmy się nad przypadkiem wirusa. Wprowadzenie wirusa do systemu może spowodować uszkodzenie lub całkowite zniszczenie danych i programów komputerowych,a w niektórych wypadkach również sprzętu komputerowego. W związku z tym w stosunku do osoby, która spowodowała szkodę, znajdują zastosowanie przepisy prawa zobowiązań, dotyczące odpowiedzialności za czyny niedozwolone (art. 415 kc).

W prawie cywilnym przez czyn niedozwolony rozumie się każde zdarzenie wyrządzające szkodę, a więc takie, w którym sprawca (odpowiedzialny za szkodę) narusza nakaz lub zakaz obowiązujący go, niezależnie od istniejącego między nim a poszkodowanym stosunku zobowiązaniowego.

Art. 415 kc stanowi, iż każdy kto ze swej winy wyrządził drugiemu szkodę, szkodę tę musi naprawić. Podstawą odpowiedzialności sprawcy szkody jest wina, czyli ujemna ocena zachowania się sprawcy (lub osoby odpowiedzialnej za szkodę). Wina stanowi połączenie elementu obiektywnego, który wypełnia każde zachowanie się niezgodne z przepisami prawa podmiotowego, i subiektywnego, polegającego na winie umyślnej lub na niedbalstwie, przy czym sprawca szkody odpowiada przy każdym stopniu winy.

[16] Uzasadnienie projektu Kodeksu postępowania karnego, s. 29 i następne

Na art. 415 kc można również oprzeć roszczenia o naruszenie dobra osobistego, jeżeli wskutek tego naruszenia zostanie wyrządzona szkoda majątkowa. Niebezpieczeństwo naruszenia niektórych dóbr osobistych ze sfery życia prywatnego, przede wszystkim zaś informacji personalnych, zaistniało z chwilą stworzenia możliwości niezgodnego z ich przeznaczeniem wykorzystywania informacji z różnego rodzaju banków danych.

Jeżeli osoba, która wyrządziła szkodę jest funkcjonariuszem państwowym (np.: w powiązaniu z art. 260 § 3 kk) lub też organem osoby prawnej, wówczas kwestia odpowiedzialności normowana jest oddzielnymi przepisami. Jeżeli odpowiedzialnym za szkodę jest organ osoby prawnej wówczas odpowiedzialność za szkodę, zgodnie z art. 416 kc, ponosi ta osoba prawna.

Osobami prawnymi są Skarb Państwa i jednostki organizacyjne, którym przepisy szczególne przyznają osobowość prawną (np.: banki, spółki, stowarzyszenia,szkoły wyższe, instytuty naukowo-badawcze).

Osoba prawna ponosi odpowiedzialność za szkodę wyrządzoną czynem niedozwolonym swojego organu, jeżeli organ działał w granicach swoich kompetencji, wynikających ze statutu lub innych przepisów. Przekroczenie tych granic i działanie jedynie w celu osobistym, nie związanym z zakresem zadań osoby prawnej, wyłącza jej odpowiedzialność z art. 416 kc. Winę organu jednoosobowego ocenia się tak jak osoby fizycznej. Dla ustalenia winy organu nieosobowego, kolegialnego, należy stwierdzić czy naruszony został konkretny nakaz lub zakaz zawarty w obowiązujących przepisach.

Art. 417 kc jest podstawą odpowiedzialności Skarbu Państwa w każdym wypadku szkody wyrządzonej z winy funkcjonariusza państwowego przy wykonywaniu powierzonej mu czynności (np.: art. 260 § 3 kk). Przez funkcjonariuszy państwowych rozumie się pracowników organów władzy, administracji lub gospodarki państwowej oraz osoby działające na zlecenie tych organów, osoby powołane z wyboru, sędziów, prokuratorów oraz żołnierzy Sił Zbrojnych. W myśl art. 420 kc, jeżeli szkoda została wyrządzona przez funkcjonariusza państwowego osoby prawnej, to odpowiedzialność za szkodę, zamiast Skarbu Państwa, ponosi ta osoba prawna.

Zgodnie z art. 422 kc winy dopuszcza się również ten, kto świadomie korzysta z wyrządzonej szkody, chociażby sam nie miał nawet pośredniego udziału w jej wyrządzeniu. Odpowiedzialność za korzystanie ze szkody jest uzasadniona korzyścią świadomie osiągniętą z tej szkody, przy czym korzystającym może być osoba prawna lub fizyczna. Do przyjęcia odpowiedzialności podżegacza lub pomocnika konieczne jest stwierdzenie, ze istnieje związek przyczynowy pomiędzy ich zachowaniem się a zaistniałą szkodą. Nie można zatem w myśl cytowanego artykułu przypisać odpowiedzialności osobie, która pomogła sprawcy ukryć szkodę już wyrządzoną, jeżeli przed jej wyrządzeniem osoba ta nie zobowiązała się wobec sprawcy szkody do takiej pomocy. Osoba taka może ponosić odpowiedzialność z mocy art. 415 kc jedynie za szkodę pozostającą w związku przyczynowym z jej działaniem.

Odpowiedzialność za wyrządzone szkody, w myśl art. 429 kc ponosi również ten, kto zlecił sprawcy wykonanie czynności, chyba że nie ponosi winy w wyborze albo powierzy wykonanie czynności, która trudni się wykonywaniem takich właśnie czynności.

Powierzający czynność musi zatem wykazać, że wyboru dokonał z należytą starannością i nie dopuścił się winy w wyborze. Z założenia przyjmuje się, że wybór jst prawidłowy, jeżeli wykonanie czynności zostało powierzone osobie lub istytucji trudniącej się zawodowo wykonywaniem takich czynności. Odpowiedzialność powierzającego wykonanie czynności opiera się na jego winie, obojętne jest więc czy można przypisać winę samemu sprawcy. Odpowiedzialność za winę w wyborze zachodzi wówczas, gdy osoba której powierzono wykonanie czynności jest samodzielna, tj. nie pozostaje wobec zamawiającego w stosunku podwładności. Podobnie osoba, która na własny rachunek powierza wykonanie czynności innej osobie, podległej zleceniodawcy i zobowiązanej stosować się przy wykonywaniu czynności do jego wskazówek, w myśl art. 430 kc ponosi odpowiedzialność za szkody wyrządzone przez wykonawcę czynności. Źródłem podporządkowania może być stosunek pracy. Przy odpowiedzialności z art. 430 kc konieczną przesłankę stanowi wina podwładnego natomiast przełożony odpowiada na zasadzie ryzyka. Odpowiedzialność przełożonego i podwładnego jest solidarna.

Odpowiedzialność solidarną wprowadza przepis art. 441 § 1 kc, który stanowi, że jeżeli kilka osób ponosi odpowiedzialność za szkodę wyrządzoną czynem niedozwolonym, to za tę szkodę odpo-

wiadają wspólnie. Odpowiedzialność solidarna występuje zatem wówczas, gdy szkodę wyrządziło kilka osób będących bezpośrednimi sprawcami, gdy za szkodę odpowiadają podżegacze, pomocnicy oraz osoby, które świadomie korzystają z wyrządzonej szkody, a ponadto wówczas, gdy za szkodę odpowiada także inna osoba np.: na zasadzie ryzyka lub winy w wyborze. Osoby te mogą ponosić odpowiedzialność za szkodę na jednej lub na różnych podstawach prawnych. Przesłanką odpowiedzialności jest fakt, że każda z tych osób z osobna zobowiązana jest wobec poszkodowanego. Przy odpowiedzialności solidarnej każda z osób zobowiązanych do odszkodowania odpowiada wobec poszkodowanego za całość szkody, to znaczy poszkodowany może według swego wyboru dochodzić wyrównania szkody od jednej lub kilku osób zobowiązanych.

Art. 441 § 2 i § 3 dotyczą odpowiedzialności regersowej pomiędzy osobami zobowiązanymi do wyrównania szkody. Zgodnie z art. 441 § 2 kc, jeżeli szkoda była wynikiem działania lub zaniechania kilku osób, ten kto szkodę naprawił, może żądać od pozostałych zwrotu odpowiedniej części. Zależnie od okoliczności, a zwłaszcza od winy danej osoby oraz od stopnia w jakim przyczyniła się do powstania szkody. Zgodnie z art. 441 § 3 kc osoba, która jest odpowiedzialna mimo braku winy i naprawiła szkodę, za którą była odpowiedzialna, ma zwrotne roszczenie do sprawcy, jeżeli szkoda powstała z jego winy.

Roszczenia z tytułu czynu niedozwolonego przedawniają się z upływem lat trzech, przy czym bieg tego terminu rozpoczyna się z chwilą dowiedzenia się poszkodowanego o szkodzie i o osobie zobowiązanej do jej naprawienia. Jednakże w każdym przypadku roszczenie przedawnia się z upływem lat dziesięciu od dnia, w którym nastąpiło zdarzenie wyrządzające szkodę. Wyjątek od tej zasady stanowi sytuacja, gdy szkoda wynikła ze zbrodni lub występku, Wówczas roszczenie o jej naprawienie ulega przedawnieniu z upływem lat dziesięciu od dnia popełnienia przestępstwa, bez względu na to kiedy poszkodowany dowiedział się o szkodzie i o osobie zobowiazanej do jej naprawienia.

VII. Jak wynika z przedstawionych tu rozważań zagadnienia prawne związane z rozwojem cyfrowego przetwarzania danych są bardzo złożone i właściwie w wielu fragmentach ochrony prawnej, a zwłaszcza prawnokarnej, wymagają nowych rozwiązań. Droga legislacyjna w tym zakresie została rozpoczęta. Doskonalenia wymagają jeszcze metody wykrywania nadużyć związanych z wykorzystaniem komputera i utrwalania materiału dowodowego w tym zakresie.

OCENA PRAWNA NIEUPRAWNIONEGO WEJŚCIA DO SIECI KOMPUTEROWEJ

Maria Ziółkowska

Naukowa i Akademicka Sieć Komputerowa

Żyć i działać we współczesnym świecie, to znaczy korzystać z informacji. Bez racjonalnie ukształtowanej sfery informacyjnej nie mogą działać skutecznie społeczeństwa, struktury państwowe, nauka, oświata, kultura, przemysł, armia. Cywilizacja, którą budujemy i obserwujemy jest cywilizacją informacyjną. Wiedza i informacja są źródłem strategii i przemian społecznych. Dostęp do informacji, możliwość jej wymiany i przekazywania są podstawą dobrobytu i rozwoju. Nie ulega wątpliwości, że informacja jest towarem bardzo wartościowym, towarem kapitałorodnym choć z drugiej strony kapitałochłonnym.

Podstawą społeczeństwa informacyjnego jest sieć informatyczna zapewniająca gromadzenie, przesyłanie oraz udostępnianie informacji z dużą szybkością. Informacja musi być jednak towarem reglamentowanym, adresowanym indywidualnie, chronionym szczególnie. Zakres ochrony informacji wyznaczają jej wytwórca i odbiorca. Nie dotyczy to informacji chronionych administracyjnie, na podstawie określonych przepisów prawa - dotyczy to w szczególności informacji stanowiących tajemnicę państwową lub mającą znaczenie dla obronności czy bezpieczeństwa kraju.

Zabezpieczenie informacji przed niepożądanym do niej dostępem polegać może na tworzeniu specjalnych systemów technicznych, czy ochronie fizycznej, tworzeniu systemów logicznych oraz na wydawaniu odpowiednich przepisów prawnych. To ostatnie zabezpieczenie znajduje wyraz w przepisach prawa karnego, administracyjnego i cywilnego, dającego możliwość wprowadzania odpowiednich zapisów w umowach między stronami. Indywidualne regulacje prawne poszczególnych państw nie dają gwarancji skutecznego zabezpieczania informacji przed nieuprawnionym do niej dostępem. Informacja przekazywana sieciami komputerowymi jest niczym nieskrępowana, nie zna granic państw ani kontynentów. Różniące się między sobą systemy prawa obowiązujące w różnych państwach dają możliwość bezkarnego do niej dostępu. Mimo, że w np. kraju nadawcy informacji jest ona chroniona kompletnie, w kraju odbiorcy takiej ochrony nie znajdzie. Wobec powyższego bardzo słuszne i najgłębiej uzasadnione jest dążenie do zawarcia międzynarodowego porozumienia w sprawie przestępczości komputerowej, które obligowałoby jego sygnatariuszy do wprowadzania jednolitych regulacji prawnych.

Stąd, jako niesłychanie ważne należy uznać Zalecenie nr R/89/9 Komitetu Ministrów Rady Europy, które wzywa rządy krajów członkowskich Rady do uwzględnienia w trakcie prowadzonych prac legislacyjnych w ustawodawstwach wewnątrzpaństwowych tzw. „listy minimalnej" przestępstw komputerowych, która obejmować powinna 8 następujących kategorii zachowań:

- oszustwo komputerowe,
- fałszerstwo komputerowe,
- niszczenie danych lub programów komputerowych,
- sabotaż komputerowy,
- nieuprawnione wejście do systemu komputerowego,
- nieuprawnione przechwytywanie informacji,
- bezprawne reprodukowanie programu komputerowego,
- bezprawne kopiowanie reprografii półprzewodników.

Wstępne badania Rady Europy wskazują, że kraje członkowskie Rady dostosowują swoje systemy karne do zaleceń.

Dążeniem Rady Europy jest Europejska Konwencja w sprawie Przestępstw Komputerowych.

Należy stwierdzić, że polskie prawo jest ciągle bardzo staroświeckie w odniesieniu do ochrony komputerowo gromadzonej, przechowywanej i przesyłanej informacji, ochrony samych przekaźników tej informacji, komputerów i sieci komputerowych.

Polskie przepisy dostrzegają istnienie komputerów i programów komputerowych wyjątkowo; traktują mianowicie o nich dwie tylko ustawy: o prawie autorskim i prawach pokrewnych oraz ustawa o rachunkowości. Ustawa o prawie autorskim stworzyła lepsze warunki do skutecznej walki z piractwem komputerowym. Poza dotychczasowymi możliwościami dochodzenia roszczeń na drodze cywilnoprawnej wprowadzono sankcje karne za plagiaty, powielanie, dystrybucję, przechowywanie i ukrywanie nielegalnego oprogramowania, zwłaszcza gdy czyny te realizowane są na masową skalę stanowiąc źródło dochodu sprawcy.

Obowiązujący obecnie polski kodeks karny jest w znacznym stopniu niedoskonały, jeśli idzie o regulacje, (raczej ich brak) dotyczące ochrony omawianego przedmiotu. Nie zna on komputerowych przestępstw nieuprawnionego wejścia do sieci, bezprawnego uzyskania informacji drogą komputerową, zacierania danych bądź zmiany informacji, oszustwa komputerowego, sabotażu i podsłuchu. Komputer występuje jako narzędzie służące do popełniania przestępstw. Przedmiotem bezprawnego zamachu jest wtedy, gdy jest np. kradziony lub niszczony. Kodeks nie zauważa, że komputer, w szczególności zaś sieć komputerowa stanowić mogą niebezpieczny środek sprzyjający popełnianiu przestępstw, a zamach na system, czy sieć może być w najwyższym stopniu niebezpieczny wobec realnej możliwości rozmaitej penetracji informacji w nim umieszczonej. Wobec braku regulacji karnej takie działania nie powodują ponoszenia przez sprawców ryzyka odpowiedzialności karnej.

Generalną zasada prawa karnego jest, że przestępstwem jest czyn społecznie niebezpieczny, zabroniony pod groźbą kary przez ustawę, obowiązującą w czasie jego popełnienia (art. 1 kodeksu karnego). Przestępstwem zatem jest tylko takie działanie lub zaniechanie sprawcy, które jest ściśle określone w przepisach karnych. Prawo karne nie dopuszcza stosowania analogii. Czyn w najwyższym stopniu naganny, nieetyczny, niemoralny, sprzeczny ze zwyczajem czy zasadami współżycia społecznego nie jest przestępstwem, dopóki nie jest zabroniony przez ustawę i zagrożony karą.

Wobec powyższego, wydawać by się mogło, że jesteśmy bezradni wobec intruza w naszej sieci, który może poczynać sobie w niej bezkarnie.

Pomijam w tym miejscu oczywistą konieczność natychmiastowego podjęcia działań technicznych mających na celu zabezpieczenie sieci przed skutkami włamania, zabezpieczenie śladów włamania oraz przywrócenie jej do poprzedniej funkcjonalności.

W razie stwierdzenia włamania do sieci przede wszystkim należy ustalić, jakie były skutki włamania. Samo bowiem nieuprawnione wejście do sieci komputerowej bez wyrządzenia żadnej szkody, w szczególności bez uzyskania informacji, jej zmiany, uszkodzenia zapisu, przerwy w działaniu sieci nie jest obecnie karalne. Projekt kodeksu karnego także nie przewiduje takiego przestępstwa (samo nieuprawnione wejście do sieci, bez jakichkolwiek dalszych działań, jest karalne mdz. in. w Danii, Szwecji, Wlk. Brytanii, USA, Holandii i Francji).

Projekt kodeksu karnego przewiduje karalność nieuprawnionego wejścia do systemu komputerowego, ale w sytuacji, gdy włamywacz włamując się wszedł w posiadanie informacji dla niego nie przeznaczonej. Najwyraźniej twórcy projektu nie uważają, że społecznie niebezpieczne są w Polsce bezskutkowe włamania do sieci. Z drugiej strony, nie ma wielu

włamywaczy, którzy za cel stawiają sobie jedynie przełamanie zabezpieczeń informatycznych. Co do tej grupy można by rozważać jedynie odpowiedzialność cywilną odszkodowawczą, wynikającą z wyrządzonej szkody, np. nieuprawnionego zajmowania czasu komputerowego, blokowania sieci.

Większość włamywaczy szperających w sieciach ma określony cel. Zamiarem ich działań i często osiąganym efektem jest:

1) pozyskanie informacji dla nich nie przeznaczonej,

2) zniszczenie, uszkodzenie lub zmiana informacji,

3) umieszczenie w sieci treści zniesławiających lub oszczerczych, albo zniewag,

4) zniszczenie, uszkodzenie lub uczynienie niezdatnym do użytku urządzenia technicznego, czego następstwem są zakłócenia w łączności.

Odnośnie do punktu 1, stwierdzić należy, że pozyskanie informacji nie przeznaczonej dla włamywacza do sieci trudno będzie zakwalifikować, jako przestępstwo. Informacje przesyłane pocztą komputerową nie korzystają w polskim prawie karnym z ochrony takiej, jak korespondencja. Można będzie mówić o naruszeniu tajemnicy korespondencji wówczas, gdy „sprawca podstępnie uzyskał nie przeznaczoną dla niego wiadomość nadaną przy użyciu środków telekomunikacji" (art. 172 kk). W teorii i praktyce prawa karnego nie budzi wątpliwości, że wiadomości przesyłane sieciami komputerowymi są objęte tajemnicą korespondencji, niejasna jednak jest wykładnia pojęcia „podstępu". Praktyka w tej materii jest niewielka, trudno doszukać się orzeczeń Sądu Najwyższego na ten temat. Wydaje się, że jeśli nawet zdarzają się incydenty wyczerpujące znamiona występku z omawianego art. 172 kk, to nie są w tych sprawach kierowane oskarżenia, tym bardziej, że postępowanie toczy się z oskarżenia prywatnego, co skutkuje obowiązek uiszczenia wpisu od sprawy. Postępowanie w tych sprawach może być prowadzone przez prokuratora, ale tylko wówczas, gdy pokrzywdzoną jest instytucja państwowa lub społeczna. Niskie zagrożenie karne (kara pozbawienia wolności do 2 lat lub kara ograniczenia wolności albo grzywna) również jest w tych wypadkach czynnikiem zniechęcającym do składania doniesień.

Jeśli idzie o zniszczenie, uszkodzenie lub zmianę informacji zamieszczonej w sieci, stwierdzić należy, że takie działanie nie jest obecnie karalne. Art.212 kk przewiduje karalność czynu polegającego na „ zniszczeniu, uszkodzeniu lub uczynieniu niezdatnym do użytku mienia społecznego lub mienia cudzego". Sama informacja nie stanowi dobra materialnego, nie jest uznawana za mienie. W wypadku zniszczenia nośnika magnetycznego, na którym jest ona umieszczona, będzie można uznać, że nastąpiło zniszczenie mienia w postaci owego nośnika. Wartością wymierną w pieniądzach, określającą szkodę będzie wartość nośnika (np. wartość zniszczonego dysku, czy dyskietki). Wartość samej informacji nie będzie miała wpływu na określenie wartości szkody wyrządzonej przestępstwem. W wypadku zniszczenia lub uczynienia niezdatnymi do użytku zabezpieczeń sieci, szkoda będzie oceniana według wartości uszkodzonych zabezpieczeń. Oczywistym jest, że w wypadku skazania sprawcy za zniszczenie takich zabezpieczeń, pokrzywdzony będzie mógł dochodzić odszkodowania na podstawie przepisów prawa cywilnego. Można tego domagać się już w procesie karnym, na podstawie wytoczonego powództwa adhezyjnego, (może je wnieść na rzecz pokrzywdzonego także prokurator, jest to wówczas wolne od wpisu sądowego) lub jeśli do wytoczenia powództwa w procesie karnym nie dojdzie, pokrzywdzony może wytoczyć osobne powództwo przed sądem cywilnym.

Karalne jest umieszczenie przez włamywacza na liście publicznej treści znieważających, zniesławiających lub oszczerczych (art. 178 i 181 kk). Wszystkie te występki podlegają ściganiu z oskarżenia prywatnego. Prokurator może objąć je ściganiem publicznym, gdy będzie tego wymagał interes społeczny.

Najpoważniejszym ze względu na skutki materialne i szkodę oraz zagrożenie karne jest zniszczenie, uszkodzenie lub uczynienie niezdatnym do użytku urządzenia technicznego,

jeśli czyn taki powoduje istotne zakłócenie w łączności (art.220 kk). Czyn taki kwalifikowany jest bardzo surowo, przewiduje się mianowicie karę pozbawienia wolności nie niższą od 3 lat. Jest to zatem zbrodnia, która ścigana jest zawsze z oskarżenia publicznego, a w sprawie prowadzone jest obligatoryjne śledztwo wszczynane przez prokuratora. Przestępstwo ma charakter umyślny. Jest to szczególne, kwalifikowane uszkodzenie mienia, wywołujące skutek w postaci istotnego zakłócenia w łączności. Trudności w postępowaniu będzie nastręczało ustalenie, czy zakłócenie w łączności miało charakter istotny. „Istotność" zakłócenia, jako konieczny element zamierzonego efektu działania przestępczego należy oceniać z punktu widzenia powagi dalszych skutków, jakie to zakłócenie mogło wywołać.

Omówione wyżej możliwości zakwalifikowania i zarzucenia hackerom przestępstw uzależnione są od zebranych w sprawie dowodów. Nie jest przesadnym sąd, że niejednokrotnie administratorzy sieci i osoby odpowiedzialne za bezpieczeństwo sieci będą posiadały dużo większą wiedzę i doświadczenie w tych sprawach, niż prowadzący postępowanie inspektorzy lub prokuratorzy. Bardzo ważne są natychmiastowe działania mające na celu zabezpieczenie śladów włamania. Ogromne znaczenie ma też pomoc fachowa świadczona prowadzącym dochodzenie. Praktyka kryminalistyczna w Polsce jest w tym zakresie niewielka. Wynika to ze sporej bariery niewiedzy i braku doświadczeń organów ścigania. Nawet przy entuzjazmie prowadzących dochodzenie, bardzo dużej ich aktywności, wyniki postępowania mogą okazać się mizerne. W Polsce powodem tego może być choćby brak zupełny(!) biegłych sądowych z zakresu teleinformatyki i zabezpieczenia sieci. Znalezienie innych osób, które mogłyby wydać opinię w tych sprawach jest również trudne. Wynika to nie tylko z niechęci do występowania w procesie karnym, ale z pracochłonności takiej opinii oraz z konieczności posiadania dużej wiedzy technicznej. Opinia, że najlepszymi biegłymi w takich sprawach bywają hackerzy jest dość popularna.

Nie bez znaczenia jest również brak polskiej literatury kryminologicznej, niewielka ilość szkoleń policjantów, brak orzecznictwa.

Jesteśmy na początku szlaku, który trzeba przecierać. Nie możemy zatem ignorować żadnych incydentów nieuprawnionych działań w sieci, choćbyśmy nie mieli pewności co do tego, czy stanowią one zdarzenia przestępcze. Kwalifikowanie prawne tego rodzaju czynów jest bardzo trudne i należy zdać się w tej mierze na organy powołane do ścigania przestępstw. W świadomości tych organów musi zaistnieć fakt, że przestępstwa popełniane przy użyciu komputerów lub sieci komputerowych zdarzają się coraz częściej, a ich skutki mogą być bardzo groźne. Nie może być tak, że legislatorzy nie mają argumentów na uzasadnienie w sejmie szkodliwości społecznej takich czynów, ponieważ nie odnotowują ich statystyki policyjne. Statystyki istotnie prawie nie znają takich przestępstw. Nie znaczy to, że one nie występują. Często zdarza się, że pokrzywdzeni nie informują o ich występowaniu. Wolą je ukrywać w obawie przed utratą prestiżu w środowisku, lub utratą wiarygodności (np. banki).

Podstawowym obecnie problemem jest brak wyodrębnionych, ściśle opisanych przestępstw komputerowych w kodeksie karnym. Duże nadzieje na poprawę sytuacji daje projekt kodeksu karnego znajdujący się w nadzwyczajnej komisji sejmowej. W opinii ministra. Kubickiego ma być on uchwalony jesienią tego roku. Projekt ten wprowadza w rozdziale o ochronie informacji przetępstwa : naruszenia tajemnicy korespondencji przez podłączenie się do przewodu służącego do przekazywania informacji, niszczenia zapisów istotnej informacji (mdz. in. danych komputerowych), zakłócania informacji o szczególnym znaczeniu dla obronności kraju. Jak wspomniałam wyżej, w projekcie nie przewiduje się w dalszym ciągu karalności samego włamania do sieci , czy systemu komputerowego (nieuprawnionego wejścia do systemu). Włamanie samo nie istnieje; za przestępstwo będzie się uważało naruszenie tajemnicy korespondencji, zmianę informacji, czy jej usunięcie itd., które zostały dokonane w wyniku nieuprawnionego wejścia do sieci (tzw. włamania).

Pozwalam sobie na zacytowanie odpowiednich przepisów projektu kodeksu karnego, wyrażając jednocześnie nadzieję, że jeśli zostaną one zmienione w toku dyskusji sejmowych, to tylko w kierunku większej ochrony sieci i informacji w nich gromadzonych.

„Rozdział XXXIII
Przestępstwa przeciwko ochronie informacji

Art. 269
§ 1. Kto bez uprawnienie uzyskuje informację dla niego nie przeznaczoną otwierając zamknięte pismo lub podłączając się do przewodu służącego do przekazywania informacji albo przełamując elektroniczne, magnetyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności lub pozbawienia wolności do lat 2.
Art. 270
§ 1. Kto nie będąc do tego uprawnionym, niszczy, uszkadza usuwa lub zmienia zapis istotnej informacji lub w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.
§ 3. Kto dopuszczają się czynu określonego w § 1 lub 2, wyrządza istotną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
Art. 271
Kto zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie informacji o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji lub funkcjonowaniu administracji państwowej, dopuszczając się czynu określonego w art.270§ 3, albo niszcząc lub wymieniając nośnik informacji komputerowej lub niszcząc urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

Rozdział XXXV
Przestępstwa przeciwko mieniu

Art.280
§ 1. Kto zabiera w celu przywłaszczenia cudzą rzecz ruchomą podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 2. Tej samej karze podlega , kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągnięcia korzyści majątkowej.
Art,287
§ 1. Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody bez upoważnienia wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5."

Problematyka ścigania przestępstw komputerowych musi stać się priorytetowym zadaniem polskich organów ścigania. Ponadnarodowość i ponadpaństwowość przestępstw komputerowych musi skutkować wspólne ujednolicone działania międzynarodowych organów ścigania. Oczywistym jest, że najdoskonalsze przepisy cywilne i karne nie będą nigdy gwarancją nietykalności systemów komputerowych. Są one ostatecznym środkiem używanym wówczas, gdy zabezpieczenia techniczne okazały się niedostatecznie skuteczne.

Bibliografia

1) A.Adamski - „Odpowiedzialność operatora sieci komputerowej i BBS za przesłaną informację" - Materiały Seminarium Miedzeszyn 95,
2)K. Buchała - „Reforma polskiego prawa karnego materialnego" - Przestępczość Komputerowa materiały z konferencji naukowej w Poznaniu pod red. A.Adamskiego,
3) M. Mohrenschlager - „Hacking: to criminalise or not. Suggestion for the legislator" publ., jak w pkt.2,
4)R. Czechowski, P. Sienkiewicz - „Przestępcze oblicza komputerów" PWN 1993 r.,
5) J. Ordyński - „Jakie powinno być prawo karne" Rzeczpospolita nr 98/96,
6)O. Sawa - „Paragraf za skok na komputer" - Computerworld nr 16/96,
7) J. Wojciechowski - „Reforma prawa karnego" Rzeczpospolita nr 74/96

WYBRANE ZAGADNIENIA ŚCIGANIA PRZESTĘPCZOŚCI KOMPUTEROWEJ

Krzysztof J. Jakubski

Biuro Dochodzeniowo-Śledcze Komendy Głównej Policji

Pojęcie przestępstwa komputerowego jest bardzo pojemne i nieostre. Polska doktryna nie wypracowała jak dotąd jednolitej definicji. Aktualnie pod pojęciem tym rozumie się zarówno przestępstwa dokonane za pomocą komputera (sprzęt komputerowy jako narzędzie przestępcy) jak i skierowrane przeciwko komputerowi i całemu systemowi komputerowemu, a także godzące w samą informację, jej obieg w komputerze i całym systemie połączeń komputerowych. Jako przestępstwa komputerowe uznaje się także czyny polegające na naruszaniu uprawnień do programu komputerowego (piractwo komputerowe).

W latach siedemdziesiątych i osiemdziesiątych problem skutków ubocznych komputeryzacji, w tym nadużywania technologii informatycznych dla celów sprzecznych z porządkiem prawnym, nie angażował szczególnej uwagi ani organizacji rządowych ani międzynarodowych. Problemy związane z komputeryzacją były wówczas postrzegane raczej w skali lokalnej niż międzynarodowej. Lata dziewięćdziesiąte przyniosły zmianę podejścia do problemu nadużyć komputerowych. Zostały one uznane za jedną z form przestępczości transgranicznej i stały się przedmiotem badań prowadzonych z inicjatywy ONZ nad przestępczością zorganizowaną. *1

Przyczyn zmiany stosunku do problemu przestępczości komputerowej jest wiele, lecz do najważniejszych z nich należy coraz częście,j ujawniany międzynarodowy charakter tej przestępczości i stały wzrost wysokości strat nią powodowanych. Rozwój globalnych sieci komputerowych potęguje skalę tych zagrożeń. Koszty związane wyłącznie z oszustwami elektronicznymi dotykającymi świat amerykańskiego biznesu w połowie lat osiemdziesiątych oceniano na 100 mln dolarów USA rocznie.*2

Badania przeprowadzone na początku lat dziewięćdziesiątych w Wielkiej Brytanii określały brytyjskie roczne straty z powodu oszustw komuterowych na ponad 407 mln funtów szterlingów, przy czym okoliczności do nadużyć komputerowych i wysokość strat rosły proporcjonalnie do technicznego postępu.*3

Przestępstwa komputerowe różnią się od zwykłych przestępstw w dwóch powiązanych ze sobą podstawowych aspektach:

1) przestępca nie musi być obecny na miejscu przestępstwa aby dokonać zaplanowanego czynu,

2) nie istnieją granice przestępstw komputerowych, przez co powstaje szereg przeszkód formalnych utrudniających ich ściganie z uwagi na różnorodność systemów prawnych oraz problemy wynikające z właściwości podmiotów uprawnionych do ścigania. Przykładami takiej transgranicznej działalności przestępczej może być przypadek Stanleya Marka R. - konsultanta w dziedzinie komputerów w Banku Pacific w Los Angeles, który po rezygnacji z pracy odwiedził pokój telegrafu bankowego i zdobył numer kodu dla przesyłek informacji drogą telegraficzną. Stosując kod, za pomocą domowego modemu, polecił przekazanie kwoty 10,2 mln dolarów do banku szwajcarskiego na konto rosyjskiego kupca diamentów. Przestępstwo nie zostałoby wykryte, gdyby sam nie pochwalił się swoim czynem jubilerowi w USA.

W innym przypadku 22-letni Hiszpan przełamał kody zabezpieczeniowe największych międzynarodowych firm telekomunikacyjnych i udostępnił je swoim kolegom, którzy prowadząc rozmowy telefoniczne spowodowali straty na ok. 140 mln USD.

Przestępstwa komputerowe dokonywane są przez różne osoby, niezależnie od wieku i wykształcenia, z reguły pasjonatów techniki komputerowej. Ilustracją tego mogą być dwa poniższe przykłady:

- w listopadzie 1980 roku czterech 14 i 15-letnich uczniów z Dalton School w Nowym Jorku wybrało za pomocą szkolnego komputera numer kanadyjskiej komputerowej sieci telekomunikacyjnej, a następnie włamało się do komputera kanadyjskiej agencji firmy Pepsico uniemożliwiając tym samym pracę tej instytucji,

- trzydziestojednoletni Kevin Mitnick z Kalifornii, już jako siedemnastolatek włamał się do sieci komputerowej systemu Obrony Powietrznej USA (NORAD) - co zainspirowało twórców filmu "Gry wojenne". Później kilkakrotnie karany, znany jako "El Condor" przełamywał wielokrotnie różne zabezpieczenia sieciowe. Ostatnio zatrzymany, po dwóch latach od zwolnienia warunkowego, za spowodowanie zniszczeń w systemach komputerowych na sumę ponad 4 mln dolarów. Ponadto zarzuca się mu kradzież około 20 tys. numerów kart kredytowych, a także oprogranowania wartości miliona dolarów. Grozi mu obecnie kara 35 lat więzienia i 500 mln dolarów grzywny. Nikt nie gwarantuje, że będzie to koniec 14 letniej jego kariery hackera.

Skuteczność ścigania przestępczości komputerowej ogranicza wiele względów. Do najważniejszych z nich zaliczyć należy braki prawne i jurysdykcyjne, trudności w terminologii i zdefiniowaniu tych przestępstw, problemy dowodowe i niedostatek kompetentnych dochodzeniowców. Trudności te potwierdzają informacje na temat powodzenia w ściganiu przestępstw komputerowych w krajach wysoko rozwiniętych. Dane Departamentu Przemysłu i Handlu Wielkiej Brytanii z lat 1987-1992 ujawniły, że na 270 zgłoszonych przestępstw komputerowych śledztwo prowadzono zaledwie w sześciu. W Niemczech w 1987 r. 2777 przestępstw sklasyfikowano jako komputerowe, a wyroki skazujące uzyskano tylko w 170 sprawach.. We Francji po wydaniu w 1988 r. ustaw dotyczących nadużyć komputerowych na 70 zgłoszeń do policji, tylko co dziesiąte dochodzenie było skuteczne i sprawy znalazły się w sądach.*4.

Ogromny rozwój nowoczesnych technologii. informatycznych znacznie wyprzedził w Polsce wprowadzenie prawa informatycznego. Spenalizowane są zachowania narusza,jące prawa do programu komputerowego oraz bezprawne kopiowanie topografii półprzewodników.*5,6

Inne działania skierowane przeciwko systemowi komputerowemu mogą aktualnie być ścigane tylko o tyle, o ile zachowania takie stypizowane są w ramach innych przestępstw. Nie można jednak zgodzić się ze stwierdzeniem, iż zamachy na dane i system komputerowy w Polsce nie są prawnie zabronione.*7.

Zamiana danych przed lub w czasie ich wprowadzenia do komputera, niszczenie lub zniekształcanie zapisów na komputerowym nośniku informacji może być kwalifikowana jako przestępstwo przeciwko dokumentom (art. 265 - 269 k.k.). Uszkodzenie komputera, nośnika informacji, programu komputerowego i danych traktować można także jako uszkodzenie mienia spenalizowane w art. 212 k.k. W przypadku, gdyby zniszczenie komputerowego nośnika informacji lub urządzeń systemu komputerowego spowodowało istotne zakłócenia w działalności gospodarczej, komunikacji lub łączności, zachowanie takie należałoby uznać za wyczerpujące znamiona zbrodni określonej w art. 220 k.k. jako niszczenie, uszkodzenie lub czynienie niezdatnym do użytku urządzenia technicznego lub mienia w znacznych rozmiarach albo utrudnienie korzystania z nich. Należy tu podkreślić, iż przestępstwa określone w art. 212 i 220 kk są podobne, a różnica wynika wyłącznie ze skutku działania sprawcy (istotne zakłócenia). *8

Czy zakłócenia są istotne czy nie, decyduje nie tylko rozmiar i wysokość strat oraz czas przestoju, lecz także a nawet przede wszystkim konsekwencje wynikłe z czynu sprawcy.*9

Straty bowiem - jako nie należące do istoty czynu - mogą mieć tylko posiłkowe znaczenie dla oceny czynu i wpływać - zgodnie z art. 50 § 2 k.k. - na wymiar kary. *10

Jeżeli natomiast przestępne działanie nie spowodowało zakłócenia działalności, ale u sprawcy istniał zamiar jego spowodowania, to wówczas jego odpowiedzialność należy oceniać jako usiłowanie przestępstwa określonego w przepisie art. 220 k.k.*11

W przypadku, gdy działanie sprawcy będzie miało na celu osiągnięcie korzyści, np. przez manipulację programem, ściganie może być prowadzone w oparciu o przepisy chroniące mienie na przykład art. 205 k.k. (oszustwo) lub art.199 - 202 k.k. (zagarnięcie mienia).

Do niedawna policja polska nie zajmowała się problematyką przestępczości komputerowej. Składały się na to między innymi następujące przyczyny:

- policja rzadko spotykała się z informacjami na temat tego typu przestępstw,

- brakowało narzędzi i wypracowanych metod służących do zwalczania tej przestępczości,

- funkcjonariusze nie byli szkoleni w zakresie tej problematyki.

Gwałtowny rozwój technologiczny a także dążenia do włączenia Polski do krajów zjednoczonej Europy spowodowały to, że problematyka przestępczości komputerowej znalazła się w sferze zainteresowania organów ścigania. Wynikiem tego jest chociażby powstanie wyspecjalizowanych komórek zajmujących się tą problematyką w organach policji, a także nawiązanie bardzo owocnej współpracy z policjami państw zachodnich. Jej wynikiem jest na przykład przekazywanie specjalistycznego sprzętu komputerowego - w tym urządzenia dla procesowego zabezpieczania informacji znajdujących się na komputerowych nośnikach informacji a także organizowania szkoleń na temat metodyki zwalczania tej specyficznej kategorii przestępstw z udziałem policjantów i specjalistów zachodnich, głównie brytyjskich.

Wyniki zmiany podejś'cia policji do problematyki przestępczości komputerowej zaczynają być już widoczne. Coraz częściej sprawcy przestępstw popełnianych przy użyciu komputera są pociągani do odpowiedzialności karnej. Ujawniane są różne przypadki przestępstw komputerowych - od faktów używania komputera do tworzenia fałszywych dokumentów poprzez fakty wprowadzania fikcyjnych danych do systemów komputerowych (oszustwa komputerowe) do uszkodzeń programów w wyniku wprowadzania koni trojańskich. Skala zagrożeń jest wielka i nie może być liczona tylko wysokością strat faktycznie poniesionych, bowiem zdarzają się np. przypadki zawirusowań systemów komputerowych na Oddziałach Intensywnej Opieki Medycznej w szpitalach, gdzie komputery nadzorują funkcje życiowe pacjentów.

W chwili obecnej, poza oczekiwanymi zmianami w zakresie uregulowań prawnych dotyczących przestępczości komputerowej *12,przed polską policją stoją jeszcze poważne problemy dotyczące wyszkolenia kompetentnych policjantów oraz przygotowania zaplecza umożliwiającego właściwe zabezpieczenie i przedstawienie dowodów przestępstwa dla sądu. W tej mierze potrzebna jest współpraca nie tylko z policjami państw wysoko rozwiniętych, ale przede wszystkim pomoc i współpraca ośrodków akademickich, firm zagrożonych tą grupą przestępstw i innymi osobami, które dostrzegają problemy jakie niesie rozwój technologii informatycznych. Z uwagi bowiem na różnorodność systemów operacyjnych, ogromną rozmaitość systemów komputerowych, banków danych, języków oprogramowania, gotowych oprogramowań itp. nie jest możliwe posiadanie wszechstronnych specjalistów w policji. Ważne jest jednak, że problem przestępczości komputerowej jest dostrzegany.

P r z y p i s y:

1. S. Redo: Prevention and control of computer related crime from the United Nation perspective / A. Adamski (red.): Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z międzynarodowej konferencji naukowej. Poznań 20-22 kwietnia 1944 r., T N Oi K Toruń 1994, s. 71 - 87

2. B. Goldstein: Electronic Fraud:the Crime of the Future, "International Criminal Police Review"1985, nr 391

3. P.A. Colier, B.J. Spaul: Forensic Science against computer crixe in the United Kigdom, "Journal of the Forensic Science Society" 1992, vol. 32, nr 1, s. 27 - 34

4. Tamże

5. Ustawa z dn. 04.02.1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24, poz. 83)

6. Ustawa z dn. 30.10.1992 r. o ochronie topografii układów scalonych (Dz. U. Nr 100, poz. 498)

7. Por. A. Adamski: Odpowiedzialność operatora sieci komputerowej i BBS-u za przesłaną informację; aktualny stan prawny w Polsce na tle tendencji światowych, /w:/ Naukowa i Akademicka Sieć Komputerowa. Materiały z seminarium, Miedzeszyn 1995, s. 82 - 88

8. Postanowienie S.N. z dn. 17.03.1970 r., sygn. V KRN 38/70, OSNPG 1x70, nr 6, poz. 77. Por. także wyrok S.N. z dn. 02. 02.1984 r., II KR 9/84, O S N KW 1984, nr 11-12, poz. 122; wyrok S.N. z dn. 14.10.1x86 r., III KR 278/86, OSNPG 1987, nr 7, poz. 83

9. Por. wyrok S.N. z dn. 29.08.1973 r., IV KR 181/73, OSNKW 1974, nr 1, poz. 16 ; wyrok S.N. z dn. 27. 05.1986 r. , Rw 368/86, OSNKW 1987, nr 3-4, poz. 31; wyrok S.N. z dn. 18. 08.1983 r., II KR 168/83, OSNPG 1984, nr 4, poz. 29

10. Por. wyrok S.N. z dn. 30. 03.1978 r., II KR 41/78, OSNKW 1978, nr 7-8, poz.86; wyrok S.N. z dn. 01.07,1977 r,, IV KR 122/77, OSNPG 1977, nr 11, poz. 107

11. Wyrok S.N. z dn. 02.03.1987 r., II KR 3/87, OSNPG 1987 nr 21

12. Zmiany te zawiera projekt Kodeksu karnego wniesiony do Sejmu

ZDIGITALIZOWANE PRAWO AUTORSKIE. PRAWNE KONSEKWENCJE ZAMIESZCZANIA INFORMACJI W SIECIACH CYFROWYCH.

Małgorzata Byrska

Uniwersytet Jagielloński,
Międzyuczelniany Insytut Wynalazczości
i Ochrony Własności Intelektualnej

31-002 Kraków, ul Kanonicza 14, tel 22-61-55, fax 22-04-82

1. Wprowadzenie

Wraz ze wzrostem mocy obliczeniowej komputerów rozszerza się obszar ich zastosowań obejmując coraz to nowe dziedziny życia. W związku z tym powstają również nowe typy oprogramowania nieraz o nieprzewidywalnych wcześniej możliwościach, a stąd wymagające nowych uregulowań prawnych.

Jako spektakularny przykład może posłużyć krótki opis rozwijanego obecnie oprogramowania umożliwiającego poruszanie się w trójwymiarowym komputerowym świecie, którego ruchomy krajobraz jest oglądany na monitorze lub w specjalnych okularach (tzw. rzeczywistość wirtualna - *virtual reality*). Ruchy głowy lub gałek ocznych powodują płynną generację coraz to innego obrazu otoczenia, przez co jak w świecie rzeczywistym można poruszać się do przodu, na boki, do tyłu zwiedzając np. kolejne sale muzem Luwr, podchodząc do poszczególnych obrazów i rzeźb, studiować ich szczegóły. Robienie komputerowych kopii wybranych obrazów mistrzów malarstwa nie będzie stanowiło żadnego problemu technicznego. Musi jednak istnieć podstawa prawna takiego

kopiowania i ogólne uregulowanie zagadnień specyfiki kopii komputerowych dzieł. Przedstawione granice ludzkiej inżynierii informatycznej są jeszcze niedostępne przeciętnemu użytkownikowi komputera, ale już dzisiaj jest możliwe wytwarzanie komputerowych kopii tekstu czy obrazu i przesyłania ich na dalekie odległości, co jest symbolem nowego pola eksploatacji utworów.

Zwiększająca się moc komputerów kieruje też wysiłki programistów na rozwój szczególnej kategorii oprogramowania zawierającego elementy sztucznej inteligencji[1]. Związana z tym problematyka tworzenia, wykorzystania i ochrony baz danych i baz wiedzy dostarcza nowych sytuacji prawno-ekonomicznych, których rozstrzygnięcie na gruncie obowiązującego ustawodawstwa nie zawsze jest możliwe. W dalszych rozważaniach postaram się więc naświetlić najnowsze aspekty rozwoju oprogramowania.

2. Miejsce komputera w nowych rozwiązaniach technologii cyfrowej

Komputer od początku swego istnienia był maszyną cyfrową, a nie analogową. Binarne stany jego układów logicznych ulegają zmianie tylko w dyskretnych chwilach czasu (nie ciągle), zgodnie z impulsami jego wewnętrznego zegara. Zaprojektowany więc do przetwarzania liczb binarnych zapoczątkował erę technologii cyfrowej, która w porównaniu z technologią analogową (ciągłą) wykazała daleko większe możliwości w precyzji, szybkości przetwarzania i przesyłaniu informacji.

W latach 90-tych powszechny dostęp do małych mikro- i minikomputerów osobistych uzyskało miliony prywatnych osób, dla których problem świadomej pracy z komputerem pozostał oczywisty. Lata 90-te przyniosły jednak zasadniczą zmianę. Komputery przeniknęły do wszystkich możliwych technicznych systemów działalności człowieka i pozostając w tych systemach ich sercem i mózgiem, przestały być jednak w tych systemach widoczne. Wykorzystując, programowane z własnego aparatu, usługi nowoczesnej centrali telefonicznej, nieświadomie korzystamy z komputera. Elektroniczne kasy sklepowe przyspieszają obsługę klientów, ale ich zasadniczym celem jest przesyłanie raportów do komputera sklepowego, który na tej podstawie decyduje o wysyłaniu zamówień dla uzupełnienia towarów. Naukowiec przeprowadzający obliczenia w sieci akademickiej nie wie dokładnie z którego komputera korzysta. Nowoczesne usługi bankowe pozwalające na podstawie karty osobistej pobrać pieniądze z automatu (Bankomatu) zainstalowanego na różnych ulicach miasta, czy system kart kredytowych obsługiwanych w większości sklepów krajów rozwiniętych działają w oparciu o bliżej niezlokalizowany komputer.

Wszystkie te rozwiązania stały się możliwe, gdy technologia cyfrowa umożliwiła dołączenie komputera do sieci komunikacyjnych.

W latach 90-tych istotną nowością stał się więc powszechny przesył informacji cyfrowej na duże odległości.

Rozwój sieci *Internet* pozwolił na wykorzystanie anonimowych komputerów i uzyskanie dostępu do ich baz danych zawierających dane encyklopedyczne czy ogłoszenia o usługach. Można dzięki nim również przesyłać własną korespondencję.

Nadszedł jednak czas w którym technologia cyfrowa w coraz większym stopniu oddziaływuje też na aspekty życia tradycyjnie związane z wytwarzaniem dzieł zaliczanych do dóbr kultury. Pociąga to za sobą konieczność modyfikacji niektórych aspektów uregulowań prawnych. Na przykład eksploatowanie utworów w

---

[1] Por. R.Tadeusiewicz, Tryumf czy kapitulacja rozumu? Znak 1995, nr 9, s.59 i n.; WIPO Worldwide Symposium on the Intellectual Property Aspects of Artificial Intelligrnce, Stanford University, March 25 to 27, 1991.

sieci komputerowej może doprowadzić do zatarcia różnicy pomiędzy autorem i wydawcą (najczęściej będzie to jedna osoba), jak również autorem a recenzentem, który często będzie współautorem pracy w tradycyjnym ujęciu[2].

3. Nowe formy przekazu w technice cyfrowej

Dotychczasowe uregulowania prawne w wystarczający sposób zabezpieczały właściwe rozstrzyganie prawie wszystkich sytuacji prawnych jakie możliwe były do powstania w procesie tworzenia i dystrybuowania dzieła. Jednak ogólność i kompletność uregulowań prawnych, powstających na pewnym etapie rozwoju cywilizacji zawsze wynika ze stopnia przewidywalności zaistnienia wszystkich możliwych sytuacji prawnych. W omawianym kontekście prawa autorskiego ogólność ta, była w sposób nieświadomy limitowana przez ustawodawcę do granic stosowalności od dawna znanych metod technologii analogowej, jakie używane były w procesie technicznego utrwalania (zapisu), powielania (kopiowania), przetwarzania (opracowywania, modyfikowania), dystrybucji dzieła lub informacji z nim związanych. Do wszystkich tych czynności można było wykorzystywać klasyczną technologię analogową (nagrywanie płyt rowkowych, magnetycznych taśm audio i video, druk książek, tworzenie i dystrybucja filmów, przesyłanie sygnałów radiowych i telewizyjnych). Obecnie w coraz większym stopniu do czynności tych angażowana jest technologia cyfrowa. Aby analiza zasadności stosowania aktualnego prawa autorskiego lub jego braków na tle tej nowej technologii była wiarygodna poniżej skrótowo wypunktuję zasadnicze techniczne różnice między tymi dwoma technologiami.

3.1. Techniczne podobieństwa i różnice technologii analogowej i cyfrowej

Nazwa "technika analogowa" związana jest z podstawową ideą stosowaną od dawna, a która polega na odwzorowaniu w sposób ciągły zmian częstotliwości drgań np. strun głosowych, strun instrumentu, światła widzialnego czyli barwy w analogicznie ciągłe zmiany innej wielkości fizycznej np. natężenia pola magnetycznego na taśmie, głębokości rowka na płycie bakielitowej, zaczernienia taśmy filmowej. Do tego procesu rejestracji ciągłych sygnałów fizycznych, ich utrwalenia i odtworzenia używany jest zestaw trzech podstawowych urządzeń tworzący pewien tor na który składa się: przetwornik sygnału mechanicznego na elektryczny np. mikrofon, urządzenie utrwalająco-odtwarzające sygnał elektryczny np. magnetofon i przetwornik sygnału elektrycznego ponownie na mechaniczny np. głośnik. Zagwarantowanie lepszej analogii między sygnałami mechanicznymi i elektrycznymi gwarantowało wyższą wierność odtwarzania, a stąd jakość urządzenia (*High fidelity*). W tej technologii najbardziej zawodnym, a więc wnoszącym największe przekłamania sygnału okazało się środkowe urządzenie utrwalająco-odtwarzające.

Rozwój technologii cyfrowej i komputerów w sposób naturalny wpłynął na modyfikację przedstawionego toru. Wprowadzono do niego dwa dodatkowe urządzenia: przetwornik analogowo-cyfrowy A/C umieszczony, mówiąc skrótowo po mikrofonie, a przed magnetofonem i przetwornik cyfrowo-analogowy C/A umieszczony po magnetofonie, a przed głośnikiem. W ten sposób sygnał elektryczny został na wstępie zamieniony na ciąg cyfr przy jednoczesnym zagwarantowaniu dowolnej dokładności tej zamiany. Ciąg cyfr może być zapamiętany w różny sposób (na taśmie magnetycznej, w pamięci komputera, na płycie CD) i w odpowiedniej chwili skierowany do przetwornika cyfrowo-

---

[2] Zob. H.Heker, The Publisher in the Electronic Age: Caught in the Area of Conflict of Copyright and Competition Law, (2) EIPR 1995, s. 75 i n.

analogowego w celu odtworzenia oryginalnego sygnału elektrycznego uruchamiającego z kolei przetwornik elektryczno- mechaniczny czyli głośnik. Sygnał cyfrowy pojawiający się w torze ma jedną podstawową zaletę: jest w najwyższym stopniu nieczuły na zakłócenia pojawiające się przy jego magazynowaniu (utrwalaniu) i jego przesyle (transmisji). Nazwa Hi-Fi dla cyfrowych urządzeń audio-video straciła rację bytu.

3.2. Nowe formy powielania

W ostatnich kilku latach nastąpiło zasadnicze rozszerzenie granic technologicznych, implikujące nowe nieprzewidywalne możliwości przetwarzania i przesyłu informacji między ludźmi. Korzenie tej nowej technologii tkwią w powstaniu nowego narzędzia jakim jest komputer. Równolegle ze wzrostem mocy obliczeniowej komputerów powstawały nowe narzędzia do współpracy z nimi, z konieczności również zbudowane w oparciu o technologię cyfrową. Niektóre z nich zwane są urządzeniami multimedialnymi[3], gdyż związane są z obróbką i przesyłaniem do komputera sygnałów pochodzących z wielu mediów: głos, obraz, ruch. Urządzenia takie wyposażone w odpowiednie oprogramowanie umożliwiają zeskanowanie (cyfrowe zapamiętanie punkt po punkcie) z wybraną dokładnością obrazu kolorowego z paletą barwną sięgającą kilku milionom odcieni kolorów. Umożliwiają również cyfrową analizę i zapamiętanie głosu z dowolną dokładnością (aż poza granice ludzkiej słyszalności) jak również skanowanie i zapamiętanie trójwymiarowych kształtów skomplikowanej rzeźby czy odlewu. Skanery umożliwiają szybkie odczytywanie tekstów wykonanych wcześniej techniką drukarską (książki, gazety), a nawet pisma ręcznego. Wszystkie te dane, o których można powiedzieć, że są dowolnie wiernymi kopiami komputerowymi oryginału mogą być zapamiętane w komputerowej bazie danych na dysku magnetycznym, compact dysku (laserowym CD) lub innym nośniku informacji. Olbrzymi stopień upakowania informacji (wielotomowa encyklopedia na jednym małym krążku laserowym) jest też jedną z cech charakteryzujących nowoczesną technologię cyfrową. Nowe techniczne możliwości stworzyły nowe pola eksploatacyjne utworów: umieszczenie w bazie (banku) danych oraz digitalizację utworu (zapis w technice cyfrowej często poprzez skanerowanie utworu).

3.3. Przekaz cyfrowy w ogólnoświatowych sieciach informatycznych

Powstanie sieci informatycznych niesie ze sobą szereg korzyści i zagrożeń. Do tych pierwszych możemy zaliczyć: bezpośredni dostęp do banków danych na całym świecie; transmisja informacji w czasie realnym; wymiana zdań bez względu na odległość i różnice czasowe; architekci mogą korzystać z trójwymiarowego obrazu swoich zmysłów przed rozpoczęciem budowy, techniki wirtualne mogą prowadzić bezbłędnie rękę chrurga itd. Wreszcie świat sztuki i rozrywki uzyska narzędzie, które pozwoli zaspokoić najbardziej wyrafinowanych twórców i odbiorców sztuki i rozrywki.

Zagrożenia: już dzisiaj mówi się o istnieniu sieci *Black Net*, która miałaby dostarczać poufnych informacji dotyczących przedsiębiorstw i pojedynczych osób. Mogą powstać sieci rasistowskie, faszystowskie, sieć dla terrorystów itp, które mogą stać w sprzeczności z prawem i moralnością.

---

[3] Por. M.D.Scott, J.L.Talbott, Interactive Multimedia: What is it, Why is it Important and What does one Need to Know about it? (5) EIPR 1993, s. 284 i n.; M.Turner, Do the Old Legal Categories Fit the New Multimedia Products? A Multimedia CD-Rom as a Film, (3) EIPR 1995, s.107 i n.; T.Wachter, Multimedia und Recht, GRUR Int. 1995, nr 11, s. 860 i n.

"Sieć - twierdzi May (dziecko McLuhana) - to anarchia. Żadnej kontroli centrum, żadnych szefów, żadnych praw. Żaden naród nie może jej sobie zawłaszczyć, żadna administracja nie może skierować na nią swojej policji". Zatem, w chwili, gdy włączamy nasz komputer działający w sieci takiej jak *Internet*, przestajemy być w Polsce, ale natychmiast znajdujemy się w świecie Disneya lub u Dicka Turnera.

Jednym z decydujących elementów w nadchodzącym stuleciu stanie się kwestia szyfrowania, kodowania przekazu nadawanego siecią cybernetyczną. Idzie tu zarówno o ochronę dóbr osobistych, jak i tamę przeciw piractwu poufnych danych.

W USA, FBI zamierzało wprowadzić do wszystkich komputerów *clipper chipy*, czyli coś w rodzaju "pchły" podsłuchiwaczki. Jednak Kongres w imię I Poprawki o wolności słowa i pod naciskiem lobby informatycznego zablokował tę decyzję.

W związku z rozwojem technologii cyfrowych umożliwiających łatwe magazynowanowanie, a następnie transfer informacji z banków czy baz danych do dowolnej osoby, zjawia się potrzeba dokładnego określenia prawnych zasad dostępu do tych zasobów oraz sprecyzowania uprawnień autorskich.

Rozwój technologii i wzrost zapotrzebowania na tego typu usługi umożliwił w konsekwencji powstanie dużych systemów komputerowych, a w końcu ich sprzęgnięcie w ogólnoświatowych sieciach informatycznych.

Już dzisiaj większość użytkowników sieci może uzyskać połączenie z każdą z wielu tysięcy baz danych włączonych w system ogólnoświatowych sieci informatycznych (najpopularniejsza z nich *Internet* wzięła początek od sieci akademickiej) i znaleźć tam odpowiedź na interesujące ich pytanie. Dostęp do komputerowych kopii największych encyklopedii zawierających kolorowe ilustracje i możliwość ich wertowania stawia pod znakiem zapytania potrzebę zakupu ich oryginału. Dostęp do najnowszych prac naukowych, które nie zdążyły jeszcze zostać wydrukowane techniką tradycyjną, a których autorzy zgodzili się na ich umieszczenie w specjalnej bazie danych musi owocować w przyśpieszeniu postępu technicznego czy kulturalnego. Dzisiejsze bazy danych umożliwiają dwojaki sposób pozyskiwania informacji (odpłatne lub nieodpłatne): tylko przez przeglądanie udostępnionych informacji oraz przez przeglądanie i kopiowanie całych zbiorów ze specjalnych katalogów, zawierających nie tylko zbiory typu *public domain*.

Najbliższa przyszłość przyniesie powstanie centrów informatycznych[4] o nieistotnej lokalizacji, w których użytkownik będzie mógł zamówić jak w wypożyczalni lub w firmie dostawczej kopię wybranej książki w wybranym języku, którą może odczytać z monitora (za mniejszą opłatą), lub której wydruk w ulubionym formacie może zostać przesłany na jego własną drukarkę (za większą opłatą). Będzie mógł zamówić kopię wybranego obrazu słynnego malarza, którą sam wykona przy pomocy kolorowego plotera, cyfrową kopię utworu muzycznego, którą następnie odtworzy w swoim domu z użyciem wysokiej jakości odtwarzacza CD, trójwymiarową kopię cyfrową rzeźby Venus z Milo, którą następnie odtworzy w pomniejszeniu w bloku gipsowym za pomocą trójwymiarowej frezarki XYZ, czy w końcu cyfrową kopię ulubionego filmu, która to kopia pod względem jakości dorównywać będzie oryginałowi (co tak bardzo odróżnia dzisiejsze analogowe kopie video od ich oryginałów). Wszystkie te zamówienia centrum zrealizuje przeszukując różne bazy danych w różnych krajach. Automatycznie też pobierze opłatę z konta użytkownika i prześle odpowiednią opłatę na konto autora. Niektóre z tych usług już są realizowane przez amerykańską sieć *CompuServe*.

---

[4] Por. Z. Kitagawa, Computers, Digital Technology and Copyright, materiały WIPO Worldwide Symposium on the Future of Copyright and Neighboring Rights, Le louvre, Paris, France - June 1 to 3, 1994, s. 115 i n.

Przyszłość więc może przynieść zniknięcie dużej ilości księgarń, a nawet idąc dalej zniknięcie w ogóle wydawców i dystrybutorów dzieł, które są jeszcze autorsko chronione, gdyż w wersji najbardziej radykalnej autorzy lub ich pełnomocnicy sami będą realizować swoje prawo do dystrybucji poprzez rozsyłanie do użytkowników dowolnej ilości swoich własnych utworów lub w ramach promocji i reklamy ich bezpłatnych streszczeń. Radykalnie ulegną więc też obniżeniu koszty ponoszone dotychczas na infrastrukturę (dukarnie, papier, składowanie, transport), a przede wszystkim skróci się czas dystrybucji od chwili stworzenia dzieła do momentu jego odbioru. Technika komputerowa umożliwi też o wiele szybszy wybór i szybszą "konsumpcję" dzieł przez odbiorcę.

Wygląda więc na to, że cyfrowa technologia w XXI wieku podporządkowana będzie jednemu zadaniu: w jak najkrótszym czasie przetworzyć i dostarczyć człowiekowi jak największą ilość wstępnie wyselekcjonowanej informacji. Rola poszczególnego człowieka sprowadzi się do jej ostatecznej selekcji i wykorzystania.

3.4. Prawne implikacje przetwarzania i przekazu informacji w technice cyfrowej

Tak łatwe operowanie cyfrowymi kopiami utworów niesie ze sobą jednak pytania o granice dozwolonego kopiowania i przeróbek, o granice dalszej redystrybucji i prawno-techniczne metody walki z piractwem.

Pojawią się pytania zasadnicze jak np. problem definicji oryginału dzieła. Utrwalone dzieło bowiem może mieć od razu postać cyfrową np. obraz zaprojektowany z użyciem komputera i zapamiętany jako zbiór binarny, choć jego analogowe ustalenie nastąpiło oczywiście wcześniej na ekranie monitora, a więc w sposób nietrwały. Gdy obraz ten zostanie wydrukowany (namalowany) po raz pierwszy stanowił będzie tylko swoją pierwszą kopię, gdyż wszystkie następne będą nie do odróżnienia. Tak więc nośnikiem oryginału dzieła będzie cyfrowa postać zbioru wyjściowego. Dzisiaj z takim przypadkiem spotyka się na codzień projektant podzespołów mechanicznych, których precyzyjny kształt powstaje w komputerze przy pomocy programów wspomagających projektowanie typu AUTOCAD (Computer Aided Design). Pierwszą rzeczywistą kopię wykonuje frezarka cyfrowa zgodnie z komputerowym projektem. W przyszłości tą metodą mogą posługiwać się rzeźbiarze.

Czy więc zdigitalizowane prace mogą być odrębnymi przedmiotami prawa autorskiego? Zdigitalizowane oryginały to jak zaszyfrowane utwory przy czym zdigitalizowana forma nie jest formą końcową, jak przy tłumaczeniu czy modyfikacjach. Jest to forma przejściowa robiona w konkretnym celu, aby ułatwić przechowywanie i transport utworów. Po dedigitalizacji przedmiot przesyłu wraca do oryginału. Jednak ta nowa kategoria utworów może zacząć żyć własnym życiem.

Zwraca się też uwagę na fakt, że taki "utwór" nie ma formy wyrazu, istotnej dla prawa autorskiego, czy zatem zdigitalizowane utwory nie będą autorsko chronione? Wydaje się raczej, że teorie prawa autorskiego dotyczące problemu: co chronimy w prawie autorskim - formę czy treść dzieła powinny więc ulec przemodyfikowaniu, ponieważ zero-jedynkowe dane w formie cyfrowej nie mają "formy" w tradycyjnym znaczeniu a równocześnie nie można im odmówić ochrony autorskoprawnej. A zatem nie forma a kontrolowalność zdigitalizowanych informacji będzie słowem kluczowym dla twierdzenia o przyjęciu ochrony autorskoprawnej.

Technologia cyfrowa niesie dalsze problemy takie jak: multimedia w prawie autorskim jako nowa kategoria przedmiotów; autorstwo utworów multimedialnych,

prawo do digitalizacji jako nowe uprawnienie autorskie, pytanie czy transmisję jest publikacją utworu?

Dane w technice cyfrowej są łatwiejsze do kopiowania z zachowaniem tej samej jakości; łatwiejsze do transmisji; łatwiejsze do modyfikowania. W konsekwencji autorzy utworów w zdigitalizowanej postaci mogą być pozbawioni możliwości kontroli korzystania ze swoich prac. Z drugiej strony, producent dzieła medialnego będzie mógł dość łatwo znaleźć informację o dziełach autorskochronionych i uzyskać licencje od uprawnionych w celu wykorzystania tych dzieł.

Jako argument w dyskusji niech posłużą dwa rzeczywistee przykłady, nad jakimi już dzisiaj zastanawiają się znawcy problemu[5].

Pierwszy związany jest z już stosowaną cyfrową techniką kolorowania starych czarno-białych filmów bez zgody jego twórców[6]. Drugi wypłynie praktycznie po roku 2000 gdy planowane jest we Francji rozpoczęcie eksploatacji telewizji cyfrowej. Obecność w każdym domu źródła cyfrowego sygnału video, który przez każdego profesjonalnego użytkownika komputera może być dowolnie modyfikowany, miksowany i używany jako materiał wyjściowy do własnej twórczości musi rodzić pytania o możliwości prawne zapobieżenia takiemu działaniu. Trzeba dodać, że takich manipulacji sygnałem TV nie umożliwia dzisiejsza analogowa technika transmisji.

Z powyższymi zagadnieniami jest też w pewnym stopniu związany praktyczny problem rozprowadzania produktów *softwarowych*[7]. Na rynku działają dwa typy instytucji rozprowadzających oprogramowanie. Pierwsza pracuje w systemie, w którym za pomocą sieci umożliwia dostęp do swojej bazy danych z kopiami prac chronionych za z góry wniesioną opłatą, druga na zasadzie kredytowej "najpierw wypróbuj-potem kup" oferuje za darmo oprogramowanie działające tylko przez krótki okres czasu. Drugi typ instytucji pracuje w systemie dostarczającym za opłatą kopie prac w formie cyfrowej na CD-ROM na zasadzie *Software Envelope System* i *CD Showcase*. Pierwszy oferuje *software* w zakodowanej formie. Po otwarciu koperty użytkownik jest zaznajamiany z informacjami na temat ochrony autorskoprawnej i otrzymuje warunki licencji takie jak ograniczenie reprodukcji, modyfikacji i magazynowania. W przypadku, gdy użytkownik decyduje się na korzystanie z wybranego oprogramowania otrzymuje identyfikacyjny numer dekodujący oprogramowanie. *System CD Showcase* działa natomiast w oparciu o omawiany już slogan "*try-and buy*". W literaturze prawniczej nie zostały jeszcze scharakteryzowane typy powyższych umów[8].

---

[5] Zob. A.Lange, The Impact of Digital Technologies on the Author's Right and Neighboring Rights, materiały WIPO Worldwide Symposium on the Impact od Digital Technology on Copyright and Neighboring Rights, Harvard University, Massachusetts, USA, March 31 to April 2, 1993, s.227 i n.

[6] Por. A.Wojciechowska, Barwienie czarno-białych filmów w świetle prawa autorskiego, ZNUJ MIW 1992, nr 58, s.49 i n.

[7] Por. Z.Kitagawa, op.cit. s.117.

[8] Łatwość kopiowania i przesyłu komputerowych kopii wymusza poszukiwanie nieprawniczych rozwiązań zabezpieczających. Techniczne zabezpieczenia dostępu do sieci to np. wykorzystanie pośredniczących przstawek kodujących i rozprowadzanych kart kodowych (jak w kodowanej telewizji kablowej) ważnych na określony okres czasu, co umożliwi odtworzenie przez użytkownika otrzymanych zbiorów na własnym komputerze tylko przez wykupiony okres czasu, lub bez limitu czasowego.

Łatwość udostępniania i pozyskiwania różnych informacji w sieciach rodzi też techniczne i prawne pytania o mechanizmy kontroli nad treścią informacji udostępnianej publicznie, np. poruszany obecnie w dyskusjach, a jeszcze nie rozwiązany problem dostępu dzieci do zbiorów o treści pornograficznej[9].

Osobna problematyka powstaje w związku z usługami poczty elektronicznej tj. przesyłania i odbierania prywatnych zbiorów binarnych do/od innych użytkowników sieci. Nieuregulowana jest jeszcze sprawa poufności tych przesyłek nie tylko na poziomie sieci międzynarodowych, ale nawet na poziomie zakładu pracy[10].

Ochrona praw osobistych w stosunku do dzieł zakodowanych w technice cyfrowej wymaga więc specjalnej uwagi.

W swoim referacie wygłoszonym na światowym sympozjum WIPO na Uniwersytecie Harvard w 1993 r. M.D.Goldberg i J.M.Feder[11] omawiając wpływ nowej technologii cyfrowej na prawo zwrócili uwagę na raczej ilościowy aspekt różnic między omawianymi technologiami. Ich zdaniem - technologia cyfrowa pozwala na większą koncentrację informacji na mniejszej fizycznie powierzchni, zwiększa łatwość reprodukcji oraz zwiększa łatwość i szybkość dystrybucji. Jednak jakościowo biorąc, według tych autorów, nie zmienia to zasadniczych jej cech ani nie tworzy nowych, które nie mogłyby być objęte obecnym ustawodawstwem. Zdecydowanie podkreślali podobieństwa obu technologii i tym samym uznali za uzasadniony brak konieczności wprowadzania zmian legislacyjnych w zakresie prawa autorskiego.

Na tym samym sympozjum inni autorzy raczej w pesymistycznym świetle przedstawiali możliwości dzisiejszych uregulowań autorsko- prawnych w stosunku do przyszłych sytuacji implikowanych przez nowe technologie, a zwłaszcza przez perfekcję kopii i łatwość jej uzyskania[12].

4. Główne przesłanki przyjęcia ochrony prawnej przesyłanych informacji

Silna ochrona autorskoprawna jest nieodzownym warunkiem ochrony nowych rozwiązań informatycznych[13]

Można wskazać na pięć cech infostruktury, które stanowią o specyfice tego nowego pola zainteresowań dla prawników.

1) Tworzenie infrastruktury obejmuje zarówno "zawartość" baz danych jak i

---

[9] N.Gurfinkel, Pornografia dziecięca w Internecie.Rzeczypospolita 1995, nr 36.

[10] Zob. I.Dobosz, Przesłanki cywilnoprawnej ochrony przed podsłuchem, ZNUJ MIW 1992, nr 58, s. 85 i n.; Kto czyta waszą pocztę, PC World Komputer 1994, nr 5,s.21 i n.;T.Beth, Poufność w Internecie, Świat Nauki 1996, nr 2, s.26 i n.

[11] M.D.Goldberg, J.M.Feder, Copyright and Technology: The Analog, The Digital, and The Analogy. WIPO Worldwide Symposium on the Impact of Digital Technology on Copyright and Neighboring Rights, op. cit., s.154 i n.

[12] Por. R.D.Hadl, Digital Technology: A Critical Crossroad in International Copyright. WIPO Worldwide Symposium on the Impact of Digital Technology on Copyright and Neighboring Rights, op.cit. s. 234 i n.

[13] Por. A.N. Dixon, L.C.Self, Copyright Protection for the Information Superhighway, (11) EIPR 1994, s.465 i n.; A.Christie, Reconceptualising Copyright in the Digital Era, (11) EIPR 1995, s. 522 i n.

2) Ładowanie (*upload*) "zawartości" będzie zazwyczaj wiązało się z zastosowaniem kodowania lub innego środka kontroli dostępu do treści (zawartości), a następnie z udostępnieniem tej treści tylko autoryzowanym użytkownikom poprzez kopiowanie lub transmisję siecią na ścieżkach ograniczonego dostępu. Należy domniemywać, że ważniejsi wydawcy, filmowcy, pracowniczy tv stworzą własne "punkty dostępu".

3) Przekazywanie treści (zawartości) i usług od ich dostarczycieli do użytkowników następowałoby przez jeden (lub kombinację) następujących przekaźników: sieć telefoniczna, inne sieci użytkowe, komunikacja komórkowa, satelitarna, światłowodowa.

4) Udostępnianie treści (zawartości) następuje w momencie, kiedy użytkownik ręcznie lub automatycznie wpisuje się w sieć, dostarcza swoją autoryzację dostępu i ma możliwość korzystania z usług i zawartości jednego lub więcej dostarczycieli.

5) W przypadku gdy dane treści wchodzące w zakres infostruktury są użytkowane *"on-line"* zagadnienia prawne związane z tego rodzaju sytuacją są analogiczne jak w przypadku udostępniania treści (pkt 4).

O odmienności zapisu cyfrowego w stosunku do tradycyjnych utworów w prawie autorskim decyduje:

1) zmiana w formie wyrazu;
2) zmiany w sposobach dystrybucji;
3) zmiany w sposobie dostępu do utworu i jego kopiowaniu;
4) zlanie się różnych typów utworów, w jedno z formalnego punktu widzenia dzieło.

Propozycje zakresu ochrony nowych cyfrowych dzieł.

1) Utrzymanie ochrony autorskoprawnej co najmniej na takim samym poziomie jak w stosunku do programów komputerowych.
2) Wzorem powinna być Dyrektywa Unii Europejskiej dotycząca ochrony oprogramowania.
3) Autor utworu cyfrowego zachowuje wyłączne prawa do powielania i modyfikowania utworu (włączając w to prawo do digitalizacji utworu), ma również wyłączne prawo do wyrażenia zezwolenia na włączenia zdigitalizowanego w całości lub części utworu, w jakiejkolwiek formie, w zakres innego dzieła.
4) Autor utworu cyfrowego zachowuje wyłączne prawo do elektronicznego wprowadzenia, przesyłania, dostępu i wyprowadzania dzieła.
5) Ograniczenia monopolu autorskiego analogiczne jak w Dyrektywie.
6) Zmiany w prawie autorskim nie powinny naruszać podstawowych założeń tego prawa, mają tylko na celu możliwość włączenia w aktualny schemat ochrony utworów cyfrowych.
7) Utwory multimedialne będą orzone, powielane i wprowadzane do obrotu tylko za zgodą autora albo innego "właściciela" włączonych w sieć utworów.
8) Przymusowa licencja powinna być zakazana.
9) Prawa własności intelektualnej winny być częścią krajowych czy międzynarodowych systemów prawnych tylko pod warunkiem wolnego dostępu do utworów na zasadach uczciwej konkurencji.
10) Nie powiny obowiązywać jakiekolwiek wymogi formalne przy przyznawaniu ochrony autorskoprawnej.
11) Prawa autorskie, prawa sąsiednie i wszelkie nowe regulacje specjalne w tym zakresie mogą być tworzone, nowelizowane i administratowane w zgodzie z pryncypiami Konwencji Berneńskiej i umowy GATT - TRIPS.
12) Nieautoryzowany dostęp do komputerów i ich zawartości winien być

traktowany jako przestępstwo (np. włamywanie się do sieci komputerowych).

13) Powinno nastąpić zaostrzenie procedury prawnej w zakresie dochodzenia i zabezpieczania roszczeń podmiotów uprawnionych.

5. Proponowany model ochrony

W dotrynie europejskiej proponuje się przyjęcie ochrony prawnej sieci informatycznych analogicznie do rozwiązań odnoszących się do ochrony oprogramowania komputerowego. Ochrona taka odnosiłaby się do zawartości przesyłu informatycznego, który można teoretycznie zaliczyć do utworów chronionych prawem autorskim. W przeważającej większości byłaby to kategoria tzw. utworów *multimedialnych*. Natomiast w zakresie ochrony całych zbiorów (chronionych i niechronionych informacji) znalazłaby zastosowanie regulacja odnosząca się do ochrony baz danych. Ten drugi zakres zainteresowń prawników pozostawiam poza prezentowanymi wywodami, gdyż są one przedmiotem innych opracowań przedstawianych na niniejszej Konferencji.

5.1. Ochrona software - trochę historii

Dyrektywa Unii Europejskiej (UE) jest kontynuacją prac podjętych już w 1988 r. Specjalna Komisja Ekspertów EWG opracowała wtedy tzw. "Zieloną Księgę"[14], na temat aktualnych problemów związanych m.in. z ochroną oprogramowania, bazami danych czy piractwem. Od tego czasu znaczenie tych problemów stale rosło i stało się przedmiotem dodatkowego opracowania w dokumencie uzupełniającym do Green Paper w tzw. "Follow-Up" z 1991 r.[15].

Na podstawie zaleceń i wskazówek zawartych w powyższych dokumentach zostały opracowane konkretne dyrektywy Wspólnoty. Pierwszym przygotowanym modelem ochrony była dyrektywa UE w zakresie ochrony *software*. Stała się ona obowiązująca w ramach Wspólnoty od 14.05.1991 r[16]. Kraje członkowskie

---

[14] Zob. EC Green Paper on the Copyright and the Challenge of technology Commission of the European Communities. Doc. COM. 88/172 final, Brussels, 7.06.1988, s.170-204; opublikowana w UFITA 1989, Bd 110, s.118 i n. Por. również; J.A. Appleton, R.J.Hart, Comments on the EC Green Paper Copyright and Challange of Technology, (10) EIPR 1988, s. 287 i n.; A.Franccon, Thoughts on the Green Paper, RIDA 1989, nr 139, s.128 i n.; M.Mollner, On the Subject of the Green Paper, RIDA 1989, nr 141, s.22 i n.

[15] Zob. Follow-Up to the Green Paper, Doc. COM (90) 584 final z 17.01.1991, Brussel.

[16] Por. Official Journal EEC, No. L. 122/91 z 17.05.1991; opublikowane również w WIPR 1991, vol. 5, s.161-162, omówienie tych Wytycznych zob. M.Lehmann, Die Europaische Richtlinie uber den Schutz von Commputerprogrammen, GRUR Int. 1991, nr 5, s. 327 i n.; W. Erdmann, J.Bornkamm, Schutz von Computerprogrammen - Rechtlege nach der EC - Rechtlinie, GRUR 1991, s. 877-880; H.W.Moritz, Die EC - Rechtlinie vom 14.05.1991 uber den Rechtsschutz von Computerprogrammen im Lichte der Bestrebungen zur Harmonisirungdes Urheberrechte, GRUR Int. 1991, s.697-703; T.C.Vinje, Die EEG - Rechtlinie zum Schutz von Computerprogramme und die Frage der Interoperabilitat, GRUR Int. 1992, s. 250-260; w polskiej literaturze Wytyczne omówili J.Barta, R.Markiewicz /w:/ Główne problemy prawa komputerowego, Warszawa 1993; A.Nowicka, Ochrona programów komputerowych w EWG, PiP 1992, nr 7, s. 75 i n.; M.Byrska, Wytyczne EWG w sprawie ochrony

zobowiązały się do dostosowania krajowych regulacji prawnych w terminie do 1 stycznia 1993 roku.

Komisja opracowująca Dyrektywę zdecydowanie preferowała punkt widzenia przedsiębiorstw przemysłowych, co nie powinno budzić zdziwienia biorąc pod uwagę fakt, że UE jest wspólnotą gospodarczą a nie wspólnotą twórców. W kręgach prawników i przedstawicieli przemysłu komputerowego[17] problematyka łączy komputerowych[18] i kwestia zezwolenia na tzw. analizę wsteczną (*reverse engineering*)[19] stały się głównym ogniskiem zapalnym w toczących się rozmowach.

Jednak także kwestia lepszego dopasowania dyrektywy do zasad Konwencji Berneńskiej w wersji paryskiej[20] była przedmiotem dyskusji (chodziło głównie o zabezpieczenie minimalnych praw twórcy).

Prace Komisji poszły w kierunku wypracowania trzech ważnych modyfikacji w

---

programów komputerowych a polski projekt prawa autorskiego, ZNUJ MIW 1993, nr 60, s.61 i n.

[17] Por. komentarz do Wytycznych największych organizacji przemysłowych: UNICE (Union of Industrial and Employers Confederations of Europe), Position Paper, CL & P 1990, s.102 i n; ECIS (European Committee for Introperable Systems), CL & P 1990, s.97 i n.; DGIR (Deutsche Gesellschaft fur Informatik und Recht), CuR 1989, s.960 i n. oraz stanowisko doktryny: M.Sucker, Lizenzierung von Computersoftware. Kartelrechtliche Grenzen nach dem EWG-Vortrag, CuR 1989, s.353 i n.

[18] Łącza komputerowe są rodzajem podprogramów (programy pośredniczące) w układzie: oprogramowanie a sprzęt (*drivers*); oprogramowanie a oprogramowanie (*protocols*); oprogramowanie a człowiek (*machine-human interfaces* zwane też *users interfaces*). Te ostatnie , szczególnie często analizowane w doktrynie prawniczej, realizują przyjazną formę komunikacji i sterowania komputerem przez użytkownika poprzez okna dialogowe, ikony, rozwijanie menu o kilku poziomach, co pozwala na wyeliminowanie funkcji klawiatury i sterowanie komputerem za pomocą myszy. Por. z literatury prawniczej O.Hirakawa, K.Nakano, Copyright Protection of Computer "Interfaces" in Japan, (2) EIPR 1990, s.47 i n.; W.R.Cornish, Inter-operable Systems and Copyright, (11) EIPR 1989, s.391 i n.; M.Lehmann, Freie Schnittstellen ("interfaces") und freier Zugang zu den Ideen ("*reverse engineering*"), CuR 1989, s.1057 i n.; M.Lehmann, T.Dreier, The legal protection of computer programs: certain aspects of the proposal for an (EC) Council Directive,CL & P 1990,s.92 i n.

[19] Por. K.A.Bauer, Reverse Engineering und Urheberrecht, CuR 1990, s.89 i n.; V.Ilzhofer, Reverse - Engineering von Software und Urheberrecht (Eine Betrachtung aus technischer Sicht), CuR 1990, s.578 i n.; M.Kindermann, Reverse Engineering von Computerprogrammen, Vorschlage des Europaischen Parlaments, CuR 1990, s.638 i n.; S.Allott, The EC software directive and the reverse engineering of policy, MIPI 1990, nr 11, s.4 i n.

[20] Konwencja Berneńska z dnia 9 września 1886 r. o ochronie dzieł literackich i artystycznych; Polska ratyfikowała Konwencję i jest związana jej tekstem paryskim z 1971 r., (Dz.U. 1994, nr 104, poz. 506). Por. S.Ricketson, The Bern Convention for the Protection of Literary and Artistic Works: 1886 - 1986, Centre for Commercial Law Studies, Queen Mary College, London 1987; W.R.Cornish, Computer-Programm Copyright and the Berne Convention, (4) EIPR, 1990, s,129 i n.; C.Masouye, Guide to the Berne Convention for the Protection of Literary and Artistic Works, Geneva 1978.

stosunku do materiałów wyjściowych[21]; po pierwsze, przyjęto, że tylko konkretna forma komunikowania się komputera z użytkownikiem jest chroniona prawem autorskim, a nie idea czy zasada leżąca u podstaw samego programu; po drugie, przyznano szerokie możliwości użytkowania nabytego zgodnie z prawem programu, łącznie z prawem testowania programu i poprawiania błędów; po trzecie, wypracowano koncepcję interoperacyjności (*software* z innymi *software* i/lub *hardware*) poprzez wyraźne zezwolenie na "*reverse engineering*" w odniesieniu do łączy komputerowych i przy spełnieniu odpowiednich, ograniczających warunków.

W Polsce programy komputerowe są *expressis verbis* chronione przepisami ustawy o prawie autorskim i prawach pokrewnych[22].

Równolegle do prac podjętych przez Unię Europejską były prace prowadzone w ramach układu "General Agreement on Tariffs and Trade" (GATT)[23]. Ostatnie propozycje USA w ramach obrad GATT zostały zgłoszone w czasie rundy urugwajskiej w 1990 roku[24]. Analiza najistotniejszych fragmentów tych

---

[21] Rozwój prac komisji został przedstawiony w artykułach; G.P.V.Vandenberghe, Copyright protection of computer programs: An unsatisfactory proposal for a Directive, (11) EIPR 1989, s. 409 i n.; I.A.Stains, The European Commission's Proposal for a Concil Directive on the legal protection of Computer Programs, (6) EIPR 1989, s.183 i n.

[22] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. nr 24, poz. 83), zob. M.Byrska, Ochrona programu komputerowego w nowym prawie autorskim, Warszawa 1994; A.Nowicka, Autorskoprawna i patentowa ochrona programów komputerowych, Warszawa 1995.

[23] Układ Ogólny o Taryfach Celnych i Handlu podpisany 30.10.1947 r. w Genewie przez 23 państwa - członków ONZ. Stany Zjednoczone i EWG przeniosły debatę na temat ustanowienia silnej ochrony własności intelektualnej z forum WIPO do GATT, aby obejść obowiązującą w WIPO zasadę jednomyślności. Na terenie GATT Stany Zjednoczone i EWG dysponują także silniejszymi argumentami presji gospodarczej. Próby dyktowania zakresu minimalnej ochrony własności intelektualnej przez te państwa wywołują zrozumiały niepokój państw mniej rozwiniętych. Por; T.Dreier, National Treatment, Reciprocity and Retorsion - the Case of Computer Programs and Integrated Circuits, GATT or WIPO, IIC 1991, s.65-67; Por. również; U.Uchtenhagen, The GATT Negotiations Concerning Copyright and Intellectual Property Protection,IIC 1990, vol.21, s.765 i n.

[24] Art.1. porozumienia urugwajskiego głosi; Contracting parties shall grant to authors and their successors in title, at a minimum, the economic rights provided in the Berne Convention for the Protection of Literary and Artistic Works. (Paris 1971); art.2;(1) Protected works include, inter alia, the following: all types of computer programs (including applications programs and operating systems) expressed in any language, whether in source or object code which shall be protected as literary works; (2) Economic rights include, inter alia, the following; (a) the right to import..., (b) the right to make the first public distribution of the original or each autorized copy of a work..., (c) the right to make a public comunication of a work...Art. 3 Contracting parties shall extend the protection afforded under Art. 1 and 2 to authers of other contracting parties, whether they are natural persons or, the other contracting party's domestic law so provides, legal entitles, and to their successors in title. Art. 5 The term of protection of a work whose author is a legal entity shall be no less than 50 years from authorized publication or, failing such authorized publication within 50 years from the making of the work, 50 years after the making.

propozycji jest interesująca, ponieważ najpełniej ukazuje kierunki legislacyjnych oczekiwań USA w stosunku do ustawodawstw krajowych innych państw. Analiza ta skłania do wyciągnięcia następujących wniosków;

- widoczna jest gotowość do traktowania programów jako części składowej katalogu dzieł z Konwencji Berneńskiej;
- Stanom Zjednoczonym zależy jednak przede wszystkim na zawartych w Konwencji Berneńskiej majątkowych prawach autora, a nie na jego uprawnieniach osobistych;
- do praw majątkowych w pierwszym rzędzie zalicza się prawo do reprodukcji (zwielokrotniania) utworu oraz prawo do tłumaczenia utworu.

W propozycjach GATT - TRIPS zupełnie pominięto problem dekompilacji programów, będący tematem wielu burzliwych sporów wewnątrz Unii Europejskiej. Wydaje się, że USA uważa regulację tej problematyki w obecnym stanie rozwoju za sprawę niezbyt pilną w odniesieniu do mniej uprzemysłowionych państw.

Przemysłowo-ochronny charakter propozycji USA w ramach porozumienia GATT -TRIPS uwidacznia się szczególnie w jego art. 3. Faktycznie jest on dopasowany do regulacji amerykańskiego Copyright Act "*work for hire*"[25] i nie można go odczytać inaczej jak przepisu międzynarodowego prawa prywatnego, którego celem jest skłonienie państw sygnotariuszy umowy do wiążącego przyjęcia w ich systemach prawnych definicji osoby prawnej występującej w prawie autorskim innego państwa.

Art. 10 (1) TRIPS-u stanowi: "programy komputerowe , czy to w kodzie źródłowym czy maszynowym, są chronione jak dzieła literackie w rozumieniu Konwencji Berneńskiej (1971)".

5.2. Przesłanki ochrony oprogramowania

Dyrektywa przewiduje w art. 1 autorskoprawną ochronę programów komputerowych jak dzieła literackiego w rozumieniu art. 2 Konwencji Berneńskiej[26].

Programy komputerowe są chronione w wersji binarnej i źródłowej jak również tzw. "*software* w opakowaniu"[27].

Programy komputerowe według dyrektywy Unii są chronione, gdy spełniają tylko minimalny warunek indywidualności, a zatem także "*kleine Munze*" w postaci programu komputerowego musi uzyskać ochronę autorskoprawną.

Zgodnie z art. 1 ust. 2 Dyrektywy ochrona autorskoprawna nie obejmuje idei i zasad leżących u podstaw programu, jak również idei i zasad leżących u

---

[25] Por. U.S.C. Title 17,Sec. 201 (b): "In the case a work made for hire, the employer or other person for the work was prepared is considered the author (...), and, unless the parties have expressly agreed othewise in a written instrument signed by them, owns all of the rights comprised in the copyright".

[26] Art. 2 Konwencji Berneńskiej stanowi że: wyrazy "dzieła literackie i artystyczne" obejmują wszelkie utwory literackie, naukowe i artystyczne, bez względu na formę ich wyrażenia.

[27] Jest to opisowa forma wprowadzania do obrotu programu komputerowego jako integralnej części składowej urządzenia komputerowego, przyjęta po raz pierwszy przez M.Kindermanna, Vertrieb und Nutzung von Computersoftware aus urheberrechtlicher Sicht, GRUR 1983, s.152 i n.

podstaw łączy między programami (*interfaces, protocols*).

Najwięcej wątpliwości i sporów budzi możliwość objęcia ochroną autorskoprawną algorytmu programu[28].

Algorytm programu nie jest tożsamy z algorytmem merytorycznej metody rozwiązania. Algorytm programu nie może być zatem wyjęty spod ochrony autorskoprawnej, gdyż warunkuje on sposób rozwiązania, sposób kompunikacji ze światem zewnętrznym, budowę struktur danych[29].

W ramach prac UE rozważano wyłączenia łączy programowych, w całości lub w części, z ochrony autorskoprawnej, w celu zapewnienia interoperacyjności pomiędzy programami. Rozważano również możliwość objęcia ich ochroną z zakresu prawa o nieuczciwej konkurencji, zalecając jednocześnie publikowanie tych łączy w ogólnie dostępnych protokołach ("*access protocols*")[30]. Obecnie zostało wyraźnie wyartykułowane w art. 1 ust. 2 Dyrektywy, że jedynie leżące u podstaw złączy komputerowych idee i zasady nie podlegają ochronie. Należy jednak zwrócić uwagę na praktyczny aspekt zagadnienia. Z powodu ciągłego rozwoju normalizacji i standaryzacji łączy programowych tylko w wyjątkowych przypadkach łącza te będą spełniać warunki konieczne do powstania ochrony autorskoprawnej[31], tak więc w praktyce same łącza programowe zwykle nie będą objęte ochroną autorskoprawną. W związku z tym zostały pośrednio spełnione dążenia Komisji EWG do zagwarantowania jak najskuteczniejszej metody zabezpieczającej interoperacyjność systemów komputerowych[32].

Polska ustawa o prawie autorskim przesądza wyraźnie kwestię ochrony programów komputerowych w art. 1 ust. 2 pkt. 1. Ochrona przysługuje niezależnie od spełnienia jakichkolwiek formalności[33]. Nie jest wymagana

---

[28] Zagraniczna literatura na ten temat jest niezmiernie bogata por. H.Haberstumpf, Computerprogramme und Algorithmus, UFITA 1983, nr 95, s.221 i n. oraz cytowana tam literatura; tegoż autora, Der urheberrechtliche Schutz von Computerprogrammen, /w:/ M.Lehmann, Rechtsschutz und Verwertung von Computerprogrammen, Koln 1988, s.36 i n.; odmienne stanowisko zajmuje A.Troller, Urheberrecht und Ontologie, UFITA 1967, nr 50, s.414 i n. W polskiej doktrynie za przyjęciem ochrony algorytmu programu komputerowego wypowiedzieli się: A.Mednis, Program komputerowy jako utwór w rozumieniu prawa autorskiego, PUG 1990, nr 12, s.209 i n.; J.Błeszyński, Ochrona programu komputerowego w świetle prawa autorskiego,PUG 1987, nr 4-5, s.117 i n.; M.Byrska, Zdolność patentowa programów komputerowych, ZNUJ MIW 1992. nr 59, s. 79 i n.; Odmienne stanowisko prezentują J.Barta i R.Markiewicz, Raport, Enter 1991, nr 5, s.45; Szczególnie na uwagę zasługuje dołączony do tego artykułu projekt przepisów dotyczących ochrony programów komputerowych opracowany przez w/w autorów, w którym zostają *expressis verbis* wyłączone spod ochrony autorskoprawnej m.in. algorytmy.

[29] Zob. J.M.Bocheński, Logika i filozofia, Warszawa 1993, s. 347 i n.

[30] Por, M.Lehmann, op.cit.,CuR 1989, s.1085 i n.

[31] Por. M.Lehmann,T.Dreier, op.cit.,CL & P 1990,s.92 i n.; M.Lehmann, op. cit., CuR 1989, s.1057 i n.; W.R.Cornish, op.cit., (11) EIPR 1989, s.391 i n.

[32] Por. K.H.Pilny, Schnittstellen in Computerprogrammen. Zum Rechtsschutz in Deutschland, den USA und Japan, GRUR Int. 1990, s.431 i n.; tegoż autora, Legal Aspects of Interfaces and Reverse Engineering - Protection in Germany, the United States and Japan, IIC 1992, s. 196 i n.

[33] Dla celów dowodowych jest przewidziana rejestracja programów komputerowych

rejestracja programu czy złożenia go do depozytu. Jedynym warunkiem ochrony utworu jest jego ustalenie w jakiejkolwiek postaci.

Rozdział 7 ustawy zawiera przepisy szczególne dotyczące programów komputerowych. Zgodnie z nimi ochroną objęte są wszystkie formy wyrażenia programu. Będzie to więc zarówno oprogramowanie firmowe, oprogramowanie systemowe (system operacyjny), programy tłumaczące - translatory, programy narzędziowe - *software tools*, programy usługowe - *utilities*, programy komunikacyjne - interfejsy obsługi w sieci oraz programy użytkowe (aplikacyjne). Bez znaczenia jest również to, czy chodzi o tzw. wersję źródłową programu (*source code*), czy też o jego wersję przedmiotową (*object code*)[34]. Będą to również wszystkie formy dokumentacji projektowej, wytwórczej i użytkowej.

Jedyną przesłanką ochrony jest stworzenie oryginalnego (indywidualnego) programu komputerowego, który powinien być wynikiem własnej twórczości intelektualnej twórcy (autora). Inne jakościowe czy też estetyczne cechy programu nie mogą stanowić przesłanek oceny czy dany program jest dziełem indywidualnym czy też nie. W Polsce programy komputerowe będą zatem chronione nawet wtedy, gdy będą spełniały tylko minimalny warunek indywidualności.

Analogicznie jak w dyrektywie ochrona autorskoprawna nie obejmuje idei i zasad leżących u podstaw programu, jak również idei i zasad leżących u podstaw łączy między programami (*interfaces, protocols*).

5.3. Autorstwo programu i uprawnieni do korzystania z ochrony

Podobnie jak w Dyrektywie, polskie prawo autorskie przewiduje, że twórcą programu jest każda osoba fizyczna lub grupa osób -współautorzy (art. 8 i 9 pr. aut.), którzy stworzyli oprogramowanie. Zgodnie z art. 74 ust. 3 pr. aut. "prawa majątkowe do programu komputerowego stworzonego przez pracownika w wyniku wykonywania obowiązków ze stosunku pracy przysługują pracodawcy, o ile umowa nie stanowi inaczej". Literalana interpretacja tego przepisu wskazuje na pierwotne nabycie uprawnień majątkowych przez pracodawcę. A zatem pracownik musi zadbać w klauzulach umownych o przyznanie mu określonych praw majątkowych względem "pracowniczego" programu.

Przyznanie pracodawcy wszelkich autorskich praw majątkowych, przy równoczesnym pominięciu kwestii wynagrodzenia dla twórcy, przesądza o tym, że poza wynagrodzeniem wynikającym ze stosunku pracy, eksploatacja programu przez pracodawcę nie upoważnia twórcy do żądania honorarium autorskigo. Dotyczy to również wykorzystywania "na zewnątrz" programu przez pracodawcę, czy to w pierwotnej wersji czy też zmodyfikowanej.

Pracodawca jest upoważniony do wprowadzania istotnych zmian w programie bez porozumienia się z twórcą, w tym zlecania dokonywania takich zmian osobom trzecim. Jeżeli twórca nie chce dopuścić do takiej sytuacji musi dołączyć odpowiednie klauzule do umowy o pracę.

Prawa nabyte *ex lege* przez pracodawcę nie są ani czasowo[35] ani terytorialnie ograniczone. A zatem po zakończeniu stosunku pracy program pozostaje w dyspozycji pracodawcy. Sprawa ta może być również odmiennie uregulowana w umowie o pracę.

---

m.in. w USA, Hiszpanii czy Japonii.

[34] Program tłumaczący tworzy wersję binarną z programu źródłowego napisanego w języku zewnętrznym - autokodach.

[35] Z wyjątkiem normalnego czasowego ograniczenia wykonywania autorskich praw majątkowych.

5.4. Wyłączne prawa autora programu

Dyrektywa opowiada się za tradycyjną konstrukcją wyłącznych praw przysługujących autorowi programu komputerowego przy jednoczesnym wprowadzeniu wyjątków ograniczających treść tych praw. I tak art. 4 Dyrektywy wylicza podstawowe prawa majątkowe przysługujące podmiotowi prawa, a art. 5 Dyrektywy nakłada na te prawa pewne ograniczenia. Zgodnie z nimi każdemu uprawnionemu nabywcy względnie licencjobiorcy zostaje przyznane (nawet jeżeli w umowie nie jest to ujęte) minimum praw do użytkowania danego programu. Podobnie art. 6 Dyrektywy regulujący analizę wsteczną ("dekompilację") programu ogranicza wyłączne prawa majątkowe jego autora.

Zgodnie z art. 4 Dyrektywy zastrzeżone zostały dla autora programu komputerowego następujące prawa wyłączne. Każda osoba trzecia musi uzyskać zgodę autora programu komputerowego na podjęcie działalności handlowej związanej z dystrybucją danego programu. Również autor musi wyrazić zgodę na każde trwałe lub tymczasowe powielenie (zwielokrotnienie) całego lub części programu komputerowego, obojętnie za pomocą jakiego środka lub w jakiej formie dokonane, jak również musi wyrazić zgodę na wszelkie modyfikacje programu. Termin "powielenie" bliżej nie jest zdefiniowany w Dyrektywie. Wydaje się być zapożyczony z anglo-amerykańskiej wersji *copyright*[36]. Zgodnie z tym ujęciem zakres pojęciowy terminu powielenie zawiera w sobie krótko czy długoterminowe odtworzenie dzieła zgodnie z jego przeznaczeniem *"in any medium by electronic means"*.

Identyczną regulację wprowadziła polska ustawa w art.74 ust. 4 pkt (1), (2) i (3). Wyjątek stanowi ustawowe upoważnienie użytkownika do "normalnej" eksploatacji programu w ramach takich czynności jak: wprowadzanie, wyświetlanie, stosowanie, przekazywanie i przechowywanie, bez zgody uprawnionego, nawet, gdy wykonywanie tych czynności wymaga zwielokrotnienia programu (art. 74 ust. 4 pkt 1 zdanie drugie).

5.5. Uprawnienia użytkownika

Art. 5 ust. 2 i 3, zgodnie z art. 9 ust. 1 zdanie 2 Dyrektywy zawiera bezwzględne uprawnienie użytkownika do wykonania kopii rezerwowej i testowania przebiegu programu, przy czym to ostatnie uprawnienie, w relacji do art. 6 Dyrektywy, służyć ma przede wszystkim ustaleniu idei i zasad leżących u podstaw struktury programu. Uprawnienia te nie mogą być ograniczone postanowieniami umownymi.

Art. 5 ust. 1 Dyrektywy zawiera natomiast względne ograniczenie praw wyłącznych. Nabywca może być pozbawiony pierwotnie przyznanych mu praw minimalnych na podstawie *lex contractus*. Ograniczenia wynikające z konkretnej umowy mogą co najwyżej podlegać kontroli poprzez prawo o nieuczciwej konkurencji czy ustawę dotyczącą ogólnych warunków umów.

Przekazanie *software* w ramach umowy licencyjnej nakładałoby również pewne ograniczenia w użytkowaniu (ograniczenie korzystania nie więcej niż z jednego twardego dysku, zakaz wielokrotnego użytkowania programu, zakaz korzystania z sieci przedsiębiorstwa itp.). W przypadku sprzedaży kopii programu, jeżeli nie

---

[36] Por. sec.17 brytyjskiego Copyright, Designs and Patent Act 1988, oraz sec. 191 amerykańskiego Copyright Act zgodnie z którym "the term "copies" includes the material objects, other than phonorecords, in which the work is first fixed by any method now know, or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device".

ma szczególnych postanowień umownych, dopuszczalna powinna być każda czynność podejmowana przez nabywcę gdy jest ona konieczna dla zgodnego ze swym przeznaczeniem użytkowaniem danej kopii. Takie rozstrzygnięcie posiada znaczenie w przypadku dzielenia programu czy jego przenoszenia, jak też w przypadku konserwacji programu[37]. Przepis art. 6 Dyrektywy, dotyczący dekompilacji programu komputerowego, ma charakter bezwzględnie obowiązujący. Oznacza to, że ani sprzedawca ani licencjodawca programu nie może narzucić użytkownikowi ograniczeń umownych zawężających przyznane mu prawo do dekompilacji (art. 9 ust. 1 zdanie 2 Dyrektywy). Tym samym z zakresu praw wyłącznych autora zostaje wykluczone prawo do powielania i modyfikowania programu w rozumieniu art. 4 (a) i (b) Dyrektywy.

Dekompilacja jest jedynie dozwolona w przypadku konieczności opracowania łączy programowych i dopuszczalna jest tylko wtedy gdy interoperacyjności programów komputerowych nie można osiągnąć w inny sposób. Art. 6 Dyrektywy zezwala co najwyżej każdemu użytkownikowi na zestawienie swego systemu komputerowego z komponentów różnego pochodzenia - jak w zabawie klockami - bez narażenia się na niebezpieczeństwo, iż te części systemowe mogłyby nie współgrać ze sobą interoperacyjnie w sposób optymalny. Być może przyszła normalizacja problematyki łączy komputerowych usunie wiele kontrowersji nękających obecnie rynek programów komputerowych. Przyczyniłby się do tego z pewnością wymóg publikowania informacji dotyczących łączy komputerowych przez przedsiębiorstwa zajmujące kluczową pozycję na rynku. W takiej sytuacji art. 6 Dyrektywy stałby się zbyteczny.

Polska ustawa o prawie autorskim przejmuje prawie dosłownie rozstrzygnięcia zaproponowane w Dyrektywie w zakresie przesłanek dotyczących celu dokonywania dekompilacji, zakresu dekompilacji (części programu) oraz upoważnia analogiczne osoby do jej przeprowadzenia. Nie występuje natomiast w polskiej ustawie klauzula generalna ujęta w art. 6 ust. 3 Dyrektywy. Nie będzie się zatem badało czy dopuszczenie dekompilacji programu może naruszać słuszne interesy uprawnionego względnie normalną eksploatację programu komputerowego. W świetle powyższych uwag, rezygnacja z tego rodzaju ograniczenia dekompilacji wydaje się uzasadniona.

6. Konkluzje

Odważne podjęcie wyzwania technologicznego musi iść w parze z wcześniej ustalonymi regulacjami prawnymi, zabezpieczającymi prawa jednostki i interesy państwa bez szkody dla jednych i drugich. Unormowania międzynarodowe - to sprawa nie tylko wyobraźni, ale też element społecznego bezpieczeństwa.

Polska technicznie bardzo dobrze się rozwija. Natomiast zastrzeżenia można mieć do naszej normalizacji prawnej. Kłopoty które dzisiaj dręczą Amerykanów czy Francuzów już niedługo staną się kłopotami Polaków. Przykład piractwa komputerowego, wideo czy CD, z którymi to zjawiskami walczymu *post factum*, dowodzi braku wyprzedzającej regulacji prawnej. Dziesięć lat temu *cyberspace* była pomysłem pisarza *science-fiction*, dziś stała się przedmiotem obrad Ministrów Unii Europejskiej a już jutro będzie naszym problemem.

---

[37] Konserwacja programu nie zastała wyraźnie wymieniona w Dyrektywie.

Wykaz skrótów używanych w opracowaniu

CL&P - Computer Law and Practice,

CuR - Computer und Recht,

Dz.U. - Dzennik Ustaw,

EIPR - European Intellectual Property Review,

GRUR - Gewerblicher Rechtsschutz und Urheberrecht,

GRUR Int.- Gewerblicher Rechtsschutz und Urheberrecht - Internationaler Teil,

IIC - International Review of Industrial Property and Copyright Law,

MIPI - Managing Intellectual Property Issue,

PiP - Państwo i Prawo,

pr.aut. - polska ustawa o prawie autorskim i prawach pokrewnych z 1994 r.,

PUG - Przegląd Ustawodawstwa Gospodarczego,

RIDA - Revue International du Droit d'Auteur,

UFITA - Archiv für Urheber-, Film- und Theaterrecht,

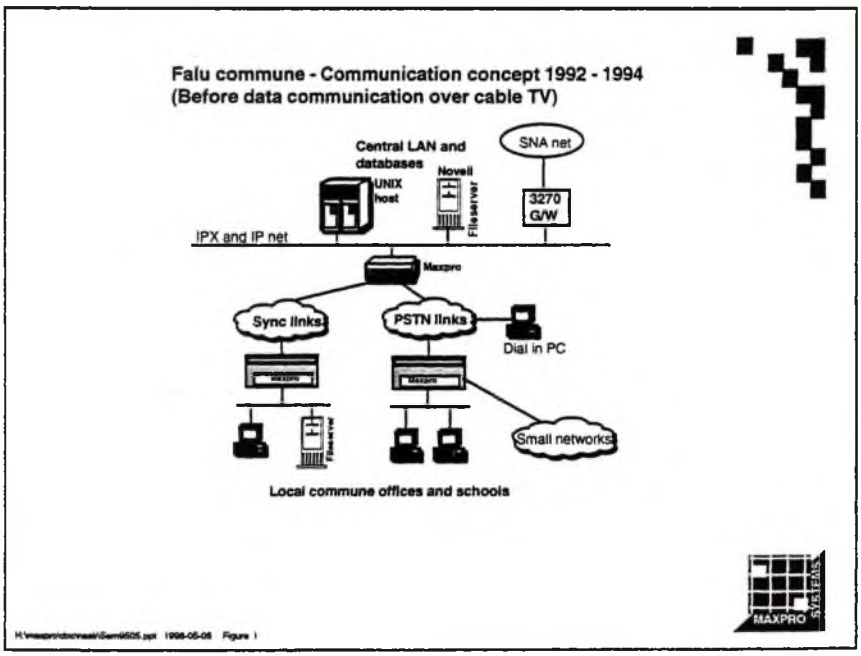
WIPR - World Intellectual Property Report,

ZNUJ MIW- Zeszyty Naukowe Uniwersytetu Jagiellońskiego. Prace z Wynalazczości i Ochrony Własności Intelektualnej.

INTERNET OVER CABLE TV
Case study - Falun City, Sweden

Jan Persson

Maxpro Systems



Falu commune network 1992 - 1994

During the period 1992 to 1993 the design phase and call for tender took place.

The first Maxpro installations was made during 1993 - 1994.

Central LAN and databases

The communities central LAN supports a city with around 50.000 citizens.

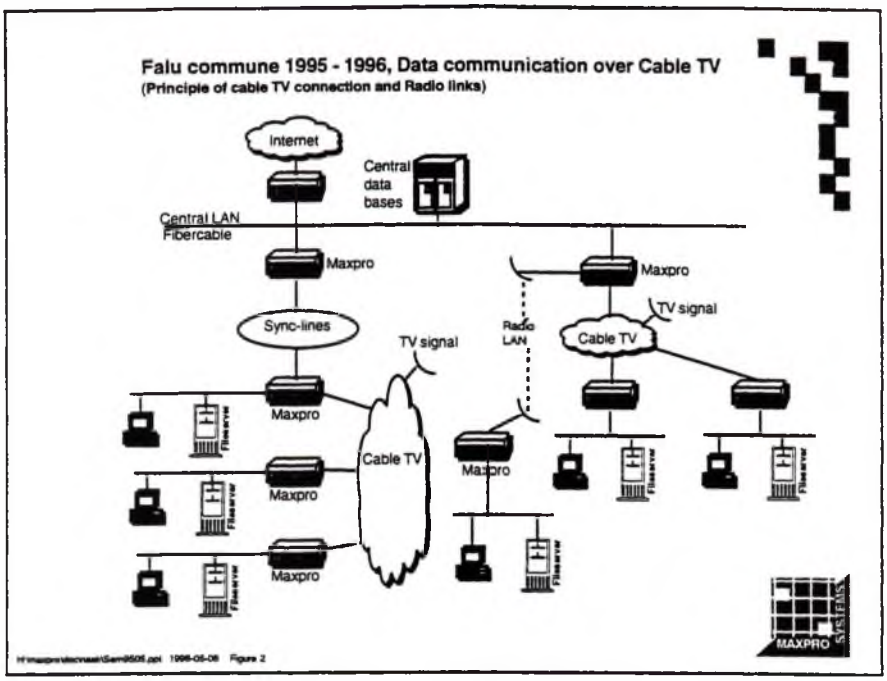
Common databases and common service applications are used by the local offices. Access to IBM main frame via the gateway, its a common service for all users. The number of users are approximately 1000.

Local offices

Local offices are connected to the central site via leased lines, PSTN lines (async) and some few ISDN lines. Local offices are the community different service organizations as school offices, security and fire-brigade, social welfare, e t c. 10 - 12 local offices with there own small offices was installed during the period.

Conclusion

The management group for datacommunication summarized that the price for operation of the network (leased line, isdn line, pstn lines) was going to be expensive with all offices connected in a network, totally more then 50 offices. The management group started to look for other solutions connecting the commune local offices together.



Falu commune current network installation

During 1995 a solution with cable TV and datacommunication was designed and installed. All routing traffic are based on Maxpro System servers (access servers and routers). The Maxpro System equipment was chosen because of the flexible interface options Maxpro can offer.

Cable TV and datacommunication net

The current number of cable TV access points for datacommunication are 45. Local offices located on longer distance from the central lan are connected via high speed links (sync links). The price per cable TV access point is $1400-1500 per year.

Radio Lan

In some locations where its difficult with cable TV lines, Falu commune and Maxpro Systems has interfaced the Maxpro equipment to Radio Lan.

One Radio Lan installation for test has been running for some months. The testresult is excellent and Falu commune is now planning for more Radio Lan installations.

Internet connection

The schools are connected to Internet via firewalls and Maxpro router servers and are totally separated from the commune administrative services. The administrative services personal uses the Internet connection for E-mail application and other services in Internet.

CERT NASK: ZESPÓŁ REAGUJĄCY NA ZDARZENIA W SIECI

Krzysztof Silicki

Naukowa Akademicka Sieć Komputerowa
Warszawa ul Bartycka 18

Streszczenie:
W referacie omówiono tematykę funkcjonowania w Internecie zespołów reagujących na zdarzenia naruszające bezpieczeństwo sieci (ang. IRT - Incident Response Team). Scharakteryzowano historię i obecne dokonania IRTów na świecie, cele funkcjonowania zespołów oraz na tym tle powołanie w NASK zespołu NASK CERT (NASK Computer Emergency Response Team)

Sieć Internet posiada specyficzne właściwości, które w dość oczywisty sposób wpływają na problematykę bezpieczeństwa w tej sieci. Jest to sieć o globalnym zasięgu, której prapoczątki sięgające sieci ARPA i założenia przyjęte przez budowniczych Internetu wyznaczyły kierunki rozwoju gdzie bezpieczeństwo pracy w sieci jest raczej problemem stałej troski niż zasadą wpisaną w Internet.

Sieć Internet charakteryzuje się między innymi tym, że:

- nie ma właściciela,
- nie posiada centralnej kontroli,
- nie istnieje centralny autorytet mogący coś narzucić społeczności Internetu,
- brak jest standardowej, zaakceptowanej przez wszystkich polityki (np. bezpieczeństwa),
- brak jest międzynarodowego prawodawstwa w dziedzinie przestępstw komputerowych.

Problematyka streszczona powyżej jest coraz bardziej istotna w kontekście przyszłości Internetu, która rysuje się w postaci wzrostu zainteresowania tą siecią ze strony tzw. użytkowników nie tradycyjnych (a więc spoza szeroko pojętego środowiska uczelnianego). Zainteresowanie tą siecią użytkowników komercyjnych, bankowości, administracji i innych wymusza profesjonalizację sieci i wzrost zainteresowania problematyką bezpieczeństwa traktowaną coraz częściej jako być albo nie być Internetu. Ma to szczególny wydźwięk także w kontekście zainteresowania Internetem rozmaitych grup anarchizacyjnych czy przestępczych.

Ataki na komputery w sieci

Na rozmaitych słabościach Internetu żerują tzw. włamywacze do sieciowych systemów komputerowych. Niektórzy robią to dla zabawy (rodzaj gry intelektualnej), inni prowadzą destrukcję w imieniu własnym lub na zlecenie (anarchiści, przestępcy, nihiliści) - istnieje też działalność wywiadowcza na tym polu. Typowy atak wpisuje się w następujący scenariusz:

- zlokalizowanie systemu do zaatakowania
- zdobycie dostępu do konta legalnego użytkownika systemu
  - brak hasel lub łamanie łatwych haseł
  - podsłuchane hasła (sniffery)
- Wykorzystanie dziur w konfiguracji i w oprogramowaniu systemowym w celu wejścia na konto uprzywilejowane
- Zatarcie śladów działalności (usunięcie zapisów z pamiętników - auditing records)
- przeprowadzenie nieuprawnionych działań
- zainstalowanie „konia trojańskiego" dla aktualnego i przyszłego wykorzystania
- ataki na inne komputery w sieci lokalnej

Intruzi atakujący systemy komputerowe znajdujące się w sieci częstokroć posługują się kilkoma złamanymi wcześniej kontami na różnych maszynach logując się kolejno z jednego na drugie. Utrudnia to śledzenie miejsca, z którego tak naprawdę przeprowadzony był atak.

Ataki na systemy komputerowe dokonywane poprzez sieć mają wieloletnią historię. Przez lata zmienił się profil i natężenie ataków. Jednakże sposoby włamywania się stosowane przed laty są także wykorzystywane dziś - stale powiększa się arsenał środków jakie są wykorzystywane przez intruzów w celu nieautoryzowanego dostępu do systemów. Poniżej przedstawiono ewolucję typowych ataków na przestrzeni lat:

- 1988
  - wykorzystywanie słabych haseł
  - wykorzystywanie znanych słabych punktów w systemach
- 1993
  - wykorzystywanie słabych haseł
  - wykorzystywanie znanych dziur
  - instalowanie programów przechwytujących (sniffer)
  - analiza kodów źródłowych w celu wykrycia nieznanych słabych punktów
  - wykorzystywanie anonymous ftp

Profil ataków roku 1994

- Ataki poprzez „sniffery:
  - przechwycenie haseł wielokrotnego użycia
  - zdobycie dostępu do root-a przy pomocy rozpropagowanych w sieci „narzędzi"
  - wymiana oprogramowania detekcyjnego na moduły konia trojańskiego

- Ataki związane z pocztą elektroniczną
  - wykorzystanie słabości sendmail-a
  - e-mail spamming

- Ataki poprzez NFS
  - przy użyciu szeroko rozpropagowanego „narzędzia"

- Ataki poprzez NIS

Rok 1995

Jednym z niebezpieczniejszych typów ataków jaki stał się „popularny" w roku 1995 jest atak typu IP spoofing.

Metoda IP spoofing była dyskutowana teoretycznie już w 1985 roku. Ataki są skuteczne nawet poprzez przegrody ogniotrwałe (firewall) jeśli nie zablokowano przepuszczania pakietów o adresie źródłowym i docelowym pochodzącym z sieci lokalnej.

Ataki na infrastrukturę internetową

Oprócz ataków na serwery użytkowników coraz częstsze w Internecie są ataki na urządzenia infrastruktury zapewniającej działanie Internetu. Są to między innymi:

- Ataki na routery
  - intruzi potrafią zmodyfikować konfigurację routerów
- Ataki na nameserwery

Ataki na inne „strategiczne" serwery

Zespoły reagujące na zdarzenia

W tak potencjalnie niebezpiecznym środowisku gdzie liczba incydentów naruszających bezpieczeństwo sieci stale rośnie (a potwierdzają to dane zbierane przez organizacje zajmujące się tym zagadnieniem) zaczęły powstawać zespoły, które w zorganizowany sposób reagują (głównie od strony technicznej na sygnały o wystąpieniu zdarzenia). Pierwszym sformowanym centrum zatrudniającym ludzi dedykowanych do reagowania na pojawiające się w Internecie zagrożenia jest działający od roku 1988 CERT Coordination Center zlokalizowany w Carnegie Mellon University. Sformowanie CERT/CC nastąpiło bezpośrednio po osławionym incydencie 'internet worm' - który zablokował na kilkanaście godzin wiele komputerów dołączonych w 1988 roku do sieci. jak misję strategiczną CERT/CC przyjął:

- stworzenie wiarygodnego i niezawodnego dwudziestoczterogodzinnego punktu kontaktowego dla zgłaszania niebezpieczeństw w sieci,

- zapewnienie komunikacji pomiędzy ekspertami pracującymi nad rozwiązywaniem określonych problemów z dziedziny bezpieczeństwa,

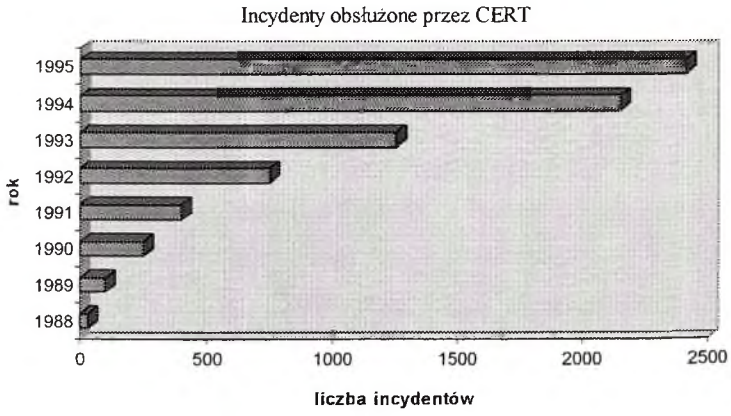
- stworzenie centralnego miejsca identyfikowania i niwelowania problemów wynikających z niedopracowania systemów komputerowych,

- działanie w dziedzinie badań nad poprawieniem bezpieczeństwa w istniejących systemach,

- działanie w kierunku propoagowania wiedzy w celu zwiększenia świadomości o problemach bezpieczeństwa wśród szerokiej rzeszy użytkowników Internetu.

W roku 1995 CERT/CC otrzymał 32 tysiące listów pocztą elektroniczną i prawie 3,5 tysiąca zgłoszeń za pomocą gorącej linii telefonicznej. Obsłużono 2412 incydentów (od początku działalności - ponad 7 000). Ponad 12000 lokalizacji na całym świecie było dotkniętych incydentami.

Poniżej diagram wzrostu obsłużonych przez CERT incydentów:



Z rocznego raportu CERT/CC wynika, że najgroźniejszymi klasami ataków w roku 1995 były:

* IP spoofing (w przeciągu kilku letnich tygodni miało miejsce ponad 170 ataków tego typu, które w większości przypadków skończyły się udanymi włamaniami)

* NFS (ataki poprzez słabości Network File System rozwinęły się w roku 1995 - pojawiły się wśród intruzów programy , które automatyzują ataki tego typu)

* Skanowanie sieci

* Sniffery (podsłuchiwanie pakietów w celu wyłapywania haseł za pomocą instalowanych przez intruzów pakietów)

* Ataki poprzez sendmail

Pod koniec roku nasiliły się ataki m.in na sieci dostarczycieli usług co zaowocowało wydaniem przez CERT generalnego ostrzeżenia o niebezpieczeństwie.

Jednym z ważniejszych przejawów działalności CERT/CC jest wydawanie tzw. „advisory" czyli tematycznych publikacji elektronicznych dotyczących pojawiających się zagrożeń. Zawierają one opis problemu, niebezpieczeństwa, potencjalne skutki dla różnych systemów operacyjnych oraz środki zaradcze.

W ciągu lat powstało na świecie wiele zespołów reagujących na zdarzenia naruszające bezpieczeństwo sieci. CERT/CC nadal jest centralnym miejscem i organizacją o światowym zasięgu jednakowoż wiele krajów posiada własne centra np. DFN - CERT w Niemczech, CERT-IT we Włoszech i wiele innych. Niektóre zespoły powstały przy „branżowych' centrach jak chociażby CIAC (Computer Incident Advisory Capability) działający z ramienia amerykańskiego Departamentu Energii.

Poszczególne IRTy (IRT: Incident Response Team) współpracują ze sobą w celu wymiany doświadczeń, ostrzeżeń itp. gdyż wiele z powstających zdarzeń naruszających bezpieczeństwo ma charakter rozległy czy wręcz międzynarodowy. Powstało także forum zrzeszające zespoły tego typu o nazwie: FIRST czyli Forum of Incident Response and Security Teams

Przygotowanie i reakcja

Zgodnie z zaleceniami bezpieczeństwa każda organizacja (sieć) powinna wypracować sobie model, który wyraża się w czynnościach takich jak:

- zidentyfikowanie dostępnych zasobów
- stworzenie program bezpieczeństwa
- zaplanowanie systemu reagującego

Intruzi są bowiem przygotowani i zorganizowani. Wykorzystują wszelkie dostępne media jak:

- modemy
- poczta elektroniczna
- BBS-y
- serwery FTP
- konferencje

Nie każdą organizację stać jednak na utrzymywaniu zespołu, który zawodowo będzie zajmował się obsługą zdarzeń naruszających bezpieczeństwo czy też w ogóle był na bieżąco z zagrożeniami. Jednakże jest celowe aby powstawały zespoły w ramach tych organizacji, które mogą nieść pomoc dla innych w celu skoordynowania całości problemu bezpieczeństwa w danym kraju czy rejonie.

Cele sformowania zespołu reagującego na zdarzenia

Wśród głównych misji jakie przyjmują powstające zespoły można wymienić:

- wsparcie dla scentralizowanego, skoordynowanego i stałego reagowania
- szybkie i efektywne reagowanie i pomoc dla „poszkodowanych"
- techniczna wsparcie dla potrzebujących oraz rozpropagowywanie wiedzy z dziedziny network security

Struktura zespołu

Wśród zespołów reagujących na zdarzenia istniejących na świecie można wyróżnić dwa podstawowe modele: zespół scentralizowany vs. zespół rozproszony

Zespół rozproszony

- zespół bliżej lokalnych problemów
- użytkownicy dobrze znają osoby , którym zgłaszają problem

Zespół centralny

- pracownicy „dedykowani"
- łatwo uzyskać odpowiedni poziom odpowiedzialności
- jedno miejsce przechowywania poufnych informacji

Formalne umocowanie zespołu

Jednym z istotnych obszarów, które decydują w ogóle o możliwości spełnienia funkcji IRT (Incident Response Team) jest strona formalna.
Zespół bowiem musi mieć instytucjonalną organizację - nie może być zawieszony w próżni.
Przedsięwzięcie wymaga także desygnowania określonego budżetu m.in na:

- organizację struktury (personel, pomieszczenie, wyposażenie)
- utrzymanie ciągłe

CERT NASK

Wobec narastającej fali incydentów naruszających bezpieczeństwo systemów dołączonych do sieci Internet na świecie i w Polsce oraz wobec faktu powstania i dalszego powstawania w wielu krajach gdzie istnieje sieć Internet zespołów reagujących na zdarzenia naruszające bezpieczeństwo w NASK podjęto inicjatywę powołania zespołu o nazwie NASK-CERT. Jest to zgodne z międzynarodowymi tendencjami przeciwdziałającymi szerzeniu się w sieciach incydentów

naruszających bezpieczeństwo. Odpowiednie zarządzenie Dyrektora NASK w sprawie powołania zespołu zostało wydane w marcu 1996 roku.

Do zadań zespołu CERT- NASK należy m.in:

- rejestrowanie zdarzeń naruszających oraz bezpośrednio zagrażających bezpieczeństwu sieci NASK, sieci abonentów NASK oraz sieci innych operatorów

- natychmiastowe podejmowanie czynności takich jak: diagnozowanie, analizowanie, znoszenie lub pomoc w znoszeniu skutków zdarzeń naruszających bądź bezpośrednio zagrażających bezpieczeństwu sieci NASK i sieci abonentów NASK oraz czynności zapobiegających powstawaniu tych zdarzeń w przyszłości,

- współpraca z zespołami o podobnym charakterze działającymi samodzielnie lub będącymi jednostkami organizacyjnymi innych podmiotów prawnych, krajowymi i zagranicznymi - w szczególności z międzynarodową organizacją FIRST (Forum of Incident Response and Security Teams) zrzeszającą zespoły reagujące na zdarzenia,
- alarmowanie użytkowników sieci o wystąpieniu bezpośrednich dla nich zagrożeń,

- prowadzenie stałej działalności informacyjno-zapobiegawczej mającej na celu podniesienie świadomości i troski użytkowników o właściwy stan bezpieczeństwa sieci.

Idea i koncepcja zespołu reagującego funkcjonującego w ramach struktury międzynarodowej zrzeszającej tego typu zespoły z całego świata została także przedstawiona w raporcie: „Opracowanie mechanizmów bezpieczeństwa i poufności pracy sieci i centrów KDM" opracowanym przez NASK na zamówienie Komitetu Badań Naukowych .

CERT NASK składa się z pracowników Naukowej Akademickiej Sieci Komputerowej oraz grupy współpracujących specjalistów spoza NASKu. W ramach prowadzonej działalności istnieje także współpraca z ekspertami w miarę pojawiania się zadań do wykonania. Zespół działa od przełomu stycznia i lutego bieżącego roku. W tym czasie zarejestrowano kilkadziesiąt zdarzeń z następujących kategorii:

a) międzynarodowe

- próby włamań do systemu w Polsce z terenu USA,

- włamanie do systemu w jednym z krajów Europy z terenu Polski,

- sygnały o domniemanych atakach z Polski na systemy w krajach Ameryki Łacińskiej

b) krajowe

- informacje ostrzegające dla administratorów komputerów , które są zagrożone lub spenetrowane przez hackerów,

- próby i udane przypadki włamań zgłaszane przez administratorów systemów w kraju,

c) lokalne

Wśród sygnałów docierających do CERT NASK (np. od innych CERTów) są także domniemane próby ataków (np. z terenu Polski do innych krajów), które po wyjaśnieniu sprawy okazują się być fałszywymi alarmami. Jednakowoż sam fakt konsultowania zdarzeń pomiędzy CERTami różnych krajów (w tym NASK CERT) oraz w następstwie kontakty bezpośrednie pomiędzy właściwymi stronami zaangażowanymi w dane zdarzenie świadczy, że Polska nie jest białą plamą na Internetowej mapie reagowania na sytuacje zagrażające bezpieczeństwu sieci. Jedną z ważniejszych cech działania systemu koordynującego zagadnienia związane z występowaniem zagrożeń w sieci jest ścisła współpraca pomiędzy zespołami w różnych krajach. Jak wspomniano koordynacją tego typu współpracy zajmuje się organizacja o nazwie FIRST. Ważnym obszarem przepływu danych pomiędzy zespołami są statystyki incydentów jakie udało się zarejestrować w obszarze działania danego zespołu i bieżąca współpraca w razie wystąpienia incydentów o zasięgu międzynarodowym. Przekazywane dane są na tyle szczegółowe na ile wymaga to prowadzenie statystyk lub analiza techniczne problemu - rygorystycznie przestrzegana jest tu zasada o prawie do tajemnicy poszkodowanego w zakresie incydentu, który go dotyczył.

Jest niezwykle istotne, aby sygnały o próbach włamań i udanych włamaniach docierały do właściwych zespołów reagujących:

a) z powodów „statystycznych"

b) z powodów „rodzajowych" (typy ataków)

c) w celu uzyskania pomocy jeśli poszkodowany tego sobie życzy

FIRST

FIRST jest międzynarodowym konsorcjum (stowarzyszeniem) grup reagujących na komputerowe zdarzenia. Grupy pracują razem aby obsłużyć zdarzenia z dziedziny komputerowej ochrony danych i promować akcje prewencyjne.

Misją FIRST jest:

- dostarczać członkom technicznych informacji, narzędzi, metod, pomocy i wskazówek;
- koordynować czynności wykonawcze i analityczne wsparcie;
- wspierać rozwój jakościowy produktów i serwisu;
- poprawiać narodową i międzynarodową ochronę informacji dla rządów, przemysłu prywatnego, akademii i osób prywatnych.

Aby wypełnić tę misje FIRST musi osiągnąć dwa cele strategiczne:

- wewnętrzną poprawę działalności i organizacji FIRST żeby spełnić potrzeby zmieniającego się środowiska;
- ugruntować i wzmocnić FIRST w zakresie koncepcji reagowania na zdarzenia.

Powyższe cele są osiągalne poprzez:

- wiarygodność i współpracę
- efektywną komunikację
- koordynację
- wspólne badania i rozwój
- dzielenie się narzędziami, technikami i informacjami
- edukację
- organizację

- fundusze wspomagania i współdziałanie

W tej chwili w samej Eropie jest juz kilka zespołów, które uzyskały członkostwo w FIRST natomiast zgodnie z informacjami uzyskanymi w czasie konferencji 7th FIRST w Karlsruhe w 1995 r kilka kolejnych krajów jest w fazie organizacji zespołów do spraw bezpieczeństwa (Słowenia, Dania, Czechy, Słowacja, Luksemburg, Chorwacja)

Firewalle i bezpieczeństwo w sieci Internet

Sławomir Górniak, Piotr Kijewski

Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
e-mail: {S.Gorniak|P.Kijewski}@tele.pw.edu.pl

Wprowadzenie

Sieć Internet z każdym miesiącem obejmuje coraz więcej węzłów, co powoduje lawinowe zwiększanie się liczby użytkowników - jest to normalne, zważywszy na ogromne możliwości szybkiej wymiany informacji pomiędzy dwoma komputerami. Internetem przesyła się najróżniejsze dane, od pozbawionych znaczenia, do bardzo ważnych. Istotne więc jest zabezpieczenie tych danych przed niepowołanymi osobami.

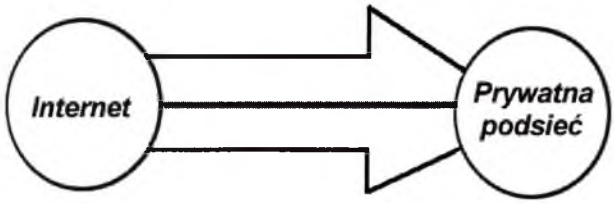
Koncepcja włamań

Każdy administrator komputera podłączonego do Internetu, szczególnie pracującego w systemie UNIX, musi sobie zdawać sprawę z tego, że jego komputer prędzej czy później stanie się potencjalnym wyzwaniem dla włamywacza. UNIX jest najlepszą platformą dla aplikacji internetowych, niestety system ten posiada wiele słabych punktów pod względem bezpieczeństwa danych. Pomimo, że firewalle nie są koniecznie związane z UNIXem, odnosić się będziemy właśnie do takiej konfiguracji. Zdarzają się różni włamywacze - jedni traktuja włamania jak sport, inni poszukują konkretnych informacji. Spotkanie z pierwszymi może być czasem gorsze w skutkach niż z drugimi, ponieważ początkujący włamywacz w obawie przed wykryciem go może nie powstrzymać się na przykład od skasowania wszystkich danych znajdujących się na dysku komputera.

Na czym w ogóle polegają włamania do systemu UNIX? Najczęściej włamywacz - zwany także hackerem lub crackerem - pragnie początkowo uzyskać zdalny dostęp do atakowanej maszyny i rozpocząć na niej sesję zwykłego użytkownika. Następnie, wykorzystując rozmaite błędy w systemie, próbuje on zdobyć dostęp do praw administratora komputera - gdy już je dostanie, integralność danych zgromadzonych w tym komputerze leży całkowicie w jego rękach. Błędy w systemie polegać mogą na wykorzystaniu źle napisanych lub skonfigurowanych programów z *Set User ID* lub *Set Group ID*. Określenie to oznacza, iż dany program uruchamiany jest z przywilejami albo właściciela pliku (najczęściej jest nim administrator systemu - *root*) albo grupy czyjej własnością jest ten plik. Umiejętne posłużenie się takim programem może spowodować otrzymanie praw administratora.

Administrator systemu ma za zadanie tak go skonfigurować, aby zmniejszyć maksymalnie prawdopodobieństwo pomyślnego włamania. Całkowicie bezpieczne systemy niestety nie istnieją, dlatego też zadanie to jest bardzo ważne. Należy więc między innymi instalować „patch-e" publikowane regularnie przez producenta używanego systemu - są to poprawki usuwające błędy w firmowym oprogramowaniu. Powinno się dokładnie kontrolować przychodzące pakiety, co umożliwiają programy w stylu TCP-wrappers, rozszerzające możliwości logowania komunikatów systemowych. Logi takie powinny być umieszczone w komputerze do którego dostęp mają tylko zaufani ludzie. Administrator powinien bardzo uważać na konfigurację komputerów w swojej podsieci. Jeśli w podsieci w której znajduje się kilkadziesiąt komputerów „ufających sobie" znajdzie się choćby jeden źle zabezpieczony, to właśnie on wyznacza jakość zabezpieczeń - włamywacz może przejść na inne komputery używając jako bazę właśnie ten komputer. Powoduje to konieczność chronienia każdego z komputerów w danej podsieci, a i nawet to nie gwarantuje pewności. Należy także uważać na to, by nie instalować w systemie zbędnych usług oraz programów mogących zmniejszyć bezpieczeństwo. Powinno za to się

instalować jak najwięcej różnych zabezpieczeń - nie można wierzyć, że jeden typ zabezpieczenia będzie wystarczający.



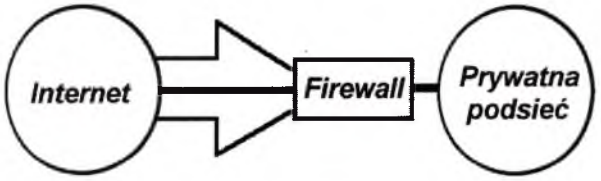
Każdy węzeł Internetu jest w stanie zaatakować każdy węzeł prywatnej podsieci.

Rys. 1 - możliwości ataku prywatnej podsieci

Wstęp do firewalli

Najlepszym do tej pory rozwiązaniem istniejącego problemu, jest firewall. Eliminuje on konieczność zabezpieczania każdego komputera z osobna, zostawiając dla wejścia do prywatnej podsieci jedynie „wąskie gardło" i potrzebę doskonałego zabezpieczenia tylko tego „wąskiego gardła".

Oczywiście sama konfiguracja firewalla musi być na tyle dobra, by nie dopuścić do ominięcia go przez włamywacza, co spowodowałoby praktycznie nieograniczony dostęp do wszystkich komputerów wpiętych w podsieć.



Dowolny węzeł Internetu jest w stanie zaatakować tylko firewall.

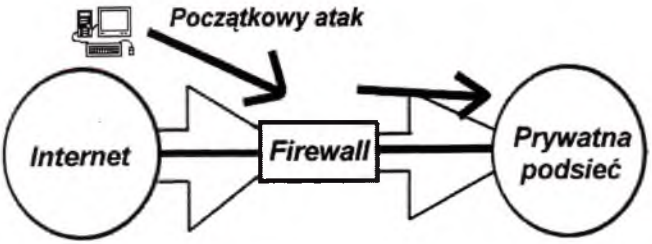
Rys. 2 - Możliwość ataku z Internetu tylko na Firewall

Polityka bezpieczeństwa

Wszędzie tam, gdzie instaluje się węzły Internetu, należy przyjąć określoną politykę bezpieczeństwa. System musi być chroniony według ściśle przyjętych reguł. Istnieją dwie główne reguły przy stawianiu firewalla: *„To, co nie jest wyraźnie zabronione, jest dozwolone"* oraz *„To, co nie jest wyraźnie dozwolone, jest zabronione"*. Przyjęcie pierwszego założenia jest dość wygodne - administrator blokuje jedynie porty IP oraz usługi o których wiadomo, że mogą być niepewne - nie jest to jednak bezpieczne. Przeciwstawić temu można drugie założenie - tutaj wszystkie porty zostają zablokowane, odblokowuje się tylko te, o których się wie, że są pewne. Jest to z punktu widzenia bezpieczeństwa dużo lepsze, niestety powoduje spore utrudnienia dla zwykłych użytkowników. Bez przyjęcia określonej polityki bezpieczeństwa nie może istnieć firewall.

Czego dotyczy firewall ?

W ogólności firewall jest złożony zazwyczaj z routerów filtrujących przychodzące pakiety (*screening router*) oraz komputerów zwanych *bastion host*. Zadanie firewalla jest proste - dokładnie



Rys. 3 - Dostęp do podsieci po złamaniu zabezpieczeń firewalla.

przefiltrować każdy przychodzący z zewnatrz pakiet i sprawdzić skąd został wysłany, do którego komputera zmierza oraz na który port IP jest skierowany. Następnie podejmowana jest decyzja dotycząca przekierowania tego pakietu - do niektórych portów będzie on mógł dotrzeć bez żadnych przeszkód, do niektórych innych - poprzez bastion host (tak zwany *proxy server* lub *gateway*), do innych zaś z definicji dostać się nie będzie mógł - zostanie po prostu odrzucony. Ma to na celu dokładną eliminację wszelkich zagrożeń płynących z zewnatrz - żadna usługa nie jest do konca bezpieczna a „dziury" w rozmaitych programach wykrywane są w bardzo krótkich odstępach czasu.
Podsieć, która nie jest chroniona przez gateway jest nazywana w skrócie DMZ - *Strefa Zdemilitaryzowana* (*De-Militarized Zone*).

Ogólne zasady

Z tych właśnie powodów instaluje się tak zwane proxy-services. W ogólnym skrócie mają one za zadanie odebrać cały ruch odbywający się na danym porcie dla konkretnej usługi tam umieszczonej, a następnie przekierować go na komputer udostępniający tę usługę - zewnętrzny świat nie komunikuje się więc z właściwym, docelowym serwerem, lecz z jego proxy. Ma to oczywiście niebagatelne znaczenie - przy przyjęciu drugiego założenia dotyczącego bezpieczeństwa każdy port który nie jest konieczny do poprawnego działania podsieci jest zablokowany - proxy umożliwiający pobranie udostępnionych informacji jest więc jedynym sensownym rozwiązaniem. Można korzystać z proxy przy takich usługach jak telnet, ftp czy www. Na przykład nowe programy obsługujące te usługi, w tym Netscape, posiadają możliwość korzystania z proxy.

Rys. 4 - Przykład działania proxy

Wszelkie usługi udostępnione obcym osobom muszą być bezpieczne dla systemu, dlatego też powinno stosować się logiczną zmianę katalogu głównego dla poszczególnych usług (ang. *chroot*) gdy instalujemy serwer WWW, FTPD lub *sendmail*. Katalogiem głównym z punktu widzenia osoby łączącej się z naszym komputerem nie może być nasz właściwy katalog główny lecz jego ścisły wycinek - np. /usr/local/httpd - bez jakiejkolwiek możliwości przedostania się w inne miejsce. Chroni to na przykład przed wykradnięciem plików konfiguracyjnych systemu, w tym pliku z hasłami użytkowników. Pomimo faktu, ze hasła te są zaszyfrowane szyfrem jednokierunkowym, przy łatwych hasłach jest możliwe ich odgadnięcie. Należy więc unikać stosowania haseł składających się z ogólnie używanych wyrazów bądz imion a zastapić je ciągiem losowo wybranych znaków, pomimo większej trudności w ich zapamiętaniu.

Przy definiowaniu firewalla należy wspomnieć o pojęciach takich jak *application level* i *circuit level*. Pojęcia te opisują sposób w jaki rozmaite usługi sa przechwytywane i przekierowywane przez firewall. O application level gateway mówi się, gdy dany pakiet przechwytuje usługa tego samego typu, co docelowa dla tego pakietu i ona przesyła go dalej swoim protokołem - dzieje się tak na przykład przy mail-exchangerze zapewniającym wymianę poczty elektronicznej. Circuit level gateway polega na przesłaniu pakietów przez usługi nie potrafiące zrozumieć informacji niesionej przez pakiet a jedynie przekierowujące go. W ekstremalnym przypadku ten gateway dla świata zewnętrznego wygląda jak proxy, zaś dla komputerów wewnątrz podsieci - jak filtr. Zaletą circuit level gateway jest możliwość zastosowania go dla różnych protokołów, niestety nie dla wszystkich. Obarczony jest on jednak różnymi wadami - na przykład nie potrafi stwierdzić, czy przesyłany przez niego pakiet jest bezpieczny dla systemu.

Koszty firewalli

Instalowanie firewalla nie jest niestety bezpłatne, obojętne, czy kupujemy go u konkretnego dostawcy, czy też budujemy go sami na podstawie darmowych, ogólnie dostępnych programów. W cenę wliczony musi być zakup oraz utrzymanie sprzętu takiego jak dobry router, umożliwiający filtrowanie pakietów oraz silne komputery. Gdy decydujemy się na komercyjnego firewalla dochodzą niebagatelne koszty zakupu i upgrade'u oprogramowania - w przypadku używania oprogramowania darmowego pozostaje śledzenie kolejnych jego wersji i przeinstalowywanie istniejącej na najnowszą. Warto tu wspomnieć o darmowym pakiecie Firewall Toolkit firmy TIS oraz o pakiecie SOCKS zawierającym narzędzia do budowania circuit level proxy-servers.

Trzeba też pomyśleć o wyszkoleniu personelu aby w każdej sytuacji można było sobie dać radę z ewentualną rekonfiguracją firewalla lub z jego naprawą. Do kosztów firewalla doliczyć trzeba też stratę pewnych usług świadczonych w Internecie, operujących na niepewnych portach bądź opartych na protokole UDP. Należy jednak zdać sobie sprawę także z kosztów ponoszonych przy zaniechaniu instalacji firewalla - trudy śledzenia działalności hackerów, konieczność ustawicznego czuwania, przy ewentualnych włamaniach - koszty reinstalacji systemu, backupu danych, które mogły być przez włamywacza zmienione (nie mówiąc już o kosztach które poniosłoby się w przypadku wykradnięcia ważnych danych). Administrator systemu może w takim przypadku bardzo łatwo stracić pracę. Zaniechanie budowy firewalla oznacza w praktyce gotowość na sponsorowanie działalności hackerów.

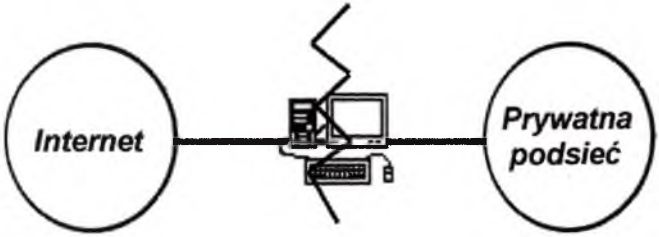
Typy firewalli

Screening Router

Najprostszym firewallem jest odpowiednio skonfigurowany router, umożliwiający filtrowanie pakietów - zwany *packet filter* lub screening router. Zadaniem takiego routera jest sprawdzenie na podstawie docelowego adresu czy powinien dany pakiet przesłać dalej, czy go odrzucić. Ustawiając pewne reguły routingu (*rulesets*), można eliminować niektóre aplikacje uchodzące za niebezpieczne - na przykład tftp, X11, RPC oraz „Berkeley 'r'-utilities" (rsh, rlogin, rcp etc.). Router taki nie musi być koniecznie sprzętowy, lecz może bazować na odpowiednim oprogramowaniu które oferuje dobre możliwości konfiguracji. Występują tu jednak pewne niedogodności - dane są sprawdzane na poziomie pakietów, nie sposób więc dokładnie sprawdzić ich zawartości. Nie można także uwierzytelnić konkretnych osób korzystających z danych usług w chronionej podsieci. Łatwo jest się pomylić przy konstruowaniu regul. Filtrowanie pakietów pociąga za sobą też spowolnienie działania sieci -

sprawdzenie każdego pakietu zajmuje pewien czas. Screening router jest jednak bardzo wygodny z punktu widzenia użytkowników - jego obecność jest prawie niewidzialna i nie wymaga instalowania proxy-servers dla żadnej z usług.

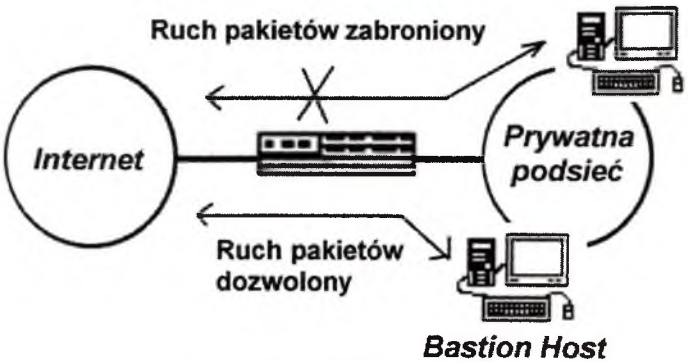
Dual Homed Gateways



Rys. 5 - Schemat Dual Homed Gateway

W tym wariancie nie występuje screening router, lecz jedynie komputer posiadający przynajmniej dwa interfejsy sieciowe. Taki komputer mógłby być routerem, ale tak nie jest. Jego zadaniem jest niedopuszczenie do bezpośrednich połączeń między Internetem a siecią chronioną. W efekcie cały firewall składa się z bastion hosta a sieć za nim staje się niewidzialna z zewnątrz. Komputery znajdujące się wewnątrz tej sieci mogą się komunikować z Internetem tylko poprzez bastion'a.

Użytkownicy mogą albo posiadać konta na bastionie, albo korzystać z proxy-services. Lepsza jest druga sytuacja. Na bastionie bowiem nie powinno się zakładać żadnych kont ani instalować żadnych usług poza niezbędnymi, zapewniającymi jedynie dobre funkcjonowanie firewalla. Każdy program na dysku komputera może stanowić zagrożenie dla jego bezpieczeństwa. Bastion host jest na tyle ważnym ogniwem firewalla (w przypadku Dual Homed Gateway - jedynym), że nie można sobie na to pozwolić. Przeniknięcie do bastion hosta oznacza w praktyce zniszczenie firewalla. Bastion pomiędzy swoimi obowiązkami powinien również sprawować pełną kontrolę nad systemowymi komunikatami i troszczyć się o ich logowanie. Każda próba przeniknięcia przez firewall musi być odnotowana. Jednakże instalowanie proxy-services, chociaż bezpiecznych, nie jest możliwe dla wszystkich usług - wiele z nich byłoby po prostu niedostępnych (szczególnie nowe usługi do których należy bądź samemu napisać odpowiedni program, bądź poczekać - czasem dość długo - aż taki program zostanie udostępniony). Chociaż Dual Homed Gateway w tym wariancie oferuje duże bezpieczeństwo (przy adekwatnej konfiguracji), jest mało elastyczne, przez co trudne do utrzymania.

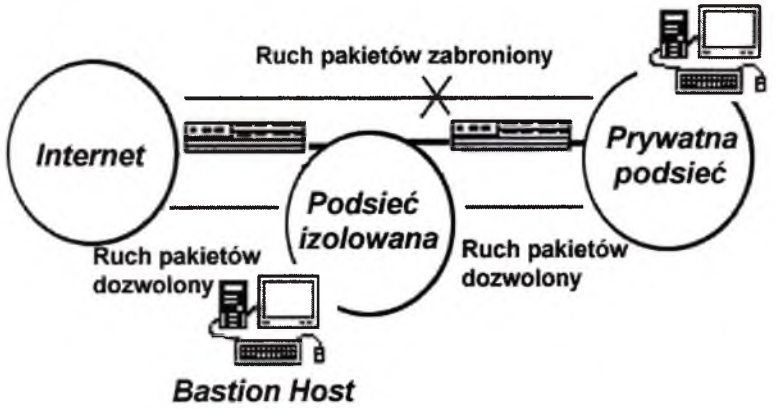


Rys. 6 - Schemat Screened Host Gateway

Screened Host Gateway

Tutaj występuje tak screening router jak i bastion host. Usługi są dostarczane poprzez proxy-services na bastion host'ie znajdującym się wewnątrz naszej sieci, do którego pakiety kierowane są przez screening router. Filtrowanie pakietów powstrzymuje pozostałe komputery wewnątrz sieci przed bezpośrednią komunikacją z Internetem, uniemożliwiając obejście proxy-services. Jednak ta konfiguracja jest dużo bardziej elastyczna niż poprzednio omawiana - możliwości połączeń nie ograniczają się jedynie do korzystania z proxy-services, lecz router może niektóre aplikacje przesyłać bezpośrednio od danego komputera na zewnątrz. Elastyczność ta ma jednak swoją cenę - nie mamy już tylko jednego newralgicznego punktu, lecz dwa - router i bastion host. Jest też drugi problem skoro istnieje możliwość uruchomienia usług omijających bastion'a, możemy ulec pokusie i naciskom użytkowników, i uruchomić usługi które mogą się okazać niebezpieczne.

Screened Subnet Gateway



Rys. 7 - Schemat Screened Subnet Gateway

Konfiguracja ta polega na utworzeniu izolowanej podsieci pomiędzy naszą chronioną siecią a Internetem. Izolowanie tej podsieci stwarza dodatkowe możliwości zabezpieczeń przed włamaniami. Teraz, uzyskanie przez obcą osobę dostępu do bastiona nie oznacza zniszczenia całego firewalla, gdyż istnieje jeszcze drugi router. Nie wchodzi tu też w rachubę podsłuchanie tego, co się dzieje wewnątrz naszej sieci. Nie są także rozgłaszane ścieżki routingu. Przykład ten przypomina trochę konfigurację Dual Homed Gateway, przy czym jeden komputer jest tu zastąpiony całą dodatkową podsiecią. Dużą zaletą Screened Subnet Gateway jest możliwość umieszczania dodatkowych hostów wewnątrz strefy zdemilitaryzowanej, na których chcielibyśmy udostępnić pewne usługi niemile widziane na bastionie. Obecnie wariant Screened Subnet Gateway jest najczęściej stosowany, jako reprezentujący najwyższy poziom bezpieczeństwa.

Wszystkie podane uprzednio konfiguracje firewalli są najczęściej wymieniane i proponowane. Nie są jednak jedyne - można sobie wyobrazić najrozmaitsze inne konfiguracje i hybrydy firewalli składających się na przykład z kilku bastionów, z połączenia bastiona z zewnętrznym routerem w jedną całość itp.

Problemy związane z filtrowaniem pakietów

Problemy z filtrowaniem pakietów wiążą się nierozerwalnie z polityką bezpieczeństwa i jej wariantami. Konfiguracja packet filter powinna uwzględniać przyjęte założenia (na przykład ewentualne założenie dotyczące blokowania wszystkich usług poza niektórymi). Wspomnieliśmy uprzednio o

konieczności bezbłędnej konfiguracji firewalla. Pamiętać należy, aby wszelkie odwołania do poszczególnych komputerów dotyczyły ich adresów IP, a nie ich nazw i domen. Gdy zaniedbamy to, sprytny hacker mógłby oszukać serwer DNS podstawiając fałszywe informacje i podszywając się za jeden z zaufanych komputerów, co ułatwiłoby mu ogromnie możliwości zniszczenia firewalla (*DNS-Spoofing-Attack*).

Można filtrować pakiety na podstawie dwóch metod: sprawdzania adresu źródłowego i docelowego oraz sprawdzania portu na którym odbywa się połączenie. Filtrowanie na podstawie adresu ma przede wszystkim jedną zaletę - może być stosowane w celu blokady propagacji pakietów wyglądających jakby zostały wysłane z naszej podsieci a w rzeczywistości pochodzących z zewnątrz. Z pakietami takimi mamy do czynienia gdy ktoś próbuje zaatakować któryś z naszych komputerów przez wysłanie pakietu ze zmienionym adresem źródła. Niestety, gdy nasz firewall ufa pewnej grupie obcych komputerów, hacker może spróbować zmienić ten adres na adres któregoś z zaufanych komputerów (*Source-Address-Spoofing*) i my tego już nie będziemy w stanie wykryć. Filtrowanie na podstawie adresu tego problemu nie rozwiązuje, a nie jest on banalny - wystarczy wspomnieć głośną niedawno sprawę Kevina Mitnicka.

Możliwe jest również dla hackera przekierowanie całego ruchu wchodzącego do naszej podsieci przez całkowicie obcy komputer poprzez zmianę ścieżek routingu (*source routing*). Dzięki temu mógłby on przeglądać każdy pakiet, co mogłoby mu na przykład ułatwić dostęp do naszych haseł (*Man-In-The-Middle*).

Rozmaite problemy dotyczą też filtrowania przez numer portu. Podczas filtrowania pakietów sprawdzana jest regularnie flaga ACK czyli potwierdzenia w nagłówku pakietu. Przy nawiązywaniu wirtualnego połączenia TCP, pierwszy pakiet nie ma ustawionej tej flagi. Gdy połączenie inicjowane jest z naszej podsieci, na przykład na zdalny port 23, jednocześnie losowo tworzony jest port na naszym komputerze - może to być port 34567. Załóżmy, że pozwalamy na ruch pakietów na porcie 23 - pakiet wychodzący nie natrafia na żadną przeszkodę. Gdy po wirtualnym połączeniu nadchodzi pakiet z zewnątrz, kieruje się on na port 34567, który nie jest bezpiecznym portem. Normalnie pakiet ten zostałby odrzucony i połączenie nie mogłoby zostać poprawnie nawiązane. Istnieje jednak wspomniana flaga ACK, która, gdy jest ustawiona, pozwala na przepuszczenie pakietu dalej. W przypadku, w którym na zdalnym porcie 23 funkcjonowałaby inna usługa niż się spodziewamy, połączenie inicjowane z obcego komputera zostałoby odrzucone - flaga ACK nie zostałaby ustawiona. Tutaj uwidacznia się problem z protokołem UDP - nagłówek UDP nie posiada takiego pola kontrolnego i nie może być w prosty sposób przesłany przez firewall. Stąd często wszelkie usługi UDP nie są możliwe do zrealizowania. Problem ten nie zachodzi tylko wtedy, gdy połączenie odbywa się jednocześnie na tym samym porcie na obydwu komputerach, jak w przypadku Domain Name Service - port 53.

Na inne trudności natrafiamy, gdy pakiet wysłany do nas z zewnątrz był zbyt duży i uległ fragmentacji. Pakiety powstałe z podziału nie niosą w sobie informacji na który port zostały skierowane (poza pierwszym). Czy taki pakiet dojdzie w dobrym stanie do docelowego komputera, to zależy od przyjętej taktyki. W mniej restrykcyjnym przypadku, każdy pakiet nie niosący informacji na jaki port został skierowany będzie przepuszczany dalej. Wówczas, gdy pierwszy pakiet zostanie odrzucony jako niepewny, dalsze jego fragmenty przejdą przez firewall i zostaną odrzucone dopiero przez docelowy komputer. Tyle mówi teoria, praktyka jednak trochę od niej odbiega. Można bowiem stworzyć sztucznie taki podział, by otrzymać bardzo małe fragmenty, w których po prostu zabraknie miejsca na część pierwotnego nagłówka - będzie się on znajdował w kilku fragmentach. Jest wówczas praktycznie możliwe przesłanie danych przez taki filtr który nie ma określonej najmniejszej możliwej wielkości fragmentu (*Tiny-Fragment-Attack*). Innym sposobem na ominięcie odfiltrowania jest stworzenie takiej serii fragmentów, z której pierwszy zawierał będzie dane bezpieczne z punktu widzenia filtru, lecz następne będą miały możliwość przykrycia niektórych pól pakietu w trakcie łączenia się. W tym przypadku, kolejne fragmenty zmodyfikują nagłówek właściwego pakietu, same jednak przejdą bez problemów przez filtr. Nie są one bowiem widziane jako fragmenty z zerowym przesunięciem, a tylko takie mogą być odfiltrowane (*Overlapping-Fragment-Attack*).

Z protokołami TCP i UDP związany jest protokół kontroli ICMP. Może on służyć do ataku polegającego na niedopuszczeniu do użycia żadnej usługi (*Denial-of-Service-Attack*). Wysyłanie pakietu ICMP zawierającego informację o rzekomym przerwaniu połączenia istotnie je przerywało na starych typach systemów UNIXowych. Jednakże całkowita blokada pakietów ICMP wiąże się ze stratą wielu użytecznych informacji przesyłanych tą drogą.

Trzeba zwrócić uwagę także na inne protokoły, takie jak IP-over-IP, wykorzystywany przez Mbone (*Multicast-Backbone*). Należy rozważyć zasadność blokowania bądź przepuszczania pakietów tego typu przez firewall.

Inne aspekty bezpieczeństwa

Pomimo istnienia firewalla, trzeba pomyśleć o logowaniu się do naszego systemu z zewnątrz. Problemem jest na przykład co zrobić, gdy nasz użytkownik pragnie rozpocząć pracę na naszym systemie z zewnątrz Internetu. Zezwolenie na to wiąże się z określonymi zagrożeniami. Po pierwsze, jego hasło może być przechwycone w podsieci z której się loguje (poprzez *sniffing*), a wiąże się to z bezpośrednim dostępem do naszej sieci. Problem ten rozwiązuje na przykład stosowanie przesyłania zaszyfrowanych haseł. Inną metodą jest używanie jednorazowych haseł, pozwalających na jedno zalogowanie się - najbardziej znanym systemem automatycznej zmiany haseł jest system S/Key, który umożliwia kolejne logowania przy każdorazowej zmianie haseł. Niestety algorytm używany przez S/Key został już złamany. Stosuje się także czasowe samoczynne zmiany haseł - jest to specyficzny typ haseł zmieniających się co pewien czas poprzez algorytm znany systemowi oraz tak zwaną kartę użytkownika z której można odczytać hasło (*Time Based Passwords*).

Kolejnym zagrożeniem w takiej sytuacji jest możliwość przejęcia przez osobę nieuprawnioną połączenia już uwierzytelnionego - właściwa osoba traci połączenie, a zyskuje je hacker. Jednym ze sposobów na przeciwstawienia się takiej sytuacji jest ufanie, że zdalny system posiada przynajmniej takie same zabezpieczenia jak nasz - połączenia z innych systemów są blokowane. Można też szyfrować wszystkie połączenia (*End-to-end encryption*).

Podsumowanie

Jak wiadomo, istnieje ogromna potrzeba chronienia swoich danych przed osobami niepowołanymi. W obecnym świecie zbyt wiele można stracić udostępniając informacje innym. Z drugiej strony coraz bardziej rozwija się sieć komputerowa, służąca do wymiany danych. Wymiana ta musi się jednak odbywać w sposób wykluczający przechwycenie informacji przez osoby nieuprawnione. Istnieją najrozmaitsze metody obrony przed włamywaczami, co zostało tu przedstawione. Jednakże najlepszą z tych metod jest zastosowanie firewalla. W tej chwili komercyjna firma nie posiadająca firewalla a powierzająca swe tajemnice komputerom niezabezpieczonym może być narażona na ogromne straty. Firewalle na świecie są instalowane coraz częściej, docierają także i do Polski. Należy utrzymać tę tendencję i propagować ten system zabezpieczeń pamietając jednak, że dobrego hackera NIC nie zatrzyma.

Literatura

1. D. Brent Chapman, Elizabeth D. Zwicky, *Building Internet Firewalls*, O'Reilly & Associates Inc., 1995
2. William R. Cheswick, Steven M. Bellovin, *Firewalls and Internet Security*, Addison-Wesley Publishing Company, 1994
3. D. Brent Chapman, *Network (in)security through IP packet filtering*, In *Proceedings of the Third Usenix UNIX Security Symposium*, p. 63-76, Baltimore, MD, 1992
4. Marcus J. Ranum, *Thinking About Firewalls*, Trusted Information Systems, Inc.
5. *Firewall Toolkit Documentation*, Trusted Information Systems, Inc., 1993
6. G. Ziemba, D. Reed, P. Traina, *RFC 1858 - Security Considerations for IP Fragment Filtering*

MECHANIZMY ZARZĄDZANIA KLUCZAMI SZYFROWYMI

Jan Andrzej Malinowski

TP S.A. - Biuro Technik Nowych Usług

1. Problematyka bezpieczeństwa i ochrony informacji

Problematyka ochrony systemów informatycznych i informacji w rozproszonych systemach jest aktualnie na świecie jedną z najintensywniej badanych i rozwijanych. Wynika to z faktu, że informacja przechowywana, przetwarzana i przesyłana w tych systemach ***jest zasobem o dużej wartości finansowej, prawnej i moralnej, a utrata informacji lub jej przechwycenie przez osoby nieuprawnione powoduje nie tylko wymierne straty finansowe, ale również skutki natury prawnej, politycznej lub moralnej.***

Często można spotkać się z zarzutem, że ochrona zasobów w systemach informatycznych jest tak pracochłonna i czasochłonna, że „gra nie jest warta świeczki". Osoby (oraz firmy) wyrażające ten pogląd zmieniają zdanie, gdy same stają się ofiarą załamania systemu, inwazji wirusów lub kradzieży cennych danych. Dopiero wtedy zaczynają uznawać rangę problemu ochrony i usiłują stosować mechanizmy ochrony. W 1988 r eksperci oszacowali, że ***na świecie z tytułu nieuprawnionego dostępu do danych straty wynosiły 500 mln USD oraz prognozowali, że wielkość ta w następnych latach będzie znacząco wzrastać.***

Każde przedsiębiorstwo, organizacja, instytucja a także każda osoba fizyczna dysponuje różnymi informacjami, które są jej niezbędne do normalnego funkcjonowania. Niektórzy przytaczają celne porównanie: informacja w każdym organizmie społecznym lub gospodarczym odgrywa taką samą rolę, jak krew w organizmie żywym, a obieg informacji można porównać do krwioobiegu. Porównanie to można nieco rozszerzyć: podobnie jak organizm żywy umiera na skutek wykrwawienia lub zatrucia krwi, ***organizm gospodarczy lub społeczny może niedomagać lub zginąć, jeśli informacja umożliwiająca jego funkcjonowanie ulegnie zniszczeniu, przekłamaniu lub zostanie wykradziona, albo jeśli jej obieg ulegnie zakłóceniu***.

W miarę coraz powszechniejszego wykorzystywania technik komputerowych do gromadzenia, przechowywania i obróbki danych rzeczą oczywistą stała się potrzeba ochrony informacji zawartych w systemach komputerowych.

2. Kryptograficzna ochrona informacji w sieciach komputerowych

Szerokie rozprzestrzenianie się sieci komputerowych zrodziło cały szereg groźnych problemów, wśród których najbardziej poważnym jest problem dostępu do systemu osób nieuprawnionych. Wymownym świadectwem tego jest duża liczba publikacji, regularnie pojawiających się w literaturze. Specjaliści doszli do wniosku, że w praktyce najbardziej skutecznym (chociaż nie jedynym) środkiem ochrony informacji w sieciach jest jej ochrona kryptograficzna realizowana za pomocą mechanizmu szyfrowania. Szyfrowanie jest fundamentalnym mechanizmem ochrony, w którym uporządkowane dane lub tekst jawny transformowane są w tekst zaszyfrowany zgodnie z ustalonym algorytmem szyfrowania i przy użyciu ustalonego klucza zwanego kluczem szyfrowania. Tekst zaszyfrowany (szyfrogram) nie jest zrozumiały dla wszystkich i może być odczytywany przez tych, którzy znają klucz lub tajny ciąg znaków, które po wprowadzeniu do algorytmu deszyfrowania razem z tekstem zaszyfrowanym reprodukują tekst jawny. Jeśli klucze szyfrowania i deszyfrowania są takie same, to taki system szyfrowania nazywany jest systemem klucza symetrycznego (zastosowanie jednego tajnego klucza) ; natomiast jeśli są różne - to system nazywany jest systemem klucza asymetrycznego

(wykorzystujący dwa klucze, jawny i tajny) - tzw. system klucza publicznego. Kryptografia służy zapewnianiu poufności, autentyczności i integralności informacji. Częścią je jest analiza kryptologiczna, która zajmuje się badaniem mocy systemów kryptograficznych.

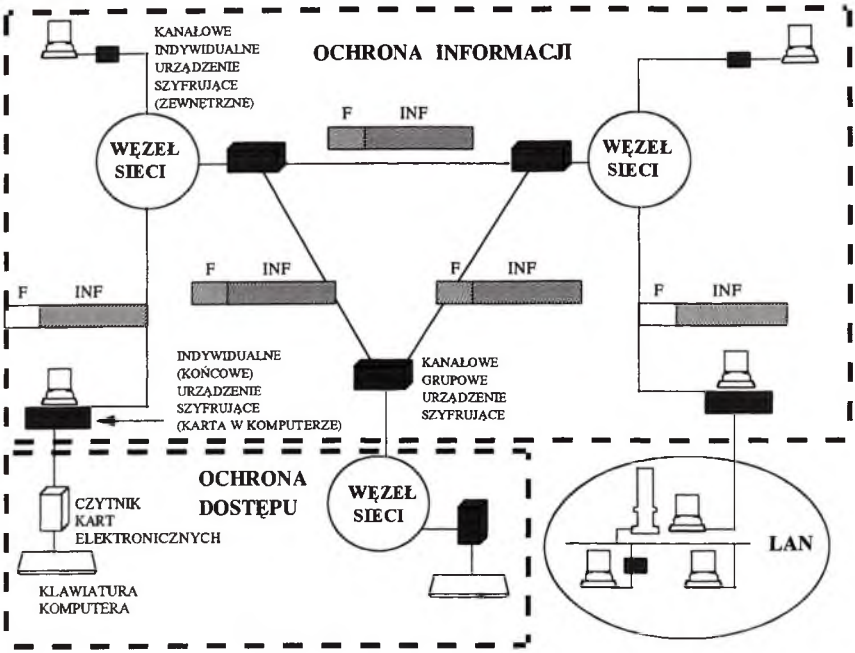
W ostatnich dwóch dziesięcioleciach w wielu krajach problemom zastosowania kryptografii do ochrony informacji w systemach informatycznych i sieciach komputerowych poświęca się szczególną uwagę.

Przy opracowywaniu kryptograficznych metod ochrony należy uwzględnić fakt, że hakerzy realizują swoje zadania wprowadzając następujące zagrożenia:

1. Uzyskanie nieuprawnionego dostępu do danych tj. naruszenie poufności informacji.
2. Podanie się za innego użytkownika i wykorzystania jego pełnomocnictw w celu: podania fałszywej informacji, zmiany prawdziwej informacji, uzyskania nieuprawnionego dostępu, uprawomocnienia fałszywych informacji lub ich potwierdzenia.
3. Zaprzeczenie faktu wprowadzenia informacji.
4. Potwierdzenie faktu, że w określonym momencie do użytkownika była wysłana informacja, chociaż w rzeczywistości nie była ona wysłana lub wysłano ją w innym czasie.
5. Zaprzeczenie faktu otrzymania informacji, (w rzeczywistości została odebrana) lub podawanie do wiadomości fałszywego czasu jej otrzymania.
6. Nieuprawnione rozszerzanie własnych uprawnień dostępu do informacji i jej tworzenia.
7. Nieuprawniona zmiana uprawnień innych użytkowników (fałszywy zapis innych osób, ograniczanie lub rozszerzanie pełnomocnictw innych użytkowników).
8. Ukrycie faktu istnienia niektórych informacji (ukryta transmisja) w innej informacji (ujawniona transmisja).
9. Włączenie się do linii miedzy dwoma użytkownikami jako aktywny retranslator.
10. Nieuprawnione monitorowanie uprawnionego dostępu do danych.
11. Modyfikacja programowego zabezpieczenia, zwykle przez niezauważalne dodanie nowych funkcji.
12. Złamanie lub zakłócenie protokołu przez wprowadzenie fałszywych informacji.

Do niedawna ze względu na wymiary i koszt urządzeń szyfrujących, ochroną kryptograficzną objęte były informacje jedynie w głównych traktach transmisyjnych (międzywęzłowych), a ochrona informacji w warstwie dostępowej była realizowana głównie metodami organizacyjnymi (np. poprzez ochronę fizycznego dostępu do urządzeń). W wyniku rozwoju technologicznego i postępującej cyfryzacji systemów powstała możliwość budowy urządzeń realizujących szyfrowanie w sposób układowy i programowy. Urządzenia te z reguły stanowią integralną część wyposażeń abonenckich (aparat telefoniczny, terminal). W takiej sytuacji możliwe jest szyfrowanie informacji w źródle i deszyfrowanie jej w punkcie docelowym.

W rozległej sieci teleinformatycznej typu WAN można zastosować dwustopniowy system ochrony informacji wykorzystujący metody kryptograficzne. Realizacja tego systemu wymaga stosowania urządzeń szyfrujących abonenckich i międzywęzłowych. Przykład takiego rozwiązania ilustruje poniższy rysunek.



W omawianym rozwiązaniu zastosowano trzy typy urządzeń szyfrujących:

- szyfrujące urządzenie końcowe (program);
- abonenckie kanałowe urządzenie szyfrujące;
- międzywęzłowe kanałowe urządzenie szyfrujące.

Proces ochrony kryptograficznej realizowany przez te urządzenia jest następujący:

Szyfrujące urządzenie końcowe (program) jest przeznaczone dla indywidualnego użytkownika końcowego. Realizuje ono funkcje ochrony informacji i kontroli dostępu do komputera, katalogów, zbiorów czy rekordów danego użytkownika. Zwykle jest zrealizowane jako dodatkowa płyta w komputerze lub specjalistyczny program.

Abonenckie kanałowe urządzenie szyfrujące może być odrębną jednostką montowaną przy terminalu lub może być wbudowane w urządzenie abonenckie; utajnia tylko część informacyjną pakietu danych, natomiast część adresowa pozostaje jawna ponieważ jest ona niezbędna dla celów komutacyjnych. Urządzenie to jest związane z danym kanałem i może obsługiwać różne systemy komputerowe.

Międzywęzłowe urządzenie szyfrujące utajnia informacje przesyłane między węzłami sieci transmisji danych maskując zarówno nagłówek pakietu jak i jego część informacyjną. Może ono pełnić rolę urządzenia grupowego pracując na potrzeby wielu użytkowników końcowych. Jego cechą jest duża szybkość szyfrowania.

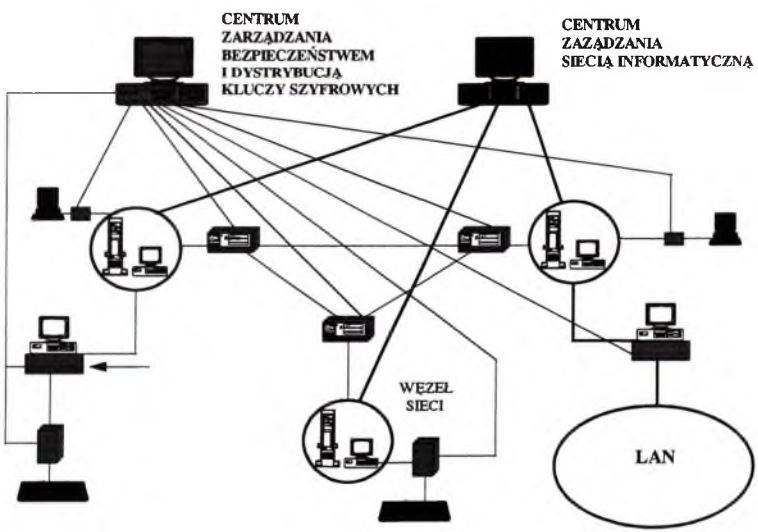
3. Dystrybucja kluczy szyfrowych

Z reguły systemy szyfrujące wymagają rozwiązania problemu dystrybucji kluczy. Problem ten jest jednym z najbardziej newralgicznych problemów eksploatacji rozbudowanych systemów kryptograficznych. Można powiedzieć, że system szyfrujący z jawnym algorytmem i protokołami kryptograficznymi jest tak bezpieczny, jak bezpieczna jest w nim dystrybucja kluczy. Nawet w systemach szyfrujących, w których algorytm jest tajny, znajomość klucza umożliwia wyciągnięcie wielu wniosków odnośnie używanego algorytmu, jego złożoności obliczeniowej i mocy kryptograficznej szyfru.

Dystrybucja kluczy obejmuje swoim zakresem: generowanie, sterowanie zmianami, magazynowanie, niszczenie, odtwarzanie kluczy oraz sposób ich rozprowadzenia do użytkowników w sieci. Wymienione elementy wymagają rozwiązania takich problemów jak:

- zagwarantowanie tajności oraz integralności kluczy szyfrowych;
- ustalenie terminu ważności poszczególnych kluczy;
- utrzymanie kryptograficznej spójności sieci, tj. taki przydział kluczy dla użytkowników, aby upoważnione do porozumiewania się ze sobą grupy rzeczywiście mogły się ze sobą porozumiewać;
- dobór kanałów używanych do dystrybucji kluczy;
- uwierzytelnienie źródła, z którego pochodzi klucz oraz stworzenie możliwości wzajemnej identyfikacji użytkowników;
- aktualizacja wykazu abonentów sieci utajnionej wymiany danych;
- minimalizacja strat poniesionych w przypadku awarii urządzenia szyfrującego lub ew. utrata zawartej w nim całej informacji dotyczącej kluczy.

W przypadku rozległych sieci (WAN) z dużą ilością węzłów, powinno się tworzyć osobne centrum zarządzania i dystrybucji.



Do jego zadań, poza wymienionymi wcześniej, należy rejestracja wszystkich operacji związanych z kluczami oraz zbieranie i przetwarzanie danych statystycznych.

W sieciach lokalnych można stosować prostsze mechanizmy rozdziału kluczy szyfrowych w postaci np. wydzielonego komputera do generacji i dystrybucji kluczy dla dwupoziomowego systemu kluczy do wymiany informacji wewnątrz LAN-u i kluczy do współpracy z siecią rozległą. W przypadku mocnych ograniczeń sprzętowych i niezbyt wysokiego stopnia tajności informacji, może wystarczyć szyfrowanie haseł dostępu do sieci LAN.

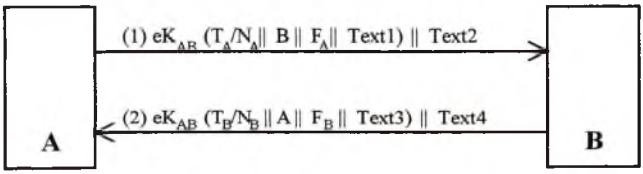
4. Mechanizmy zarządzania kluczami z wykorzystaniem technik symetrycznych

Organizacja ISO poświęca szczególną uwagę problemom dystrybucji kluczy w środowisku systemów otwartych. Poniżej przedstawiono trzy spośród dwunastu opracowanych przez ISO protokołów wymiany informacji kluczowej między terminalami sieci.

We wszystkich protokołach wymiany informacji kluczowej przyjęto założenie, że komunikujący się użytkownicy sieci (użytkownik A i użytkownik B) dysponują a'priori dostarczonym wcześniej kluczem K_{AB}.

4.1. Prosty protokół wymiany informacji kluczowej

Protokół umożliwia obydwu abonentom A i B współtworzenie klucza seansowego K. Protokół zapewnia wzajemne uwierzytelnienie nadawcy i odbiorcy informacji. Uwierzytelnienie jest uzyskiwane poprzez przesyłanie znaczników czasowych T lub numerów sekwencyjnych N zestawianych między nimi połączeń.



Protokół wymiany informacji kluczowej

Kroki:

(1) A wysyła do B zmienny w czasie parametr T_A/N_A (znacznik czasu lub numer sekwencyjny połączenia), identyfikator użytkownika B oraz materiał kluczowy F_A. Pola danych szyfrowane są przy użyciu klucza K_{AB}.

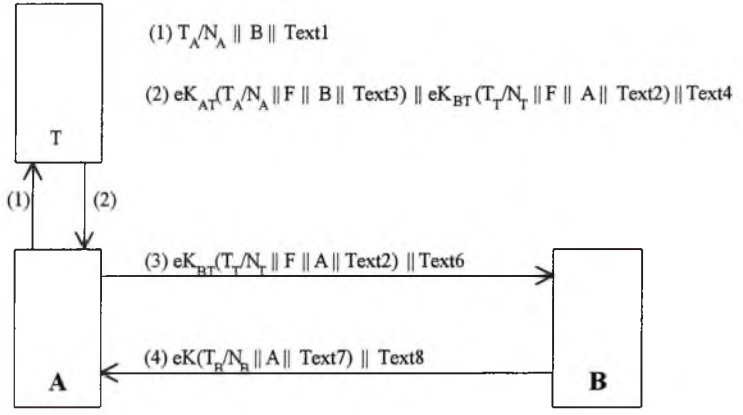
(2) B wysyła do A zmienny w czasie parametr T_B/N_B (znacznik czasu lub numer sekwencyjny połączenia), identyfikator użytkownika A oraz „materiał kluczowy" F_B. Pola danych szyfrowane są przy użyciu klucza K_{AB}.

(3) Abonenci A i B wyznaczają wspólny klucz seansowy K bazując na materiale kluczowym F_A oraz F_B a wykorzystując funkcję f znaną zarówno A i B (być może także innym użytkownikom sieci). Obydwie strony wyznaczają klucz seansowy K jako $K=f(F_A,F_B)$.

4.2. Przesyłanie klucza z wykorzystaniem Centrum Dystrybucji Kluczy

Zadaniem Centrum Dystrybucji Kluczy (CDK) jest wygenerowanie i dystrybucja lub tylko pośrednictwo w wymianie informacji kluczowej między abonentami, którzy posiadają indywidualne klucze wykorzystywane przy komunikowaniu się z CDK. Aktualnie rozważane są protokoły dwukluczowe, w których jeden z abonentów (inicjator) żąda klucza K od CDK potrzebnego do komunikowania się ze wskazanym abonentem. Centrum Dystrybucji Klucza wytwarza lub tylko pośredniczy w przekazaniu inicjatorowi współpracy klucza K, zaszyfrowanego przy użyciu klucza wspólnego dla inicjatora i CDK.

W protokole tym klucz K jest dostarczany przez Centrum Dystrybucji Kluczy. Użyty mechanizm zapewnia wzajemne uwierzytelnienie obydwu użytkowników. Autentyczność jest weryfikowana za pomocą znaczników czasu lub przesyłanych numerów sekwencyjnych zależnych od ilości przeprowadzonych seansów między obydwoma użytkownikami. Protokół wymaga aby istniała możliwość tworzenia znaczników czasu T lub numerów sekwencyjnych N oraz sprawdzania aktualności tych parametrów.



Protokół wymiany informacji kluczowej z udziałem CDK

Kroki:

(1) A składa zapotrzebowanie do CDK na klucz seansowy z abonentem B wysyłając wiadomość w postaci jawnej zawierającą parametr T_A/N_A (znacznik czasu lub numer sekwencyjny) oraz identyfikator odbiorcy B. Parametr T_A/N_A służy do weryfikacji autentyczności zaszyfrowanej wiadomości odebranej zwrotnie (czy zaszyfrowana wiadomość z CDK nie jest rezultatem podstawienia).

(2) CDK przesyła do A wiadomość zawierającą materiał kluczowy F (oraz ew. inne dane) zaszyfrowane kluczem K_{AT}. Wiadomość ta składa się z dwóch zasadniczych części:

(a) $eK_{AT}(T_A/N_A$ || F || B || Text3)

(b) $eK_{BT}(T_T/N_T$ || F || A || Text2)

(c) oraz opcjonalnej części Tekst4

(3) A przesyła do B wiadomość zawierającą część (b) wiadomości (2). Wiadomość ta wskazuje użytkownikowi B, że nadawcą jest A. Text6 może zawierać dodatkowo informację umożliwiającą

sprawdzenie integralności klucza K wyodrębnionego z materiału kluczowego F. W tym przypadku Text6 jest zastępowany przez $eK(T_A/N'_A \| B \| Text5) \| Text6$.

(4) *opcjonalnie* : B zwraca do A wiadomość $eK(T_B/N_B \| A \| Text7)$ potwierdzając w ten sposób odbiór K. Krok (4) jest opcjonalny i może zostać pominięty w przypadku gdy wymagane jest tylko jednostronne uwierzytelnienie.

4. 3. Przesyłanie klucza z wykorzystaniem Centrum Translacji Klucza

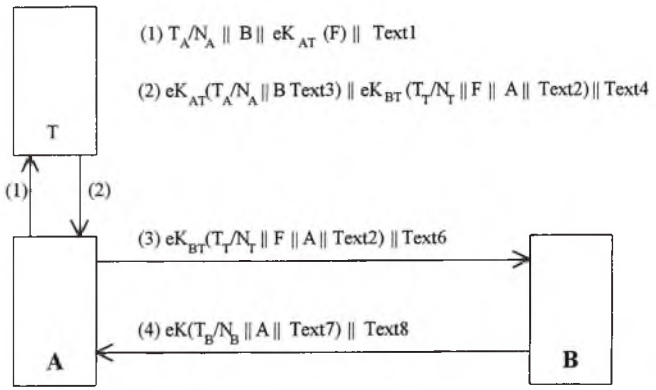
Zadaniem Centrum Translacji Klucza (CTK) jest pośredniczenie w przekazywaniu klucza pomiędzy abonentami, z których każdy posiada klucz używany przy kontaktowaniu się z CTK. Jeden z użytkowników - inicjator (nadawca) przesyła klucz K do CTK zaszyfrowany kluczem wspólnym dla inicjatora i CTK. CTK deszyfruje klucz K a następnie ponownie szyfruje ten klucz przy użyciu klucza wspólnego dla CTK i danego użytkownika - odbiorcy. Tak przygotowaną informację odsyła do inicjatora (nadawcy), który z kolei wysyła tę wiadomość do ustalonego odbiorcy. Innym wariantem tej metody jest przesłanie klucza „przeszyfrowanego" w CTK wprost do wskazanego odbiorcy. W tej metodzie inicjator - nadawca powinien mieć możliwość wygenerowania klucza seansowego (lub przynajmniej jego uzyskania). Po ustaleniu klucza seansowego przy współpracy z CTK obydwaj komunikujący się użytkownicy pracują w trybie punkt-punkt.

Dla protokołów przedstawionych w tym rozdziale wymaga się:

- Powołania zaufanego pośrednika w postaci CTK, z którym użytkownicy A i B posiadają wspólne klucze K_{AT}.oraz K_{BT} odpowiednio;
- Pośredniczący zaufany pośrednik jest zawsze dostępny;
- Jeden z użytkowników A lub B, zależnie od konkretnie przyjętego mechanizmu posiada możliwość wytworzenia (wygenerowania) klucza K;
- Wymagania dotyczące bezpieczeństwa są związane z zachowaniem poufności klucza K, ochroną przed jego modyfikacją i wykrywaniem potencjalnego zagrożenia podszycia się.

W protokole tym klucz K jest dostarczany przez użytkownika A. Autentyczność dostarczanego klucza jest sprawdzana z wykorzystaniem znaczników czasu lub numerów sekwencyjnych.

Protokół zapewnia wzajemne uwierzytelnienie użytkowników komunikujących się z jego wykorzystaniem. Protokół umożliwia weryfikację znaczników czasu T oraz numerów sekwencyjnych N przez obydwu użytkowników A i B oraz zaufanego pośrednika CTK.



Protokół wymiany informacji kluczowej z udziałem CTK

Kroki:
(1) A żąda przekazania klucza poprzez przesłanie do CTK wiadomości, która zawiera uzależniony od czasu parametr T_A/N_A (znacznik czasu lub numer sekwencyjny), identyfikator użytkownika B oraz pola danych zaszyfrowane kluczem K_{AT} zawierające materiał kluczowy F (obejmujący klucz K oraz ew. inne dane). Parametry T_A/N_A są wykorzystywane do weryfikacji autentyczności wiadomości odebranej od CTK (tzn. Sprawdzenia czy nie jest ona efektem maskarady).
(2) CTK zwraca do A wiadomość zaszyfrowaną kluczem K_{AT}. Wiadomość ta składa się z dwóch części:

(a) $eK_{AT}(T_A/N_A \| B \| Text3)$

(b) $eK_{BT}(T_T/N_T \| F \| A \| Text2)$

(c) oraz opcjonalnej części Tekst4

(3) A przesyła do B część (a) wiadomości (2). Wiadomość ta wskazuje B, że została ona wysłana przez nadawcę A. Text6 może zawierać opcjonalnie pola danych, które umożliwiają sprawdzenie integralności klucza K wyodrębnionego z materiału kluczowego F. W tym przypadku Text6 jest zastępowany przez $eK(T_A/N'_A \| B \| Text5) \| Text6$.
(4) *opcjonalnie* :B zwraca $eK(T_B/N_B \| A \| Text7)$ do A potwierdzając w ten sposób, że również posiada klucz K. Opcjonalny krok (4) może być pominięty w przypadku wymagania jedynie jednostronnego uwierzytelnienia.

5. Zarządzanie kluczami z wykorzystaniem systemu klucza publicznego

W odróżnieniu od klasycznych systemów szyfrowych, w których strona nadawcza i odbiorcza posługują się identycznym kluczem, istnieją systemy , w których klucze szyfrujący i deszyfrujący różnią się. Nazywamy je asymetrycznymi systemami szyfrowania lub systemami szyfrowania z kluczem publicznym Jednym z najważniejszych powodów, dla których opracowane zostały takie systemy, była próba ominięcia problemu klasycznej dystrybucji kluczy. W systemach szyfrowych z kluczem publicznym przyjmuje się następujące założenia:

a) do szyfrowania i deszyfrowania wykorzystywane są dwa różne klucze D i E. Klucza deszyfrowania D nie można uzyskać w oparciu o znajomość jedynie klucza szyfrowania E lub na odwrót, chociaż między nimi istnieje ścisły związek matematyczny.

b) klucza E nie można (w przypadku jego nieznajomości) złamać poprzez atak tekstem jawnym. Przy spełnieniu tych dwóch warunków, klucz szyfrujący E może zostać ujawniony. Z tego powodu klucz ten jest nazywany kluczem publicznym, w odróżnieniu od drugiej części klucza zwanej kluczem tajnym bądź prywatnym

Seans transmisji danych pomiędzy dwoma abonentami sieci oznaczonymi A i B posiada następujący przebieg: Wiadomość M. Przeznaczona do zaszyfrowania jest przedstawiona w postaci cyfrowej i dzielona na bloki jednakowej długości. Następnie użytkownik A pobiera z publicznego katalogu kluczy klucz E_B abonenta B i przy jego pomocy szyfruje wiadomość M., wysyłając do B szyfrogram wiadomości $M. = E_B (M.)$. Z uwagi na spełnienie podanego wcześniej postulatu a) tylko użytkownik B posiada klucz D_B i jest w stanie deszyfrować kryptogram $E_B (M.)$ poddając go operacji $D_B(E_B(M.))$ przekształcającej szyfrogram w wiadomość jawną M.

5.1. Wymiana klucza zaszyfrowanego

Protokół wymiany klucza zaszyfrowanego (ang. Encrypted key exchange - EKE) został zaprojektowany przez Steve'a Bellovina i Michaela Merrita. Umożliwia on zapewnienie poufności i uwierzytelnianie w sieciach komputerowych.

Jedną z implementacji protokołu EKE jest algorytm **Diffiego - Hellmana**. Przy jego użyciu klucz K jest generowany. Dla wszystkich użytkowników sieci ustanowiono dwie liczby a i p. Użytkownik A posiada prywatną liczbę losową X_A, a użytkownik B - liczbę X_B. Algorytm jest następujący:

1. **A wysyła do B liczbę** $Y_A = a^{X_A} (\bmod p)$
2. **B oblicza** $K = Y_A^{X_B} (\bmod p) = a^{X_A X_B} (\bmod p)$
3. **B generuje ciąg losowy R_B a następnie oblicza i przesyła do A :**

   $P(a^{X_B} (\bmod p)), K(R_B)$

4. **A deszyfruje pierwszą połowę wiadomości B w celu uzyskania** $a^{X_B} (\bmod p)$. **Następnie oblicza** K **i stosuje do odszyfrowania** R_B. **Wytwarza inny ciąg losowy** R_A, **szyfruje oba ciągi za pomocą** K **i wynik przesyła do B :**

   $K(R_A, R_B)$

5. **B deszyfruje wiadomość w celu uzyskania R_A i R_B. Jeżeli ciąg R_B, który otrzymał od A jest taki sam jak ten, który wysłał do A w kroku 2, to szyfruje R_A przy użyciu klucza K i przesyła do A :**

   $K(R_A)$

6. **A deszyfruje wiadomość w celu uzyskania R_A. Jeżeli ciąg R_A, który otrzymał od B jest taki sam jak ten, który wysłał do B w kroku 3. to protokół ustalania klucza sesyjnego jest zakończony. Obie strony komunikują się teraz przy użyciu klucza sesyjnego** K.

6. Standaryzacja technik szyfrowania i zarządzania kluczami

Wszystkie mechanizmy zabezpieczeń w przedstawionych standardach są ściśle powiązane z różnego rodzaju technikami szyfrowania. Oczywiste jest, że ze względu na nadrzędną cechę systemów otwartych - wzajemną współpracę systemów pracujących na różnych platformach sprzętowo-programowych - także w zakresie technik szyfrowania konieczna jest standaryzacja.

Najbardziej znanym standardem szyfrowania z kluczem symetrycznym jest DES (Data Encryption Standard). Wspominana wielokrotnie bezpieczna usługa katalogowa X.509 jest standardem, który korzysta z klucza publicznego do tworzenia certyfikatów o oparciu o podpisy cyfrowe. DES może być stosowany także jako algorytm szyfrowania, zapewniający poufność w systemach powiązanych ze standardem X.509.

Oprócz potrzeby standaryzacji technik szyfrowania, istnieje także konieczność unormowania w zakresie stosowania algorytmów kryptograficznych. Na przykład: organizacje korzystające z niepublicznych algorytmów utajniania wiadomości, mogą wymagać oceny algorytmów przez niezależnego eksperta. Ocena ta może być szczególnie istotna dla przypadków wykorzystywania protekcji w systemach wymiany danych. Przykładem tego typu prac są działania podjęte przez ISO/IEC, uwieńczone standardami Bezpiecznego Protokołu w warstwach transportowej i sieciowej.

Najsłabszym punktem każdego systemu kryptograficznego są klucze szyfrowe. Wynika to z faktu, iż zarządzanie kluczami w sposób bezpieczny jest trudne do zrealizowania. Niełatwo jest zaprojektować bezpieczny algorytm i protokół kryptograficzny, ale jeszcze trudniej jest zapewnić

utrzymanie tajności wykorzystywanych kluczy. Istniejące standardy próbują normować te problemy. Ich podsumowaniem są następujące dokumenty:

- *ANSI*. Financial Institution Key Management (Wholesale) - X9.17:1985,1991 (także ISO/IEC 8732:1988); Certificate Management for DSA - X9.30-3 (draft), Mangement of Symmetric Algorithm Keys Using Irreversible Cryptography - X9.30-4 (draft), Certificate Management for RSA - X9.31-3 (draft) oraz Management of Symmetric Algorithm Keys Using RSA - X9.31-4 (draft)
- *ISO/IEC*. Banking Key Management by Means of Asymmetric Algorithms (Part 2: Approved Algorithms Using the RSA, CD 11166-2:1991
- *RSA PKCS*. Diffie-Hellman Key-Agreement Standard - PKCS #3:1993

Podsumowanie

Złożoność opracowywanych algorytmów dystrybucji kluczy i konieczność ich oceny z punktu widzenia ochrony wymaga tworzenia własnych ośrodków badań, analizy i oceny mocy kryptograficznej systemu ochrony. Problem ten dotyczy również oceny stosowanych algorytmów do szyfrowania i deszyfrowania informacji. W przypadku dużych sieci korporacyjnych jest bardzo istotne posiadanie takiego ośrodka, ponieważ od wyników jego pracy zależy jakość ochrony informacji w sieci. Żadna firma ani instytucja zewnętrzna nie powinna wykonywać takiej pracy samodzielnie; pewne zasadnicze elementy powinny być opracowywane w ramach danej korporacji.

Najlepszym wzorcem w tym zakresie jest dotychczasowa polityka ochrony informacji w USA, która opiera się na następujących przesłankach:

- **rozwój systemów ochrony informacji jest prowadzony w bezpiecznym (objętym kontrolą) środowisku;**
- **rozwój systemów ochrony informacji jest prowadzony tylko w oparciu o własny potencjał naukowy i produkcyjny;**
- **eksport systemów i urządzeń ochrony informacji używanych w USA jest zabroniony.**

Literatura

1) ROBLING DENNING, *Kryptografia i ochrona danych*, WNT Warszawa 1992.
2) ISO/IEC 11770, part 2, *Key management mechanisms using symmetric techniques*.
3) BRUCE SCHNEIER, *Kryptografia dla praktyków*, WNT 1995.
4) ANDRZEJ PASZKIEWICZ, *Mechanizmy uwierzytelniania informacji w zautomatyzowanych systemach dowodzenia*, materiały z konferencji KNSŁ Zegrze 1995
5) MAREK SUCHAŃSKI, *Wybrane zagadnienia ochrony informacji w systemach teleinformatycznych*, materiały z konferencji „Teleinformatyka w wojsku i policji", Kraków 1995

ROZPRASZANIE ELEKTROMAGNETYCZNE W SIECIACH KOMPUTEROWYCH I OCHRONA INFORMACJI UŻYTECZNEJ PRZED NIEPOŻĄDANĄ DETEKCJĄ

Waldemar E. Grzebyk, Jarosław M. Janukiewicz

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1. Wprowadzenie

Informacja jest najbardziej poszukiwanym i najlepiej chronionym towarem. Obserwujemy gwałtowny rozwój sieci komputerowych. Podstawowym problemem staje się zrównoważenie wymagań dotyczących łatwego dostępu do zasobów przez uprawnionych użytkowników sieci i ochrona tych zasobów przed osobami niepowołanymi. Skala problemu zwiększa się wraz z lawinowo rosnącą ilością instalacji. Przede wszystkim na administratorze sieci spoczywa obowiązek zabezpieczenia zasobów sieci. O ile dostrzegamy potrzebę stosowania mechanizmów zabezpieczeń przed nieuprawnionym dostępem wewnątrz sieci komputerowej to często nie zwracamy uwagi na niebezpieczeństwo podsłuchu za pomocą odbioru promieniowania elektromagnetyczne od linii komunikacyjnych, terminali i innych urządzeń sieciowych.

Współczesne metody detekcji skrajnie słabych sygnałów obarczonych szumami i zakłóceniami o dużej intensywności umożliwiają wykrycie sygnałów o poziomach mniejszych o ponad 40 dB od poziomu szumów cieplnych w obwodach elektrycznych. W systemach komputerowych detekcja transmitowanych sygnałów jest możliwa dzięki emisji wielu składowych widma transmitowanego sygnału.

2. Detekcja i rozpraszanie elektromagnetyczne

Detekcja jest to proces fizyczny mający na celu odtworzenie sygnału źródłowego (informacji użytecznej) z sygnału wypromieniowanego przez urządzenie nadawcze i odebranego przez antenę.

Pod pojęciem rozproszenia elektromagnetycznego informacji użytecznej urządzeń komputerowych należy rozumieć energię wypromieniowaną przez te urządzenia i przenoszoną przez:

- pole elektryczne (sprzężenia pojemnościowe),
- pole magnetyczne (sprzężenia indukcyjne),
- pole elektromagnetyczne (promieniowanie wysokiej częstotliwości),
- przewody (sprzężenia galwaniczne).

3. Rozpraszanie elektromagnetyczne w sieciach komputerowych

3.1 Mechanizm rozpraszania elektromagnetycznego w sieciach komputerowych

Urządzenia cyfrowe wykorzystują sygnały binarne, tzw. "zero-jedynkowe". Czas przejścia z jednego stanu do drugiego często jest mniejszy od nanosekundy. Równocześnie zmienia się natężenie prądu płynącego w liniach sygnałowych i zasilających. W konsekwencji obwody te promieniują energie elektromagnetyczna w zakresie od częstotliwości akustycznych do kilkuset MHz a dla niektórych urządzeń ponad 1 GHz. Większość emitowanej energii skupia się jednak poniżej 300 MHz.

Szczególnym rodzajem urządzeń cyfrowych jest sprzęt sieciowy i komputerowy. Mamy tam do czynienia praktycznie ze wszystkimi zjawiskami tworzenia i rozchodzenia się energii elektromagnetycznej, charakterystycznych dla urządzeń cyfrowych (wynika to z istnienia w instalacjach komputerowych zasilaczy, modemów, monitorów ekranowych, i wielu innych urządzeń peryferyjnych oraz połączeń w ramach sieci).
Jak już zostało wspomniane istnieją cztery drogi przenoszenia rozproszenia elektromagnetycznego. Należy zwrócić uwagę na dwie zasadnicze drogi emisji energii. Pierwsza przez przewody, a więc za pośrednictwem sieci i linii elektrycznych a druga przez promieniowanie, czyli rozchodzenie się energii w otaczającej przestrzeni w postaci fal elektromagnetycznych. Należy zwrócić uwagę, że często występują razem obydwa zjawiska. Np. jeżeli w pobliżu źródła promieniowania, którym może być okablowanie sieci komputerowej znajdzie się przewód zasilający, to stanowi on wraz z impedancjami sieci zasilającej i okablowania pętlę, w której indukuje się energia. Energia ta przenosi się do sieci zasilającej już drogą przewodową.

3.2 Źródła rozpraszania elektromagnetycznego w sieciach komputerowych

Zasadniczymi źródłami rozproszenia elektromagnetycznego w sieciach komputerowych są urządzenia aktywne i bierne. W szczególności można wyróżnić:

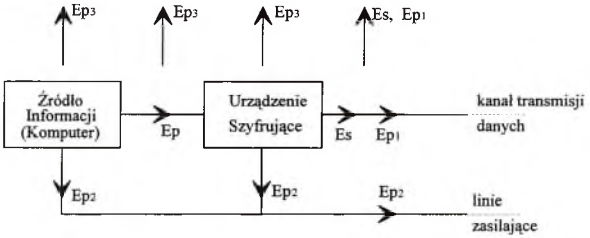
- układy scalone wraz z doprowadzeniami sygnałów np. zegarowych, sterujących,
- linie zasilające układy scalone, zwłaszcza gdy układy pracują synchronicznie np. bufory szyn i magistral, pamięci (prądy wieloamperowe),
- okablowanie wewnątrz urządzeń np. płaskie taśmy wielożyłowe, skrętki, kable ekranowane, pojedyncze połączenia,
- korpusy urządzeń wykonane z materiałów przewodzących,
- zasilacze, zwłaszcza impulsowe,
- niezakończone obciążeniem linie sygnałowe i sterujące np. do nieużywanych gniazd interfejsów,
- wszelkie przekaźniki, klucze, włączniki,
- połączenia sieciowe między urządzeniami,
- monitory ekranowe, zwłaszcza układy odchylania i zasilania lampy kineskopowej.

4. Ochrona informacji użytecznej przed niepożądaną detekcją.

Minimalizacja rozproszenia elektromagnetycznego informacji użytecznej jest ściśle związana z jej detekcja i ma do spełnienia dwa zasadnicze zadania :

- ochrona przesyłanych i przetwarzanych informacji przed ich przekłamaniem lub zanikiem oraz przed niepożądanym dostępem,
- zapewnienie kompatybilności elektromagnetycznej urządzeń tzn. wypromieniowana przez te urządzenia energia nie powinna powodować zakłóceń w pracy innych urządzeń zarówno w ramach danego systemu (zakłócenia wewnątrzsystemowe), jak i innych systemów (zakłócenia międzysystemowe).

Ochrona informacji przed niepożądanym dostępem oprócz "klasycznych" form zabezpieczenia jak zapobieganie nielegalnemu dostępowi do pamięci masowych i wydruków itp. wymaga minimalizacji rozproszenia elektromagnetycznego. Staje się to szczególnie konieczne gdy instalacje obejmujące komputery łączone są w sieć. Podsłuch może być stosowany znacznie częściej niż to sobie wyobrażamy. Gdy istnieje dość duże rozproszenie w postaci pola elektromagnetycznego podsłuch stosować może każdy, kto zada sobie trud ustawienia anteny. Należy zatem ograniczyć rozproszenie elektromagnetyczne i szyfrować dane aby stały się niezrozumiale dla wszystkich z wyjątkiem właściwego adresata.
Powszechne szyfrowanie informacji jest trudne, gdyż jest bardzo kosztowne a dystrybucja i stosowanie kluczy wymaga dużo czasu i zasobów. Zastosowanie skutecznego szyfrowania danych w systemach informatycznych, mimo iż jest nieodzowne dla zapewnienia poufności przetwarzania i transmisji informacji, nie jest w stanie zwykle zapewnić wysokiej protekcji systemu przed niepowołanym dostępem do wiadomości chronionych ze względu na niepożądana emisję wiadomości pierwotnej (*Rysunek 1*).



Ep1 - niepożądane nałożenie składowych widma wiadomości na widmo zaszyfrowanego sygnału Es i zawartość tych składowych w widmie emisji przewodzonych i promieniowanych Es,
Ep2 - zawartość widma emisji wiadomości pierwotnej w liniach zasilających systemu,
Ep3 - promieniowanie widma emisji wiadomości pierwotnej przez obwody i linie źródła wiadomości i szyfratora.

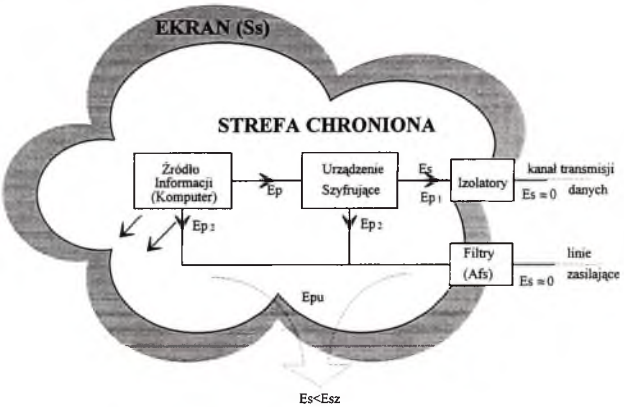
Rysunek 1. Schemat przetwarzania i transmisji wiadomości ze skutecznym jej szyfrowaniem i możliwymi drogami rozpraszania elektromagnetycznego wiadomości

W sieciach komputerowych które powinny być chronione przed możliwością elektromagnetycznej detekcji wiadomości należy ograniczyć emisyjność składowych widma wiadomości. W takich systemach powinny być spełnione wymagania w zakresie dopuszczalnego rozproszenia elektromagnetycznego. Te wymagania można spełnić przez osiągnięcie w rozpatrywanym systemie stopnia protekcji $ps>1$ w całym zakresie częstotliwości, w którym występują składowe widma wiadomości. Stopień protekcji *ps* wyraża się zależnością *(1)*

$$ps = Ed/Es \qquad (1)$$

gdzie: Ed - minimalny poziom emisji widma wiadomości przy którym istnieje potencjalna możliwość detekcji elektromagnetycznej wiadomości,
Es - emisja widma wiadomości przez system jako całość.

Zależność ta powinna być spełniona dla każdej z możliwych dróg rozproszenia elektromagnetycznego wiadomości.



Es - emisja widma wiadomości pierwotnej przez system jako całość
Esz - emisja szumów,
Epu - dopuszczalny poziom emisji widma wiadomości pierwotnej,
Ss - skuteczność ekranowania ekranu,
Afs - skuteczność filtrów.

Rysunek 2. Schemat instalacji systemu ze skutecznym szyfrowaniem i ochroną przed rozpraszaniem elektromagnetycznym informacji

Obszar chroniony stanowi strefę ekranowaną o odpowiednio dużej skuteczności ekranowania *Ss [dB]*, wyposażoną w filtry elektryczne o odpowiedniej skuteczności *Afs*. Urządzenia systemu zainstalowanego w tej strefie powinny mieć odpowiednio ograniczona emisyjność *Epu* tak aby:

$$Epu = max \{ Epur, Epuc \} \quad (2)$$

oraz

$$ps(f)\ [dB] = 20*log(Ed/Epu) + Ss\ [dB] = 20*log(Ed/Es) > 0\ [dB] \quad (3)$$

gdzie: Epur - maksymalna dopuszczalna emisja promieniowana widma wiadomości przez urządzenie,
Epuc - maksymalna dopuszczalna emisja przewodzona widma wiadomości.

Najistotniejsze elementy takiej instalacji decydujące o stopniu zabezpieczenia poufności informacji to (*Rysunek 2*):

- rozproszenie elektromagnetyczne wiadomości przez urządzenia, linie transmisyjne i zasilające systemu mniejsze niż dopuszczalny poziom *Epu*),
- strefa ekranowana o dostatecznie dużej skuteczności ekranowania systemu *Ss*,
- filtry o odpowiednio dużej skuteczności *Afs* na wejściach zasilających,
- izolatory minimalizujące możliwość rozproszenia elektromagnetycznego wiadomości przez.

5. Minimalizacja rozpraszania elektromagnetycznego w sieciach komputerowych

Chcąc minimalizować rozproszenie elektromagnetyczne informacji użytecznej z punktu widzenia kompatybilności elektromagnetycznej oraz ochrony przed jej przekłamaniem lub zanikiem należałoby:

- wyeliminować źródła rozproszenia,
- zapobiegać propagacji rozproszenia elektromagnetycznego wiadomości,
- chronić przed rozproszeniem układy na nie wrażliwe.

Chcąc minimalizować rozproszenie elektromagnetyczne informacji użytecznej z punktu widzenia ochrony przed niepożądaną detekcja należałoby:

- szyfrować przesyłane i przetwarzane informacje,
- ekranować i filtrować,
- zmniejszać poziomy emitowanej informacji.

Rysunek 3.

W artykule zwrócono uwagę na drugi z wyżej wymienionych aspektów minimalizacji rozpraszania elektromagnetycznego w sieciach komputerowych - ochrona informacji przed detekcją.
Często zadajemy sobie pytanie: ***Szyfrować czy ekranować ?***

5.1 Ekranowanie

Należy pamiętać, że nawet posługując się wszystkimi najważniejszymi sposobami redukcji rozproszenia elektromagnetycznego - takimi jak ekranowanie, uziemianie, filtracja, izolowanie, dobór kabli - nie można zazwyczaj w pełni wyeliminować rozproszenia elektromagnetycznego informacji użytecznej. Może ono być jedynie zminimalizowane do pewnego poziomu. Dwoma podstawowymi środkami zmniejszania przenikania rozproszenia elektromagnetycznego są: ekranowanie i uziemianie. Metody ekranowania i uziemiania są ściśle powiązane ze sobą.

W sieciach komputerowych ekranowane mogą być kable lub kompletne urządzenia (komputery, serwery, rutery itp.). Skuteczność ekranowania zmienia się wraz z częstotliwością sygnału, strukturą geometryczną ekranu, rodzajem ekranowanego pola, kierunkiem jego padania i polaryzacją. Do podstawowych charakterystyk ekranów zaliczamy skuteczność ekranowania S_s (dB) i charakterystykę częstotliwościową tej skuteczności. Skuteczność danego ekranu przy określonej częstotliwości zależy zarówno od materiału i grubości ścianek konstrukcji ekranującej jak też od odległości miedzy powierzchnią ekranująca a źródłem promieniowania r [m]. Skuteczność ekranów idealnych (czyli w pełni jednorodnych, bez złącz szczelin i otworów) można obliczyć przy pomocy teoretycznych zależności matematycznych. Jednak rzeczywiste ekrany maja skuteczność znacznie mniejszą z powodu niejednorodności powierzchni ekranującej oraz przerw w powierzchni ekranującej. Charakterystyki ekranów rzeczywistych najłatwiej wyznaczyć na drodze pomiarów. Materiały o dużej przewodności są w stanie ograniczyć jedynie rozproszenie składowej elektrycznej pola elektromagnetycznego. Składowa magnetyczna pola wymaga stosowania materiałów o dużej przenikalności magnetycznej takich jak np. stal.

5.1.1 Ekranowanie urządzeń

Osłona ekranująca działa najskuteczniej, jeśli jest szczelna (klatka Faraday'a), a napięcia zasilające są doprowadzone poprzez filtry dolnoprzepustowe. W urządzeniach stanowiących elementy sieci komputerowych ekrany metalowe są stosowane w wykonaniach specjalnych. W urządzeniach komputerowych ogólnego przeznaczenia, dostępnych na rynku, powszechnie są stosowane obudowy plastykowe. Do tych konstrukcji opracowano liczne technologie zapewniające ekranujące właściwości takich obudów. Między innymi:

- metalizowanie,
- natryskiwanie i malowanie obudów pokryciami przewodzącymi,
- stosowanie przewodzących mas plastycznych do tłoczenia obudów,
- stosowanie elastycznych tkanin przewodzących wykonanych z metalizowanych włókien, połączonych z masą plastyczną w procesie tłoczenia obudowy,
- wykorzystanie samoprzylepnych przewodzących folii nakładanych na obudowę.

5.1.2 Ekranowanie kabli

Stosuje się dwie metody minimalizacji rozpraszania elektromagnetycznego sieciowych instalacji kablowych. Pierwsza z nich polega na ekranowaniu torów kablowych. Druga wykorzystuje zjawisko kompensacji zakłóceń w torach symetrycznych. Stosowanie ekranowania kabli wymaga spełnienia wielu warunków (dobre uziemienie, brak „pętli prądowych", mała impedancja połączeń ekranów) a w praktyce jest trudne do wykonania. Odporność torów symetrycznych na zakłócenia impulsowe jest szczególnie istotna w przypadku braku dobrze zdefiniowanego uziemienia. Ekranowanie torów symetrycznych może zmniejszyć rozpraszanie elektromagnetyczne informacji użytecznej lecz źle wykonane może je zwiększyć.

W sieciach komputerowych stosuje się dwa podstawowe typy kabli miedzianych:

- kabel symetryczny typu „skrętka",
- kabel współosiowy.

Dla zapewnienia dobrego ekranowania przewodów należy:

- minimalizować długości nieekranowanych części przewodu,
- zapewnić dobre uziemienie ekranu.

Przewód ekranujący (ekran) powinien być dołączony do masy tylko z jednej strony, w przeciwnym bowiem razie z połączenia mas powstać może pętla prądowa. Przy większej liczbie źródeł rozproszenia należy każde połączenie oddzielnie ekranować.

W przypadku kabli symetrycznych (skręconej pary przewodów) jeżeli prądy w obu przewodach są równe to linie pola od jednej pary znoszą się nawzajem. Większe tłumienie rozproszenia w tym przypadku można uzyskać przez dodatkowe ekranowanie skręconych przewodów.

W przypadku kabli koncentrycznych przewód zewnętrzny stanowi przewodzącą powierzchnie, na której kończą się linie sił pola elektrycznego pochodzące od przewodu wewnętrznego. Jeżeli w ekranie spowoduje się przepływ prądu równego i przeciwnie skierowanego niż w przewodzie wewnętrznym, to wytworzy on równe, lecz przeciwnie skierowane pole magnetyczne. Pole to znosi się z polem magnetycznym wytwarzanym przez przewód wewnętrzny na zewnątrz ekranu.

6. Szyfrowanie

Zastosowanie skutecznego szyfrowania danych w sieciach komputerowych jest nieodzowne dla zapewnienia poufności przetwarzania i transmisji informacji. Nie jest natomiast w stanie zapewnić wysokiej protekcji sieci komputerowej przed niepowołanym dostępem do wiadomości chronionych ze względu na niepożądaną emisję wiadomości pierwotnej.
Rozwój dziedziny ochrony danych uległ gwałtownemu przyspieszeniu w połowie lat 70-tych W 1977 roku w Stanach Zjednoczonych opracowano i wprowadzono DES (ang. Data Encryption Standard) w systemach cyfrowych. Opracowano metody szyfrowania z kluczem jawnym, podpisy cyfrowe, schematy ochrony kluczy i protokoły dystrybucji kluczy. Rozwinięto techniki weryfikacji zabezpieczeń kryptograficznych.
Prace nad algorytmami systemów kryptograficznych zaowocowały stworzeniem szeregu standardowych rozwiązań, stosowanych obecnie w sieciach transmisji danych. Podstawowym mechanizmem zabezpieczenia systemów komputerowych oraz urządzeń sieciowych przed nieuprawnionym dostępem jest autentyzacja użytkowników. W tym celu stosuje się hasła, które powinny być znane tylko przez osoby uprawnione. Względnie łatwo osoba niepowołana może wejść w posiadanie hasła pozwalającego na dostęp do zasobów. W praktyce nie zawsze są

przestrzegane lub są nieznane zasady dotyczące sposobu tworzenia haseł i posługiwania się nimi w sposób bezpieczny. Zalecane reguły są kłopotliwe w użyciu. Z drugiej strony wiele systemów korzysta z haseł, które przesyłane są przez sieć w jawnej postaci, łatwej do odczytania przez posiadacza analizatora protokołów. Aby zminimalizować udział człowieka w procesie autentyzacji coraz częściej stosuje się urządzenia służące do generowania haseł jednorazowego użytku, o krótkim czasie ważności.

6.1 Ochrona kryptograficzna

Kryptografia jest podstawową formą ochrony informacji składowanej i przesyłanej w obszarze współczesnych sieci komputerowych. Dzięki postępowi technologii możliwe jest szyfrowanie i deszyfrowanie informacji w czasie rzeczywistym. Powstała szeroka rodzina specjalizowanych układów scalonych, które potrafią przetwarzać strumienie informacji o przepustowości rzędu kilkuset kb/s. Znanych jest kilka standardowych algorytmów szyfrowania, które przyjęły się w rozwiązaniach cywilnych.
Współczesna rola kryptografii to:

- autentyzacja nadawcy i odbiorcy - dzięki metodom szyfrowania asymetrycznego lub algorytmów *hash (one-way functions)* jest możliwe stosowanie elektronicznych podpisów dołączanych do przesyłanych danych.
- ochrona niezmienności informacji - realizowana poprzez stosowanie numeracji sekwencji, sum kontrolnych i oznaczanie okresu ważności informacji w sposób podobny jak podpis elektroniczny
- ochrona tajności i poufności - realizowane poprzez szyfrowanie metodami symetrycznymi, asymetrycznymi lub kombinowanymi.

6.1.1 Algorytmy szyfrowania

Elementem systemu kryptograficznej ochrony informacji mającym decydujący wpływ na jego skuteczność jest algorytm szyfrowania. Użycie jednego z istniejących, sprawdzonych rozwiązań daje pewność niezawodnej pracy systemu i gwarancję bezpieczeństwa danych.

W ciągu ostatnich lat, wraz z rozwojem komputerowych technik obliczeniowych, powstało wiele rozmaitych algorytmów szyfrowania. Zbudowane są one zazwyczaj w oparciu o szyfry iloczynowe stosowane wielokrotnie lub też wykorzystują słabości matematyki wielkich liczb.

Wśród współcześnie uznanych i szeroko stosowanych algorytmów ochrony informacji na uwagę zasługują:

- systemy z kluczem publicznym,
- Data Encryption Standard (DES),
- funkcje jednokierunkowe,

7. Wnioski

1. Konwencjonalne metody odbioru sygnałów promieniowania elektromagnetycznego pochodzącego od elementów sieci komputerowych mogą umożliwić otrzymanie informacji, które nie zawsze są chronione przez metody kryptograficzne.

2. Ekranować należy wszędzie tam gdzie jest to możliwe i konieczne oraz uzasadnione ekonomicznie.

3. Szyfrowanie informacji należy stosować wszędzie tam gdzie jest to konieczne.

8. Literatura

[1]. Chołownia J., "Współczesne problemy kompatybilności elektromagnetycznej sprzętu komputerowego", Raport nr I-28/SPP - 008/86 Instytutu Telekomunikacji i Akustyki Politechniki Wrocławskiej, Wrocław 1986.
[2]. Ottt H.W., "Metody redukcji zakłóceń i szumów w układach elektronicznych", WNT, Warszawa 1979.
[3]. White D.R.J., "EMI Control Methodology and Procedures", Don White Consultants Inc., Gaineswille, USA.

Naukowa i Akademicka Sieć Komputerowa

oraz

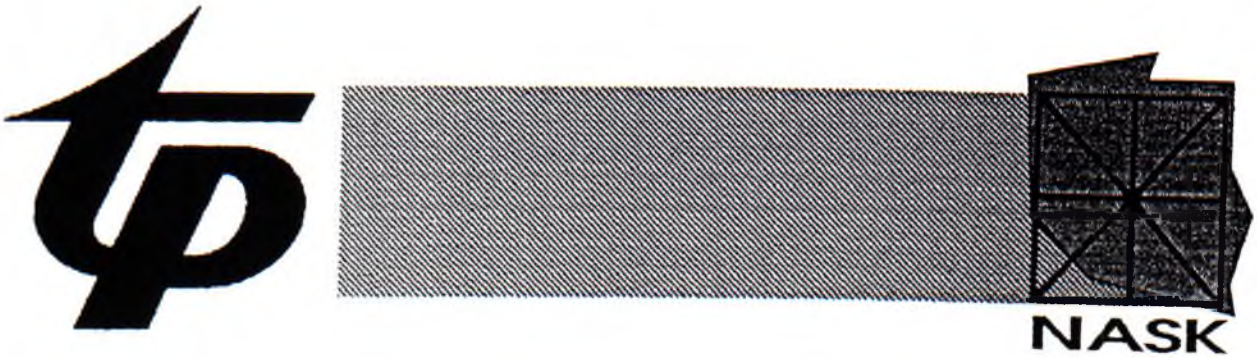
Telekomunikacja Polska S.A.

Materiały seminarium

MIEDZESZYN '96

Część II

22-24 maja 1996 r.



Naukowa i Akademicka Sieć Komputerowa

oraz

Telekomunikacja Polska S.A.

Materiały seminarium

MIEDZESZYN '96

Część II

22-24 maja 1996 r.

Spis treści

Część II

EKSPLOATACJA SIECI WARMAN - WYBRANE ZAGADNIENIA

Tadeusz Rogowski, Andrzej Skrzeczkowski, Piotr Wróblewski

Naukowa i Akademicka Sieć Komputerowa

ul. Bartycka 18, 00-716 Warszawa

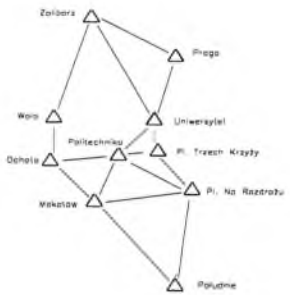
I. Koncepcja budowy sieci metropolitalnej w Warszawie *WARMAN* w oparciu o technologię ATM powstała w 1992 r [1]. Po szeregu ekspertyzach, dyskusjach i sporach, a także rozpoznaniu potrzeb, w 1993 roku powstały Założenia Techniczno-Ekonomiczne oraz rozpoczęto przygotowania do realizacji projektu. Szczegółowy opis fazy przygotowawczej i koncepcyjnej był wielokrotnie omawiany m.in. na Konferencji POLMAN 1994 [2]. W najbardziej skrótowy i przewrotny sposób ówczesne dyskusje można podsumować następująco: z dużym prawdopodobieństwem wiadomo już było w 1992/93 roku, że technologią przyszłości będzie ATM. Postawiono więc pytanie: czy należało budować sieć FDDI czyli wybrać wariant migracji od FDDI do ATM, czy budować sieć w technologii ATM, wybierając wariant migracji od ATM nie w pełni wystandaryzowanego do ATM wystandaryzowanego. Dzisiejsze doświadczenia - nie tylko nasze - potwierdzają, że wybór technologii ATM był prawidłowy.

Obecnie sieć *WARMAN* mimo dalszej rozbudowy weszła w fazę pełnej eksploatacji. Przyjęta w *Założeniach* infrastruktura zakładająca budowę 10 węzłów połączonych liniami światłowodowymi z pewnymi zmianami została utworzona. W trakcie realizacji projektu *Założenia* były aktualizowane między innymi z następujących powodów:

- powstały nowe jednostki naukowe, w tym uczelnie prywatne, zmieniła się struktura i lokalizacja niektórych istniejących instytutów naukowych,
- zmiany gospodarcze w kraju spowodowały zmianę struktury przemysłu, jego zaplecza naukowego, pojawiły się nowe podmioty gospodarcze,
- relatywnie wolniej niż przewidywano powstaje zapotrzebowanie na usługi teleinformatyczne szeroko rozumianej administracji państwowej, jest to wynik prawdopodobnie braku wystarczających środków finansowych,
- środki przeznaczone na budowę sieci *WARMAN* okazały się niewystarczające na planowaną budowę połączeń światłowodowych do węzłów na Żoliborzu i Pradze,
- pojawiły się nowe lokalizacje atrakcyjne pod względem liczby klientów np. CRiT i CT Piękna.

To tylko kilka przykładów uzasadniających pewne zmiany w stosunku do wcześniejszych *Założeń*.

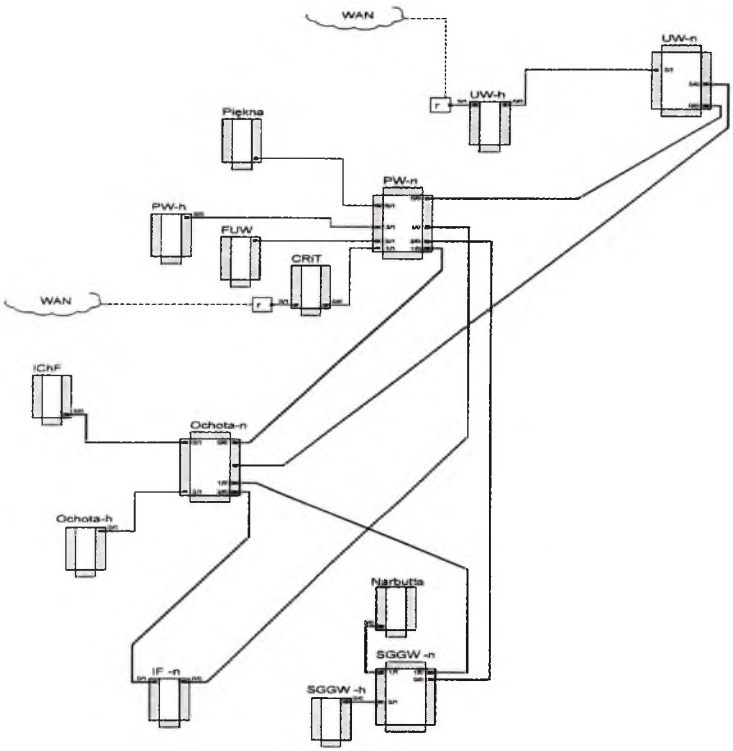
Planowaną w *Założeniach* z 1993 r. strukturę węzłów pokazano na rys. 1.



Rys. 1

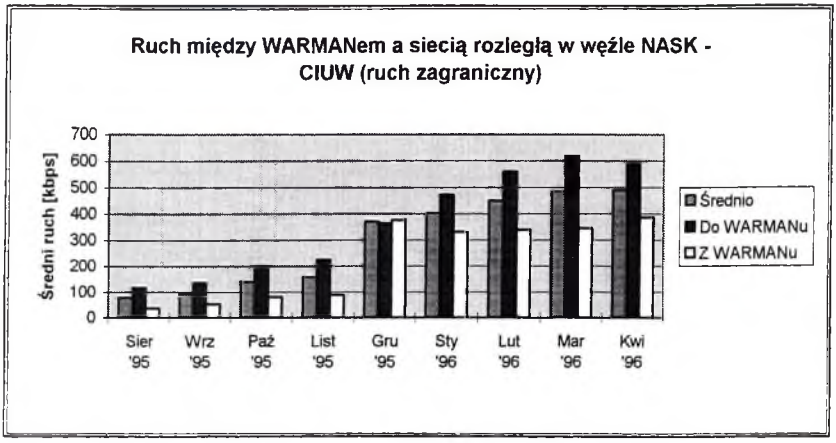
W chwili obecnej uruchomionych jest 15 węzłów sieci *WARMAN*, z czego 10 wyposażonych jest w urządzenia ATM. Stan obecny szkieletu sieci przedstawiono na rys. 2.

Schemat ogólny sieci WARMAN, część ATM (stan aktualny).

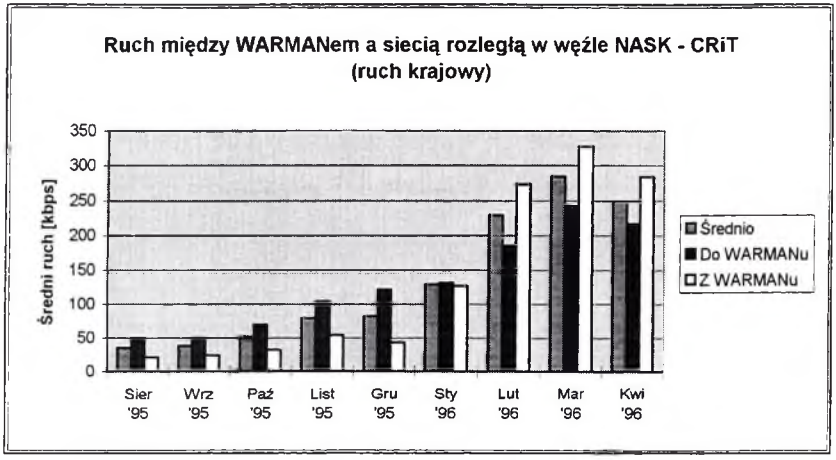


Rys. 2.

Okres budowy sieci *WARMAN* zbiegł się w czasie z gwałtownym rozwojem nowych technologii wymiany informacji, rozwojem systemów informacyjnych i wprowadzeniem komputerów dużej mocy. Duża przepustowość sieci, jeszcze nie w pełni wykorzystana daje możliwości rozwoju nowoczesnych aplikacji, które w większości wymagają dużego pasma. Analiza ruchu w sieci pokazuje jego systematyczny wzrost. Na rys. 3 i 4 pokazano statystyki w ruchu do/z sieci miejskiej w relacji ze „światem".



Rys. 3.



Rys. 4.

◊ Jak wynika z zamieszczonych wykresów, w ciągu ostatnich trzech kwartałów średni ruch między WARMANem a światem wzrósł 6-7 krotnie, a średni ruch WARMAN - kraj - 8 krotnie. W tym samym okresie około 2,5 krotnie wzrosła liczba abonentów sieci miejskiej.

◊ Z chwilą wprowadzenia nowego cennika NASKu ruch z WARMANu na kraj przewyższył ruch z kraju do WARMANu. Oznacza to wzrost zainteresowania zasobami włączonymi do sieci miejskiej.

◊ Ruch między WARMANem a światem jest około 2 krotnie większy niż ruch między WARMANem a krajem. Zdaje się to świadczyć o ciągle jeszcze ubogim zbiorze usług internetowych w Polsce lub o ich nieznajomości. Tymczasem dynamika wzrostu tego ruchu wskazuje na możliwość zniknięcia takiej dysproporcji w ruchu.

◊ Należy zwrócić również uwagę na skokowy wzrost zainteresowania zasobami w Warszawie w ruchu z zagranicy w grudniu 1995r. Może to być spowodowane rozreklamowaniem sieci w Polsce przy okazji ogłoszenia nowego cennika NASKu.

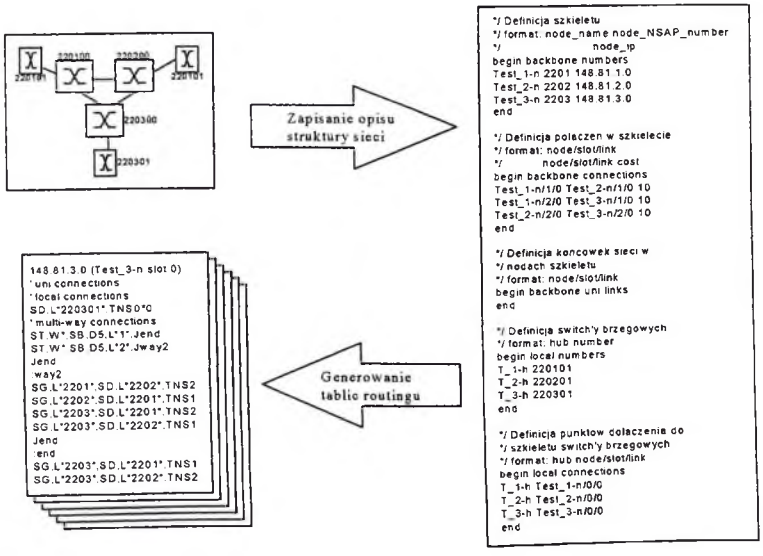
II. Sieć metropolitalna w pierwszym okresie praktycznie stała się *nośnikiem Internetu*. Wynika to po pierwsze z przejęcia dotychczasowych funkcji od zespołu NASK, który eksploatował *klasyczne* połączenia w Warszawie. Po drugie zapotrzebowanie na inne usługi miało charakter ograniczony i wreszcie, mimo teoretycznych możliwości technologii ATM realizowania różnych usług, w swojej pierwotnej wersji istniejące przede wszystkim oprogramowanie, a także dostęp do kart dostępowych uniemożliwiał zaoferowanie innych usług. W chwili obecnej istnieje możliwość zaoferowania szeregu dostępnych opcji, jak na przykład:

- tworzenie sieci wirtualnych i korporacyjnych,
- realizacja profesjonalnych wideokonferencji,
- realizacja transmisji kanałów PCM poprzez sieć ATM.

Możliwości takie zostały przetestowane w sieci *WARMAN*. Warto zaznaczyć, że w okresie uruchamiania sieci postępowała standaryzacja ATM, a co za tym idzie wymiana przede wszystkim oprogramowania *switchy* ATM. W kontrakcie na dostawę technologii ATM był zagwarantowany *upgrade* oprogramowania. W konsekwencji przez nasze laboratorium przeszło 8 wersji oprogramowania (od 3.0.0 do 4.1.0) z czego kilka było instalowanych w sieci. Aby nie zakłócać pracy sieci, wprowadzaliśmy tylko te wersje, które istotnie zmieniały jej funkcjonalność. Przykładem może być tutaj pełna implementacja *SPVC* (*switched permanent virtual circuits*) i *SVC* (*switched virtual circuits*).

1. Funkcje SVC i SPVC

Wdrożenie funkcji SVC/SPVC było szczególnie ważne. Połączenia takie są automatycznie przełączane w przypadku awarii, co istotnie wpływa na poprawę niezawodności sieci. Przełączaniem sterują *tablice routingu* (jedna tablica na każdą kartę w switchu). W przypadku dużych sieci tworzenie tablic routingu jest dość złożone. Aby uprościć problem, wprowadzono adresowanie switchy, dzięki czemu sieć została zhierarchizowana. W przekierowywaniu ruchu uczestniczą tylko te węzły, z których odchodzą co najmniej dwie drogi. Kolejnym doświadczeniem było stwierdzenie, że tablice te można przygotowywać w sposób strukturalny, co pozwoliło na opracowanie programu do automatycznego generowania tablic. Przykład tworzenia tablic routingu został pokazany na rys. 5.



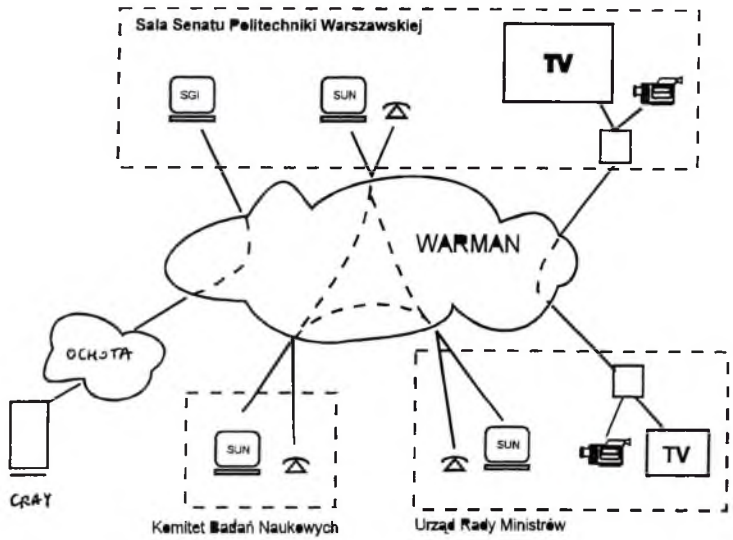
Rys. 5.

3. Wideokonferencja

Technologia ATM z uwagi na m.in. swój *izochronizm*, szerokie pasmo z możliwością dynamicznego przydziału i technologię przełączania jest przygotowana do przesyłania ruchomych obrazów i głosu. Istnieją różne możliwości realizacji wideokonferencji w oparciu o technologię ATM, np:

- komputery wyposażone w karty ATM, kartę video z kamerą i mikrofonem oraz odpowiednie oprogramowanie,
- wyspecjalizowana karta umieszczona w switchu ATM do której podłączona jest kamera, mikrofon i monitor (telewizor), z wykorzystaniem pełnego pasma (w przypadku naszych testów było to maksymalnie ok. 30 Mbps) oraz kodowania obrazu w standardzie MJPEG.

Oba te warianty zostały sprawdzone podczas sesji związanej z przekazaniem sieci *WARMAN* do eksploatacji. Schemat testowanej struktury pokazano na rys. 6.



Rys. 6.

Zebrane doświadczania w pełni potwierdzają przydatność technologii ATM do transmisji obrazu i głosu w sposób nieopóźniony i bez zakłóceń.

3. PCM via ATM

Kolejną usługą dostępną w sieci ATM jest możliwość udostępniania kanałów cyfrowych w celu łączenia central telefonicznych *PABX*. Zrealizowane połączenie pracuje łącząc centralę telefoniczną w Gmachu Głównym PW z centralą na tzw. terenie południowym PW (Gmach Wydz. Mechaniki Precyzyjnej) poprzez switche ATM w kolejnych węzłach: PW, SGGW i PW-Południe. Zestawiony został kanał E1, a podstawowe cechy tak zestawionego kanału, to:

- nieramkowany sposób transmisji (*unframed signal pattern*),
- możliwość wyboru źródła sygnału zegara: zegar adaptacyjny, zegara systemowy, lokalny oscylator, zegar pobierany z linii,
- możliwość przesyłania danych w *slocie 16* (*time slot* TS16),
- typ interface'u 120 ohm symetryczny lub 75 ohm asymetryczny,
- transmisja ATM przy użyciu kanału PVC (*permanent virtual circuits*) z opcją CBR (*constant bit rate*).

Przedstawione wyżej doświadczenia pokazują, że technologia ATM w praktyce, nie tylko na prospektach firmowych, umożliwia już obecnie:

- realizację jednocześnie transmisji danych, obrazu, głosu,
- operowanie przydziałem pasma,
- realizację sieci wirtualnych i korporacyjnych.

Literatura:

[1] Andrzej Zienkiewicz: Koncepcja sieci WARMAN; opracowanie wewnętrzne NASK, 1993

[2] Maciej Kozłowski, Tadeusz Rogowski: WARMAN, miejska sieć komputerowa; materiały konferencji POLMAN '94

[3] Roman Adamiec, Maciej Kozłowski, Tadeusz Rogowski: WARMAN - miejska sieć komputerowa oparta o technologię ATM; materiały konferencji POLMAN '95.

[4] Maciej Kozłowski, Roman Adamiec: WARMAN - doświadczenia eksploatacji; materiały seminarium Miedzeszyn '95; wydanie NASK

[5] Andrzej Skrzeczkowski: Technologia ATM w praktyce; materiały seminarium Miedzeszyn '95; wydanie NASK.

[6] Maciej Kozłowski, Roman Adamiec, Andrzej Skrzeczkowski: Miejska sieć komputerowa WARMAN; materiały konferencji POLMAN '96

PREZENTACJA SYSTEMU JEDNOKROTNYCH HASEŁ

Krzysztof Silicki

Naukowa Akademicka Sieć Komputerowa
Warszawa ul. Bartycka 18

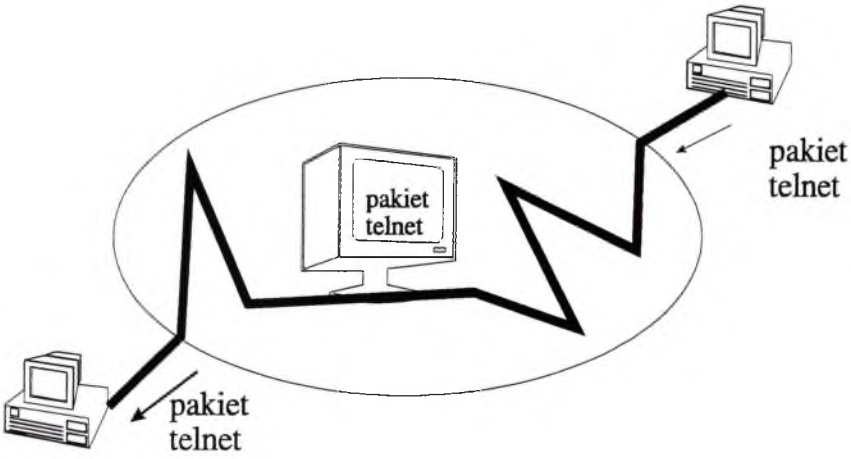
Wielka użytkowa wartość sieci rozległych w tym Internetu jest dziś powszechnie uznana. Praca w sieci podlega jednak określonym zagrożeniom, które mogą tą użytkową wartość obniżyć. Na słabościach Internetu żerują bowiem różnej maści włamywacze do systemów komputerowych podłączonych do sieci. Niektórzy robią to dla zabawy (rodzaj gry intelektualnej), inni prowadzą destrukcję (anarchiści, przestępcy, nihiliści) - istnieje też działalność wywiadowcza na tym polu.

Typowy atak intruza wpisuje się w następujący scenariusz:

- zlokalizowanie systemu do zaatakowania
- zdobycie dostępu do konta użytkownika systemu
  - brak haseł lub hasła łatwe do złamania
  - podsłuchane hasła np. wykorzystaniem snifferów
- Wykorzystanie dziur w konfiguracji i w oprogramowaniu systemowym w celu wejścia na konto uprzywilejowane
- Zatarcie śladów działalności (usunięcie z pamiętników - odpowiednich zapisów)
- przeprowadzenie nieuprawnionych działań (ich przebieg zależy od celu włamywacza)
- zainstalowanie „konia trojańskiego" dla aktualnego i przyszłego wykorzystania
- ataki na inne komputery w sieci lokalnej

W tym scenariuszu zdobycie dostępu do konta użytkownika systemu jest przełomowym etapem w przeprowadzanym przez intruza ataku. Po złamaniu lub przechwyceniu statycznego hasła należącego do użytkownika intruz uzyskuje dostęp do maszyny gdzie może już działać w sposób nieuprawniony (m.in próbować zdobywać coraz wyższe uprawnienia). Tak więc system haseł jest pierwszym i kardynalnym elementem ochrony systemu. Jest godne podkreślenia , iż nawet bardzo trudne hasła, które opierają się programom łamiącym hasła stosowanym przez hackerów (crackerów) nie stanowią wystarczającego zabezpieczenia z powodu rosnącej liczby dostępnych w Intenecie programów przechwytujących pakiety, w których przesyłane są hasła (np. tzw. sniffery) - hasła bowiem są standardowo przesyłane w postaci jawnej - łatwej do przechwycenia przez intruza.

Internet Sniffer



Rys. 1 Przechwytywanie pakietu telnet w celu podsłuchania hasła użytkownika

Oprócz ataków na serwery użytkowników coraz częstsze w Internecie są ataki na urządzenia infrastruktury zapewniającej działanie Internetu. Są to między innymi:

- Ataki na routery, serwery komunikacyjne
  - intruzi potrafią zmodyfikować konfigurację routerów
- Ataki na nameserwery i inne „strategiczne" serwery

W każdym przypadku furtką do wejścia do systemu może być przechwycenie lub złamanie hasła dostępowego.

Autentyzacja i autoryzacja

Autentyzacja i autoryzacja czyli inaczej identyfikacja i uwierzytelnienie użytkownika jawią się więc jako dwa kardynalne aspekty bezpieczeństwa stojące na straży uprawnionego dostępu do zasobów danego systemu.

Autentyzacja czyli proces identyfikacji użytkownika w momencie tzw. logowania się do systemu przysparza wielu kłopotów administratorom systemów i ich użytkownikom.

- wiele kont w sieci ma trywialne lub zbyt proste hasła (administratorzy muszą stale kontrolować odporność stosowanych przez użytkowników haseł względnie stosować mechanizmy nie zezwalające na ustawienie zbyt łatwego hasła)
- administratorzy systemów muszą stosować metody ukrywające zbiory z hasłami przed niepowołanym dostępem (np. tzw. „shadow passwords")
- nie jest możliwa pełna kontrola czy ktoś nie podsłuchuje podawanych w czasie logowania haseł użytkowników

Lepszym wyborem jest stosowanie tzw. haseł jednokrotnego użycia gdyż:

- hasła wielokrotnego logowania mogą zostać „podsłuchane" lub złamane
- hasła jednokrotne
  - są bezużyteczne dla atakującego nawet po przechwyceniu

Hasła jednokrotne mogą być implementowane programowo lub sprzętowo.
Spora ilość produktów jest dostępna już teraz. Przykładem rozwiązania programowego jest pakiet public domain S-KEY.

Najbliższa przyszłość należy jednak niewątpliwie do rozwiązań sprzętowo-programowych gdzie użytkownik posługuje się żetonem autentyzacji (ang. token) w postaci urządzenia wielkości karty kredytowej lub małego kalkulatorka z wyświetlaczem i ewentualnie klawiaturką. Żeton generuje bezpieczne hasło ważne tylko jeden raz a decyzję o pozytywnym lub negatywnym wyniku procesu autentyzacji (np. logowanie do komputera) podejmuje oprogramowanie serwera autentyzacji znajdującego się w sieci.

Autentyzacja nowoczesnymi metodami może przebiegać według dwóch schematów: metody synchronizacji czasowej lub metody „pytanie - odpowiedź"

Metoda synchronizacji czasu

- rozwiązanie sprzętowe lub mieszane
- użytkownik jest identyfikowany przy pomocy:
  - czegoś co zna (PIN)
- czegoś co posiada (token)
- system opiera się na precyzyjnej synchronizacji serwera i kart autentyzacji

Metoda pytanie-odpowiedź

- metoda sprzętowo-programowa
- serwer wysyła zapytanie do użytkownika w momencie logowania
- użytkownik przy pomocy tokena oblicza odpowiedź i wysyła do serwera autentyzacji

Jest godne podkreślenia , że metody autentyzacji w oparciu o żetony są dość niezależne od platform systemowych i nie wymagają żadnego dodatkowego wyposażenia w rodzaju - np. czytników kart.

Rozległa struktura autentyzacji

W systemach autentyzacji dostępnych obecnie u tych producentów, którzy dostosowują swą linię do specyfiki sieci rozległych - czytaj głównie Internetu dominuje kierunek umożliwienia użytkownikowi stosowania tego samego żetonu w celu logowania się na rozmaite typy urządzeń znajdujących się w sieci (patrz rys. 2). Wśród tych urządzeń są oczywiście serwery i stacje robocze (wszelkie odmiany UNIXa, NetWare, VMS i inne) ale także routery, serwery komunikacyjne a także superkomputery. Oczywiście nie chodzi tu o jakiś cudowny „superklucz" pozwalający dostawać się wszędzie - użytkownik może się pomyślnie autentyzować jedynie na te maszyny , do których dostęp został dla

niego zdefiniowany przez administratora serwera autentyzacji. Celem takiego podejścia jest po pierwsze rozszerzenie gamy urządzeń , które mogą być włączone do jednolitego systemu autentyzacji w sieci danej instytucji a po drugie maksymalna prostota w używaniu żetonów (nie jest celowe aby użytkownik posiadał kilka żetonów w celu autentyzacji na różne maszyny). W sytuacji kiedy hasło ma charakter jednokrotnego użytku jest również w naturalny sposób realizowane zalecenie aby na różne maszyny autentyzować się różnymi hasłami.

Bardzo istotne przy obsłudze rozbudowanego systemu autentyzacji jest właściwe administrowanie bazą danych użytkowników jak też opracowanie organizacji oraz procedur wydawania żetonów, czasu ich ważności, reagowania na sytuacje nietypowe itp.

Typowy proces autentyzacji

W typowej konfiguracji sieciowej systemu autentyzacji centralne miejsce zajmuje serwer autentyzacji, który częstokroć jest zduplikowany lub multiplikowany w celu podniesienia niezawodności. Klientami tego serwera są systemy stacji roboczych, routerów, serwerów komunikacyjnych, serwerów kont użytkowników czy superkomputerów. Warunkiem jest aby oprogramowanie systemowe danego urządzenia (klienta) potrafiło porozumieć się z serwerem autentyzacji w celu zaakceptowania lub odrzucenia danego użytkownika w czasie procesu autentyzacji. Użytkownik - korzystając z dowolnego terminala- w czasie procesu logowania na maszynę, która jest klientem serwera autentyzacji podaje swój identyfikator oraz hasło wygenerowane przez token (lub jego programową emulację). Żądanie zostaje przesłane poprzez sieć od maszyny klienta do serwera autentyzacji, który to serwer posiadając centralną bazę użytkowników i przypisanych im praw wydaje decyzję o odrzuceniu lub zaakceptowaniu żądania. Decyzja ta jest zwracana (także przez sieć) do maszyny klienta (router, stacja robocza, serwer kont użytkowników itp).

Autoryzacja

- Autoryzacja czyli weryfikacja czy dany użytkownik jest uprawniony do korzystania z określonych zasobów w większości przypadków wymaga modyfikacji aplikacji (wymagany dostęp do kodów źródłowych lub API). Zetony używane w procesie autentyzacji mogą również służyć do autoryzacji dostępu do aplikacji pod warunkiem stworzenia interfejsu programowego pomiędzy aplikacją a procedurami obsługi żetonu.

Józef Zalewski
TP S.A. - Dyrekcja Spółki

Cyfrowa sieć transmisyjna z dostępem do kanałów 64 kbit/s

Na temat przebudowy sieci telekomunikacyjnej TP SA z analogowej na cyfrową ukazało się już wiele publikacji. Jak sądzę - większość szczegółów dotyczących przebudowy jest ogólnie znana. Dla właściwego naświetlenia problemów towarzyszących budowie tej sieci przytoczę państwu garść faktów w moim przekonaniu już historycznych. Rozmiar i obszary wprowadzanych w sieci zmian zilustruję kilkoma istotnymi szczegółami. Oto one:

• Do końca dekady lat osiemdziesiątych w sieci telekomunikacyjnej w Polsce dominowały systemy analogowe. Systemy cyfrowe o niskiej krotności stosowano już od roku 1977 w sieciach miejscowych i strefowych, głównie dla zapewnienia współpracy central o komutacji przestrzennej z centralami E-10A.

• Szybki wzrost zapotrzebowania na połączenia międzymiastowe i międzynarodowe oraz wprowadzenie cyfrowych central telefonicznych ujawniły wady sieci analogowej. Szczególnie jej ograniczona wydolność, podatność na zakłócenia i bardzo wysokie koszty rozbudowy spowodowały podjęcie decyzji o budowie linii cyfrowych światłowodowych i radiowych. Pierwszymi zwiastunami przemian technologicznych w sieci telekomunikacyjnej w Polsce były: podmorski kabel światłowodowy Polska-Dania uwielokrotniony za pomocą systemów PDH o przepływności 140 Mbit/s, cyfrowa linia radiowa Koszalin-Warszawa o przepływności 140 Mbit/s, cyfrowa linia radiowa

Warszawa - Psary - Katowice także o przepływności 140 Mbit/s oraz cyfrowy system łączności satelitarnej INTELSAT, obsługujący region Oceanu Atlantyckiego. Zachodzące w świecie i Polsce przemiany polityczne oraz złagodzenie restrykcji technologicznych przez państwa zachodnie pozwoliły na przekazanie do eksploatacji na przełomie lat 1993/1994 linii cyfrowych Północ-Południe (NSL) i Wschód-Zachód (TEL) oraz 16 cyfrowych linii radiowych 140 Mbit/s.

Pod koniec 1995r. TP SA posiadała:

- 5100 km linii światłowodowych w sieci międzymiastowej o łącznej długości torów około 98100 km. W sieci tej pracuje 1340 grup 2 Mbit/s. Potencjał ten po przeliczeniu na kanały 64 kbit/s i porównaniu z eksploatowanymi kanałami analogowymi daje 58% cyfryzacji sieci międzymiastowej.
- 4981 km linii światłowodowych w sieci wewnątrzstrefowej o łącznej długości torów około 57000 km. W tej płaszczyźnie sieci TP SA pracuje 1540 grup 2 Mbit/s. Przeliczenie grup na kanały telefoniczne i porównanie z ilością eksploatowanych kanałów analogowych daje około 52% zcyfryzowania tej płaszczyzny sieci.

W latach 1996/1997 zostanie wybudowanych dalszych 2600 km linii światłowodowych, co umożliwi uruchomienie wiązek łączy cyfrowych do wszystkich 49 central międzymiastowych w Polsce. Rozpoczął się proces budowy sieci synchronicznej, który ma być zakończony w 1999 roku. Aktualnie funkcjonującą sieć cyfrową TP SA oraz przewidywane do budowy w najbliższych latach linie światłowodowe pokazano na rys. 1. Proszę zwrócić uwagę na fakt, że w tej nowoczesnej sieci cyfrowej pod wpływem nacisku lobby businessu na poprawę łączności telefonicznej i faksowej zapomniano o potrzebie wydzielania niekomutowanych kanałów o przepływnościach mniejszych niż 2 Mbit/s. Oznaczało to niedostosowanie sieci do świadczenia nowych usług oraz zamknięcie

dostępu do sieci wszystkim służbom i użytkownikom, które dla organizacji swoich sieci lub usług, stosują kanały o przepływnościach 64 kbit/s i ich wielokrotności. Oczekiwania operatorów wydzielonych sieci resortowych, sieci zakładowych, abonentów biznesowych, sieci specjalizowanych, jak np. POLPAK, NASK oraz komputeryzacja zarządzania TP SA i utrzymania infrastruktury sieciowej, spowodowały podjęcie decyzji o budowie takiej sieci. Ze względu na uniwersalność zastosowań i opłacalność ekonomiczną sieć ta powinna spełniać następujące główne wymagania:

- w maksymalnym stopniu wykorzystywać istniejącą infrastrukturę telekomunikacyjną TP SA;
- umożliwiać przesyłanie sygnałów zegarowych z zachowaniem taktów zegarowych pochodzących od sieci nadrzędnej;
- umożliwiać świadczenie różnego rodzaju usług, głównie dzierżawę kanałów cyfrowych 64 kbit/s i ich krotności w relacjach międzymiastowych, a także umożliwiać wydzielanie łączy na użytek własny TP SA dla potrzeb zarządzania i organizacji sieci;
- węzły sieci od strony liniowej i abonenckiej powinny być wyposażone w styki według Zalecenia G703 CCITT;
- sieć powinna być nadzorowana przez jednolity system zarządzania;
- rozwiązania techniczne powinny umożliwiać skalowalność sieci w sensie rozmiarów, przepustowości gałęzi i stosowanych protokołów komunikacyjnych;
- wydzielane dla potrzeb wewnętrznych TP SA kanały powinny umożliwiać zorganizowanie transportu informacji dla różnych systemów informatycznych TP SA a między innymi F-K, SEZTEL, Billing, Polpak, X400 itp.

Do budowy zalążków takiej sieci przystąpiono w 1994 roku. Spośród wielu oferowanych rozwiązań technicznych multiplekserów

wybór padł na multipleksery *MainStreet 3600* firmy Newbridge. Multiplekser ten jest bardzo elastycznym inteligentnym węzłem sieciowym, który spełnia równocześnie funkcje banku danych oraz zintegrowanego multipleksera kanałów głosowych i danych, a ponadto:

- umożliwia przyłączenie do 32 strumieni tak w standardzie plezjochronicznym (E1 lub T1), jak i z interfejsami V35 oraz X21 (przy przepływnościach n x 64 kbit/s;
- dla transmisji danych realizuje kanały cyfrowe z interfejsami V24; V35; X21; G703 z transmisją synchroniczną lub asynchroniczną i prędkościami transmisji od 150 bit/s do 1920 kbit/s;
- realizuje kanały głosowe ze stykami według Zalecenia G703 w tym także z możliwością kompresji 2-, 4- i 8-krotnej;
- przez zmianę wyposażenia węzeł *MainStreet 3600* może spełniać rolę komutatora pakietów *(Frame Relay)* oraz X25;
- daje się łatwo rozbudowywać przez co zwiększenie ilości kanałów w czasie eksploatacji nie jest zbyt kosztowne.

Multipleksery zastosowane w sieci TP S.A. zostały wyposażone w zespoły umożliwiające współpracę z siecią za pomocą styku 2.048 Mbit/s, a od strony abonenta:

- w karty ze stykiem X21 zgodnym z Zaleceniem X21 CCITT oraz EIA Rs-449/422 dla 3 lub 6 łączy na jednej karcie z szybkością transmisji od 150 bit/s do 1,92 Mbit/s;
- w karty 64 kbit/s współbieżne *(co-direktional)* według Zalecenia G703 dla 4 łączy na 1 karcie;
- w karty liniowe DNIC z interfejsami 2B+D dla 12 kanałów na jednej karcie, każdy port może współpracować z odległym do 4 km terminalem;

- port w karcie DNIC i terminal wyniesiony DTU współpracują ze sobą w kodzie 2B1Q, co umożliwia utworzenie kanału 2x64 kbit/s na jednej parze przewodów.

Obecnie w sieci jest zainstalowanych 48 węzłów *MainStreet* z czego w Warszawie 9. W sieci na obszarze Warszawy węzły zostały rozlokowane w CRT oraz w 8 centralach tranzytowych co pokazano na rys. 2. Szkieletowa sieć międzymiastowa jest zbudowana z kanałów o przepływności 2 Mbit/s zakończonych w węzłach usytuowanych w Białymstoku, Białej Podlaskiej, Bielsku-Białej, Bydgoszczy, Ciechanowie, Cieszynie, Gdańsku, Gdyni, Gliwicach, Jeleniej Górze, Kaliszu, Katowicach, Kielcach, Koszalinie, Krakowie, Legnicy, Lublinie, Łodzi, Łomży, Olsztynie, Opolu, Płocku, Pile, Piotrkowie Trybunalskim, Poznaniu, Radomiu, Rzeszowie, Siedlcach, Sieradzu, Słupsku, Skierniewicach, Szczecinie, Toruniu, Tarnobrzegu, Wałbrzychu, Włocławku, Wrocławiu i Zielonej Górze. Konfigurację sieci i dyslokację węzłów pokazano na rys.3. W CRT został zainstalowany duży węzeł *3645 MainStreet*, umożliwiający zakończenie 256 strumieni 2,048 Mbit/s. Będzie on spełniał rolę centralnego węzła w sieci. Już obecnie sieć jest wyposażona w dwa centralne systemy zarządzania:

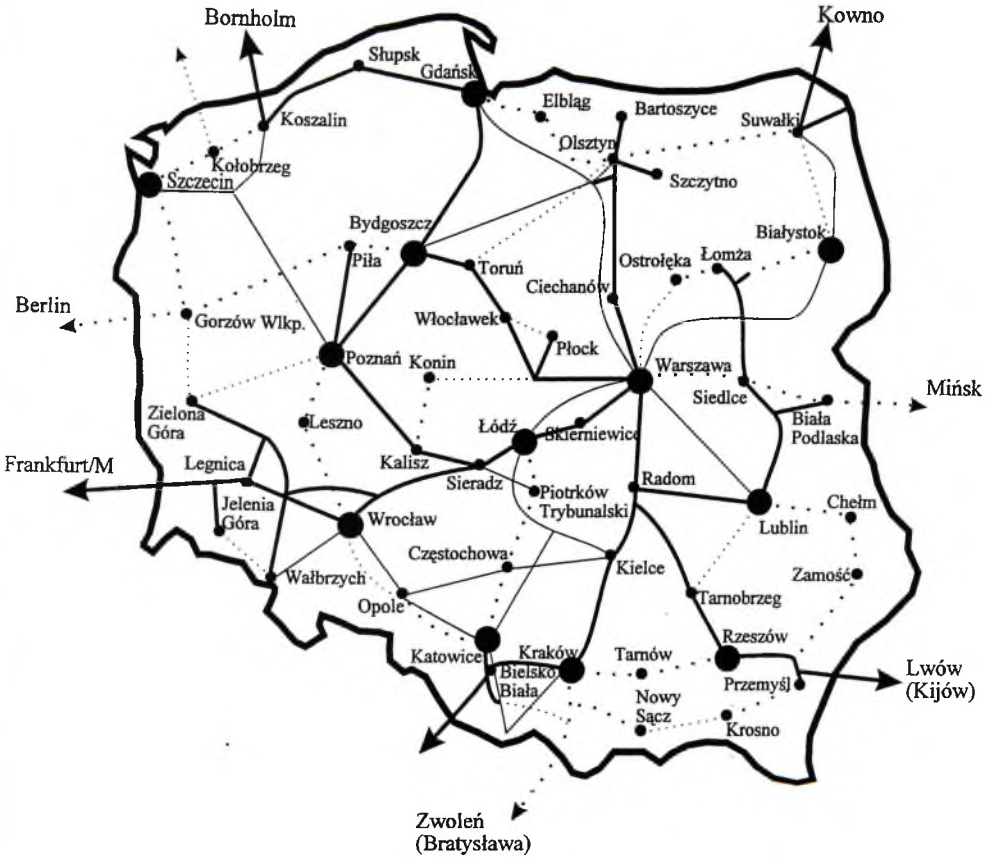
- system *4602 MainStreet*, zarządzający węzłem warszawskim;
- system *4601 MainStreet*, zarządzający węzłami w sieci międzymiastowej.

Zamierzeniem TP SA jest wybudowanie i przekazanie w 1996r. do eksploatacji węzły zainstalowane w każdym mieście wojewódzkim. Tak zbudowana sieć pozwoli TP SA zaspokoić najpilniejsze potrzeby klientów takich jak np. NASK czy TELBANK, sieci Polpak oraz własne potrzeby, niezbędne do obsługi systemów zarządzania i utrzymania infrastruktury. Równocześnie budowana jest sieć rozległa (WAN) łącząca sieci metropolitalne (MAN) zbudowane w 12 aglomeracjach (Bydgoszcz,

Gdynia, Gdańsk, Katowice, Kraków, Lublin, Łódź, Olsztyn, Poznań, Szczecin, Warszawa, Wrocław). Sieć ta umożliwi organizację usług:

- poczty elektronicznej (E-Mail);
- elektroniczny transfer dokumentów (EDI);
- dostęp do publicznych baz danych;
- realizację wirtualnych sieci prywatnych.

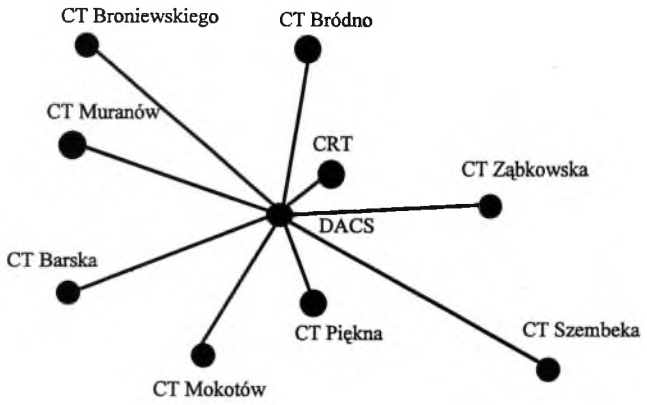
Powstanie zatem nowoczesna sieć cyfrowa, która umożliwi TP SA nie tylko świadczenie swoim klientom usługi w standardach X25, Frame Relay i ATM, ale także pozwoli zapewnić tranzyt dla ruchu generowanego przez sieci NASK, TELBANK itd.



LEGENDA:

- Istniejące linie optotelekomunikacyjne
- Istniejące cyfrowe linie radiowe
- Linie optotelekomunikacyjne budowane w latach 1995-1997 faza B I Projektu Telekomunikacyjnego
- Linie optotelekomunikacyjne przewidziane do budowy w latach 1998-1999
- Międzymiastowe centrale węzłowe
- Inne centrale międzymiastowe

Rys 1. Cyfrowa sieć międzymiastowa TP S.A.



Rys 2. Rozmieszczenie multiplekserów MainStreet na terenie Warszawy

Możliwości rozbudowy sieci transmisji danych dla potrzeb systemów teleinformatycznych TP S.A. w 1996 r.

LEGENDA:

——— Sieć istniejąca

- - - - - Plan na rok 1996

● Mainstreet 3645

● Mainstreet 3600

• Mainstreet 3630

MOŻLIWOŚCI TELEKOMUNIKACYJNE TPSA REALIZACJI USŁUG EDI W OPARCIU O PROTOKÓŁ X.435

Sławomir Michalski
Marian Suskiewicz

Telekomunikacja Polska S.A.
Warszawa, ul. Świętokrzyska 3

Wstęp

Referat ten opisuje punkt styku pomiędzy dwiema rewolucjami jakie zachodzą w świecie informatyki w ostatnim czasie - jedną w sferze telekomunikacji i drugą w sferze biznesu.

Pierwsza z nich rozpoczęła się dwadzieścia lat temu, w momencie pojawienia się eksperymentalnych prób łączenia komputerów w sieci. Przechodząc przez rozwój systemów komunikacji międzykomputerowej, doszła obecnie do powstania systemów wymiany wiadomości X.400 - zestawu międzynarodowych zaleceń, które stały się siłą napędową rozwoju ogólnoświatowej sieci wymiany informacji biznesowych.

Druga rozpoczęła się kilkadziesiąt lat temu od opracowania algorytmów obiegu dokumentów w gospodarce. Przechodząc poprzez ich wymianę za pomocą systemów pocztowych, doszła obecnie do powstania międzynarodowych standardów elektronicznej wymiany dokumentów w handlu, administracji, transporcie i przemyśle EDIFACT (w Europie) i X.12 (w USA).

W ostatnich latach stało się oczywiste, że dla szybkiej i bezbłędnej wymiany dokumentów pomiędzy partnerami gospodarczymi potrzebna jest pewna i bezpieczna, elektroniczna transmisja komputerowa. Postanowiono więc połączyć zalety transmisji X.400 ze zbieranymi przez lata doświadczeniami standaryzacji wymiany dokumentów EDI. W wyniku tego połączenia powstał nowy standard wymiany informacji X.435 dostosowany do wymiany typowych, zestandaryzowanych dokumentów biznesowych.

Protokół X.435, zwany popularnie P_{edi}, ze względu na dużą różnorodność typów przesyłanych dokumentów jest bardzo rozbudowany i skomplikowany. Głównym celem niniejszego referatu jest przybliżenie przeciętnemu słuchaczowi problematyki tego protokołu z pominięciem wszelkich zawiłości i złożoności opisujących go norm i zaleceń.

Podstawy X.400

X.400 są serią Zaleceń CCITT oraz ISO opisujących międzynarodowy standard struktury i transmisji wiadomości elektronicznych.

Analogia do tradycyjnych mechanizmów łączności telefonicznej, czy pocztowych systemów wymiany wiadomości pomaga łatwiej zrozumieć zasady działania systemów X.400.

Jeżeli porównamy X.400 do systemu telefonii kablowej, to można by powiedzieć, że X.400 odpowiada standardom rządzącym transmisją sygnałów po liniach telefonicznych: sygnały te są używane zarówno do wybierania numerów telefonicznych, jak i do transmisji wiadomości. Standardy telefoniczne nie precyzują np. kształtu, koloru i funkcji aparatów telefonicznych u użytkowników końcowych. Podobnie X.400 nie określa struktury i funkcji programów dostępowych końcowych użytkowników systemu. Natomiast X.400 ściśle określa strukturę i protokół transmisji danych przesyłanych pomiędzy dwoma takimi użytkownikami.

Państwowi operatorzy telefoniczni oferują za pomocą central różne usługi swoim abonentom. Analogiczną rolę w X.400 pełnią ADMD (Administrative Management Domains), czyli Państwowe Administracje X.400.

Poza tym większe firmy i organizacje prywatne posiadają własne wewnętrzne centralki PBX dla obsługi swoich abonentów. Podobną rolę w X.400 pełnią PRMD (Private Management Domains), czyli Prywatne Administracje X.400.

Jeżeli porównamy X.400 do systemu pocztowego, to można by powiedzieć, że X.400 jest serią standardów, które na zasadzie analogii z systemem pocztowym regulują: wielkość i kształt koperty, strukturę i zawartość adresu na kopercie oraz strukturę wiadomości przesyłanej w tej kopercie.

ADMD w tym przypadku odpowiadałaby za usługi poczty publicznej, a PRMD za usługi poczty wewnętrznej w dużych przedsiębiorstwach.

Dwoma kluczowymi pojęciami w X.400 są: UA (User Agent - Agent Użytkownika, czyli odpowiednik skrytki pocztowej) i MTA (Message Transport Agent - Agent transportu wiadomości, czyli odpowiednik urzędu pocztowego).

X.400 jest atrakcyjnym mechanizmem transmisyjnym dla danych EDI ponieważ spełnia podstawowe funkcje wymagane przez użytkowników EDI:

- Jest uniwersalnym systemem łączności: ma zasięg ogólnoświatowy, realizuje różnorodny dostęp do wszystkich użytkowników, posiada bardzo dobry i bezpieczny mechanizm transmisji danych
- Realizuje mechanizm transmisji Store and Forward (Zapamiętaj i Przekaż) tzn., że użytkownik powierza swoją wiadomość systemowi X.400, który bierze na siebie odpowiedzialność za dostarczenie jej odbiorcy nawet w przypadku, kiedy komputer odbiorcy w danym czasie nie jest dostępny

Podsumowując te dwie analogie, można by powiedzieć, że system X.400 jest jakby połączeniem standardów łączności telefonicznej i pocztowego systemu transmisji wiadomości, bardziej jednak podobny jest do systemu pocztowego, ponieważ np. w tradycyjnej telefonii przewodowej nie jest możliwe przekazanie wiadomości w sytuacji, kiedy aparat telefoniczny nie odpowiada.

Podstawy EDI

EDI (Electronic Data Interchange) może być zdefiniowane jako wymiana zestandaryzowanych dokumentów pomiędzy aplikacjami komputerowymi użytkowników końcowych.

EDI wewnątrz przedsiębiorstwa nie jest koncepcją nową. Wiele dużych firm używało EDI od kilkudziesięciu lat do wymiany wewnętrznych informacji biznesowych (np. do przesyłania zamówień) przy pomocy każdych dostępnych w danym momencie środków transmisji. Natomiast zastosowanie EDI do wymiany dokumentów z zewnętrznymi partnerami biznesowymi jest pomysłem stosunkowo nowym, bardzo dynamicznie rozwijającym się w ostatnim czasie.

Wszystkie standardy opisujące dokumenty EDI (EDIFACT, czy X.12) są standardami znakowymi, tzn. że dane wynikowe przesyłane są jako znaki ASCII lub EBCDIC. Fakt ten jest uwarunkowany historycznie.

Uzgodnienie znakowego charakteru przesyłanych dokumentów nie jest wystarczające dla EDI, ponieważ do ich transmisji muszą być używane różnego rodzaju standardy transmisji w sieciach komputerowych. Standardowe protokoły transmisyjne muszą z drugiej strony zapewnić przezroczystą, blokową transmisję danych uwzględniającą np. dzielenie bloków na pakiety, czy tzw. skramblowanie przesyłanych danych.

W dużym przedsiębiorstwie wiele różnych aplikacji biznesowych pracuje w różnych miejscach. Dopóki to było możliwe, łączono te aplikacje bezpośrednio stosując zasadę „każdy z każdym". Stosowano wówczas różne dostępne sposoby komunikacji. Taki był początek powstawania biznesowych sieci komputerowych wewnątrz przedsiębiorstw.

Nieco później powstały standardy wymiany dokumentów i co za tym idzie tzw. gateway'e korporacyjne, które przekształcały dokumenty z istniejących wcześniej formatów wewnętrznych danego przedsiębiorstwa na standardowe formaty EDI (jak np. EDIFACT, czy X.12) i przesyłały je do innych partnerów biznesowych używając prywatnych sieci komputerowych i prywatnych protokołów transmisyjnych (takich jak np. OFTP).

Następował burzliwy rozwój, zarówno prywatnych sieci komputerowych jak i prywatnych protokołów transmisyjnych. Powstały zamknięte organizacje branżowe takie jak np. CEFIC w przemyśle chemicznym, EDIFICE w elektronicznym, ODETTE w samochodowym itd.

W miarę rozwoju wymiany dokumentów biznesowych przyszedł w końcu czas na uregulowania normatywne zarówno w sieciach komputerowych jak i w protokołach transmisyjnych. Efektem przeprowadzonych na początku lat dziewięćdziesiątych prac normalizacyjnych na szczeblu międzynarodowym jest omawiany tu protokół X.435, zwany potocznie P_{edi}.

Szczególne cechy protokołu X.435

Protokół P_{edi} posiada kilka szczególnych cech unikalnych dla niego samego, których nie można znaleźć, ani w ogólnie znanym protokole X.400, ani w innych, prywatnych protokołach transmisyjnych do dzisiaj powszechnie stosowanych w EDI.

Należą do nich między innymi :

- Struktura dokumentów EDI
  - Nagłówek dokumentów EDI
  - Wieloczęściowa treść dokumentów EDI
- Odsyłacze do poszczególnych części dokumentów EDI (Cross-referencing)
- Przekierowania przesyłanych dokumentów EDI (Forwarding)
- Odpowiedzialność za przesyłane dokumenty EDI (Responsibility)
- Zawiadomienia EDI (Notifications)
- Bezpieczeństwo transmisji dokumentów EDI (Security)

Struktura dokumentów EDI

Najogólniej rzecz ujmując, dokument EDI składa się z nagłówka i treści dokumentu.

Nagłówek dokumentów EDI, w stosunku do typowego nagłówka wiadomości X.400, jest bardziej rozbudowany, ponieważ zawiera w sobie zarówno dane specyficzne dla komunikatu X.400, jak i dla dokumentu elektronicznego.

Treść przesyłanego dokumentu EDI, zwana także wymianą, zawiera pakiet różnych dokumentów przeznaczonych dla danego partnera biznesowego.

Nagłówek dokumentów EDI

Nagłówek dokumentów EDI zawiera wiele pól, które można podzielić na dwie kategorie:

- pola dotyczące transmisji X.400, jak np. adres odbiorców przesyłanych dokumentów EDI
- pola dotyczące wymiany EDI, realizujące wszelkie wymagane żądania użytkownika końcowego, jak np. standard dokumentu EDI (EDIFACT, X.12, ...), format dokumentu (ASCII, EBCDIC), rodzaj dokumentu (np. zamówienie, potwierdzenie zamówienia, faktura ...), sposób realizacji zawiadomień o dostarczeniu dokumentu.

Wieloczęściowa treść dokumentów EDI

Treść wymiany dokumentów EDI z reguły bywa wieloczęściowa. W czasie transmisji nie ma możliwości wprowadzania jakichkolwiek zmian w przesyłanej treści. Istnieje jednak możliwość przesyłania poszczególnych części treści różnym użytkownikom końcowym (np. zamówień do działu inwestycji, faktur do działu księgowości) lub dynamicznego dodawania nowych elementów treści do danej wymiany w czasie transmisji.

Odsyłacze do poszczególnych części treści dokumentów EDI (Cross-referencing)

Odsyłacze, obok wieloczęściowej treści dokumentów, są jeszcze jednym uzupełniającym mechanizmem EDI. Służą do dodatkowego wiązania poszczególnych części treści wiadomości między sobą.

Informacja o odsyłaczach przechowywana jest w nagłówku przesyłanego dokumentu. Daje to możliwość inteligentnym aplikacjom użytkowników końcowych uzyskania informacji o powiązaniach pomiędzy poszczególnymi częściami treści dokumentów bez ingerencji do ich wnętrza. Wykorzystując odsyłacze można np. automatycznie przesłać załączone do dokumentu rysunki do działu projektowania przedsiębiorstwa.

Przekierowania przesyłanych dokumentów EDI (Forwarding)

W sytuacji, w której poszczególni użytkownicy połączeni są bezpośrednio „każdy z każdym" nie ma potrzeby przekierowywania przesyłanych dokumentów. Potrzeba taka powstaje wówczas, kiedy sieć staje się coraz bardziej skomplikowana np. kiedy zainstalowane są w niej gateway'e korporacyjne. Zdarzyć się wtedy może sytuacja, w której odbiorca końcowy dokumentu EDI nie jest osiągalny bezpośrednio, a poprzez sieć gatweay'ów korporacyjnych. W czasie transmisji dokumentu do takiego odbiorcy konieczny staje się mechanizm przekierowywania przesyłanego dokumentu przez poszczególne gateway'e.

Odpowiedzialność za przesyłane dokumenty EDI (Responsibility)

Przy przesyłaniu dokumentów EDI nadawcami i odbiorcami są aplikacje poszczególnych użytkowników końcowych. To one faktycznie decydują co, do kogo i w jaki sposób jest przesyłane. Biorą one także na siebie pełną odpowiedzialność za przesyłane dokumenty. Ma to istotne znaczenie w sytuacji konieczności przekierowywania dokumentów w czasie transmisji, bowiem oprócz przekierowywania dokumentów musi zostać rozwiązana sprawa przekazywania odpowiedzialności za te dokumenty.

Zawiadomienia EDI (Notifications)

Z odpowiedzialnością wiążą się zawiadomienia o przesyłanych dokumentach EDI, które zasadniczo różnią się od potwierdzeń stosowanych w standardzie X.400, a mianowicie potwierdzenia X.400 realizowane są automatycznie pomiędzy zaangażowanymi MTA, zaś zawiadomienia EDI realizowane są na żądanie przez poszczególne UA.

Istnieją trzy typy zawiadomień EDI:

- PN (Positive Notification, czyli Zawiadomienie pozytywne), kiedy aplikacja użytkownika końcowego przejmuje odpowiedzialność za przekazany dokument
- NN (Negative Notification, czyli Zawiadomienie negatywne), kiedy aplikacja użytkownika końcowego odrzuca odpowiedzialność za przekazany dokument
- FN (Forwarding Notification, czyli Zawiadomienie o retransmisji), kiedy w przypadku przekierowania dokumentu zostaje także przekierowana odpowiedzialność za przekazany dokument

Bezpieczeństwo transmisji dokumentów EDI

Protokół P_{edi} zawiera w sobie kilka elementów bezpieczeństwa unikalnych dla niego samego, które zapewniają bezpieczne przesyłanie dokumentów pomiędzy użytkownikami końcowymi, nawet w przypadku, kiedy komunikaty EDI muszą być przekierowywane.

Zagrożenia

Podstawowymi zagrożeniami bezpieczeństwa przesyłania dokumentów EDI uszeregowanymi według priorytetu ważności są:

- Utrata łączności w czasie transmisji
- Ujawnienie przesyłanych informacji
- Nieautoryzowany dostęp do sieci z poza przedsiębiorstwa
- Oszustwa
- Nieautoryzowany dostęp do sieci wewnątrz przedsiębiorstwa

Podstawowe elementy bezpieczeństwa EDI

Podstawowymi elementami bezpieczeństwa z punktu widzenia protokołu P_{edi} są:

- Zapewnienie jednoznacznej identyfikacji użytkownika końcowego (User authentication)
- Zapewnienie integralności przesyłanych dokumentów (Message integrity)
- Potwierdzenie otrzymania przesyłanego dokumentu pomiędzy użytkownikami końcowymi (Confirmation of end-to-end delivery)

Nieprzerwana dostępność usługi EDI (Availability), łącząca się z utratą łączności w czasie transmisji, tak naprawdę nie jest cechą bezpieczeństwa przesyłanej informacji z punktu widzenia protokołu P_{edi}, a elementem bezpieczeństwa mechanizmów wykorzystywanej sieci.

Wymagane elementy bezpieczeństwa EDI

Wymaganymi elementami bezpieczeństwa z punktu widzenia protokołu P_{edi} są:

- Tajność przesyłanych komunikatów EDI (Message confidentiality)
- Możliwość rejestracji i monitorowania wszystkich zdarzeń zachodzących w czasie przesyłania poszczególnych dokumentów EDI (Audiatability)
- Niezaprzeczalność potwierdzenia odbioru przesyłanych dokumentów (Non-repudiable confirmation of receipt)

Zastosowanie protokołu X.435 w EDI

Istnieje wiele sposobów w jaki poszczególni użytkownicy wykorzystują EDI. Protokół P_{edi} zawiera w sobie wszystkie cechy użyteczne, niezbędne w typowych przypadkach zastosowań:

- UA obsługujący jedną aplikację
- Gateway korporacyjny obsługujący całe przedsiębiorstwo
- VANS (Value Added Network Service, czyli Sieć Usług Dodanych)

W praktyce zwykle spotykane są różne przypadki pośrednie pomiędzy wymienionymi wyżej najbardziej typowymi.

UA obsługujący jedną aplikację

Jest to najprostszy przypadek i jedyny, który nie wykorzystuje licznych zalet protokołu P_{edi}. W tym przypadku każda aplikacja użytkownika końcowego UA posiada swój własny adres X.400 i funkcjonuje w pełni samodzielnie.

Gateway korporacyjny

Z punktu widzenia zewnętrznych partnerów biznesowych danego przedsiębiorstwa, jedynie gateway korporacyjny posiada własny adres X.400 dostępny na zewnątrz firmy. Przejmuje on i rozsyła całą korespondencję dla danej instytucji. Jeżeli chodzi o odpowiedzialność za przesyłane dokumenty, to mamy tu dwa przypadki:

Gateway korporacyjny przejmujący odpowiedzialność za dostarczenie wiadomości EDI

W pierwszym przypadku gateway korporacyjny przejmuje odpowiedzialność za wszystkie wymiany dokumentów jakie otrzymuje i potwierdza ich odbiór na żądanie nadawców.

Gateway korporacyjny przekazujący odpowiedzialność za dostarczenie wiadomości EDI

W drugim przypadku gateway korporacyjny nie przejmuje odpowiedzialności za wymiany dokumentów jakie otrzymuje i nie potwierdza ich odbioru na żądanie nadawców. Poszczególne wymiany i odpowiedzialność za nie są przekierowywane do aplikacji użytkowników końcowych, które z kolei przejmują tę odpowiedzialność i udzielają potwierdzeń za odbiór otrzymanych dokumentów na żądanie nadawców.

VANS, czyli Sieć Usług Dodanych

Jest to najbardziej zaawansowany przypadek zastosowania EDI.

Polega on na przekazaniu wszelkich obowiązków gateway'a korporacyjnego operatorowi zewnętrznemu - prywatnemu lub państwowemu i na rozszerzeniu usług EDI o dodatkowe elementy, takie jak np. kodowanie dokumentów przygotowywanych w różnych standardach (EDIFACT, X.12, ...), konwersja między różnymi protokołami transmisyjnymi (X.435, OFTP, ...), ochrona przesyłanych dokumentów itp.

Umowa z operatorem sieci VANS nie musi dotyczyć odpowiedzialności za odbiór poszczególnych dokumentów, a jedynie za ich poprawną transmisję.

Moduł EDI w systemie POLKOM/400 firmy ISOCOR

Po podpisaniu w 1995 r. kontraktu z francuską firmą SYSECA, TP S.A. zakupiła system wymiany wiadomości X.400, nazwany później POLKOM/400. Jądrem tego systemu jest oprogramowanie znanej amerykańskiej firmy ISOCOR. System ten stanowi kompletne rozwiązanie, zarówno dla operatora publicznego, jak i dla użytkownika końcowego.

POLKOM/400 jest systemem wymiany wiadomości X.400 uruchomionym niedawno w Centrum Systemów Teleinformatycznych TP S.A. (Polpak). Zbudowany jest on z wielu specjalizowanych modułów funkcjonalnych takich jak np. Poczta elektroniczna X.400 ('88), Książka teleadresowa X.500, fizyczne moduły dostępowe: faksowy i teleksowy, gateway'e do innych systemów poczty elektronicznej: CC-mail, MS-mail, czy Internet.

Moduł realizujący EDI jest integralną częścią tego systemu ściśle współpracującą z jego pozostałymi elementami. Realizuje on w pełni standard X.435 łącznie ze szczególnymi cechami i licznymi udogodnieniami opisanymi w tym referacie.

Za pomocą tego modułu można przesyłać dokumenty EDI w następujących standardach:
- EDIFACT
- X.12
- UN/TDI

Moduł EDI systemu POLKOM/400 współpracuje z dowolnymi aplikacjami końcowymi użytkowników działającymi w standardzie X.435. Posiada także interfejs programowy (API - Application Programming Interface) pozwalający na tworzenie własnych aplikacji użytkownika.

Podsumowanie

Wykorzystanie elektronicznej wymiany dokumentów EDI w naszej gospodarce stało się faktem. Coraz więcej firm, banków i dużych przedsiębiorstw zaczyna dostrzegać korzyści płynące z tej formy wymiany dokumentów.

Opisany w tym referacie poglądowo protokół P_{edi}, którego dokładny opis znajduje się w zaleceniach F.435 i X.435 CCITT, a także w ich odpowiednikach ISO, jest rozwiązaniem bardzo młodym. Dopiero w ostatnich latach pojawiły się pierwsze jego implementacje na różnych platformach sprzętowo-programowych. System POLKOM/400 jest też przykładem takiego rozwiązania.

Prawdą jest także to, że wdrożenie EDI jest długotrwałym i kosztownym procesem. Dlatego też adresowane jest ono głównie do zasobnych i dużych klientów. Koszt usługi EDI wynika z faktu wykorzystywania przez nią bezpiecznych rozwiązań sieci X.400, która obecnie jest stosunkowo droga na całym świecie.

Z drugiej zaś strony realizacja EDI w sposób bezkosztowy, za pomocą publicznej sieci telefonicznej, z pominięciem podstawowych zasad bezpieczeństwa wprowadza duże ryzyko dla wszystkich partnerów wymiany dokumentów. Pozorne, chwilowo osiągane oszczędności mogą okazać się nieopłacalne na dalszą metę.

Rozsądnym więc podejściem jest wykorzystanie tej nowej i bezpiecznej możliwości realizacji EDI jaka pojawiła się na naszym rynku.

Literatura

1. CCITT Recommendation X.208 (ISO 88241), Specification of Abstract Syntax Notation One (ASN.1), 1988.
2. CCITT Recommendation X.209 (ISO 88251), Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1), 1988.
3. CCITT Recommendation X.400 (ISO 10021-1), [Recommendation for Message Handling (MHS); International Standard for Information Processing Systems - Text Communication - Message-Oriented Text Interchange Systems (MOTIS)]: Systems and Service Overview, 1988.
4. CCITT Recommendation X.402 (ISO 10021-2), [Recommendation for MHS; International Standard for MOTIS]: Overall Architecture, 1988.
5. CCITT Recommendation X.403, Recommendation for MHS: Conformance Testing, 1988.
6. CCITT Recommendation X.407 (ISO10021-3), [Recommendation for MHS; International Standard for MOTIS]: Abstract Service Definition Conventions, 1988.
7. CCITT Recommendation X.408, Recommendation for MHS: Encoded Information Type Conversion Rules, 1988.
8. CCITT Recommendation X.411 (ISO 10021-4), [Recommendation for MHS; International Standard for MOTIS]: Message Transfer System: Abstract Service Definition and Procedures, 1988.
9. CCITT Recommendation X.413 (ISO 10021-5), [Recommendation for MHS; International Standard for MOTIS]: Message Store: Abstract Service Definition, 1988.
10. CCITT Recommendation X.419 (ISO 10021-6), [Recommendation for MHS; International Standard for MOTIS]: Protocol Specifications, 1988.
11. CCITT Recommendation X.420 (ISO 10021-7), [Recommendation for MHS; International Standard for MOTIS]: Inter Personal Messaging, 1988.
12. CCITT Recommendation X.500 (ISO 9594-1), [Recommendation for Directory International Standard for Information Processing Systems - Open Systems Interconnection - The Directory (Directory)]: Overview of Concepts, Models, and Service, 1988.
13. CCITT Recommendation X.501 (ISO 9594-2), [Recommendation for Directory International Standard for Directory]: Models, 1988.
14. CCITT Recommendation X.511 (ISO 9594-3), [Recommendation for Directory International Standard for Directory]: Abstract Service Definition, 1988.
15. CCITT Recommendation X.518 (ISO 9594-4), [Recommendation for Directory International Standard for Directory]: Procedures for Distributed Operation, 1988.
16. CCITT Recommendation X.519 (ISO 9594-5), [Recommendation for Directory International Standard for Directory]: Protocol Specifications, 1988.
17. CCITT Recommendation X.520 (ISO 9594-6), [Recommendation for Directory International Standard for Directory]: Selected Attribute Types, 1988.
18. CCITT Recommendation X.521 (ISO 9594-7), [Recommendation for Directory International Standard for Directory]: Selected Object Classes, 1988.
19. CCITT Recommendation X.509 (ISO 9594-8), [Recommendation for Directory International Standard for Directory]: Authentication Framework, 1988.
20. CCITT Recommendation F.435, Recommendation for Message Handling: EDI Messaging Service.

21. CCITT Recommendation X.435, Recommendation for Message Handling Systems: EDI Messaging System.
22. ISO 9735, Electronic data interchange for administration, commerce and transport (EDIFACT) - Application level syntax rules, 1987.
23. The EDI Handbook: Trading in the 1990s, edited by Mike Gifkins and David Hitchcock, published by Blenheim Online Publications, 1988.
24. What is EDI?, by Martin Preston, published by NCC Publications, 1988.
25. Electronic Data Interchange and Paperless Trading, The Implementation Guide, by Euromatica, published by Euromatica, 1988.
26. L'EDI pour l'entreprise, by Victor Sandoval, published by Hermes, 1990
27. La Technologic de l'EDI, by Victor Sandoval, published by Hermes.

INTERNET W DZIAŁALNOŚCI GOSPODARCZEJ - USŁUGI, SPOSOBY DOSTĘPU, BADANIA WYKORZYSTANIA SIECI INTERNET DO DZIAŁALNOŚCI KOMERCYJNEJ

Józef Janyszek

Naukowa i Akademicka Sieć Komputerowa
ul. Bartycka 18
00-716 Warszawa

1. Wstęp

Historia światowej sieci komputerowej Internet liczy sobie zaledwie 15 lat. W 1996 roku liczba komputerów włączonych do sieci Internet przekroczyła 10 mln sztuk. Historia polskiego Internetu jest znacznie krótsza i zaczyna się 10 lat później. W końcu marca 1996 roku do sieci Internet w Polsce było włączonych ponad 30 tys. komputerów. Wśród krajów Europy Środkowej i Wschodniej, w liczbach bezwzględnych Polska posiada obecnie największą ilość komputerów włączonych do sieci Internet. Gdyby jednak porównać ilości komputerów przypadających na 100 tys. mieszkańców to Polskę znacznie wyprzedzają Czechy i Węgry.

Z sieci Internet korzystają różne środowiska: naukowo-akademickie, szeroko pojętej administracji państwowej, szkolnictwa i gospodarki.

Środowisko gospodarcze w wielu krajach jest dominujące wśród użytkowników sieci Internet. W Polsce sieć Internet w sektorze gospodarczym zaczyna się również szybko rozwijać. Gdyby rozwój polskiego Internetu przebiegał podobnie jak w Stanach Zjednoczonych, to w najbliższych latach należy spodziewać się spowolnienia tempa rozwoju w sektorze naukowo-akademickim, a zwiększenie tempa w sektorze gospodarczym (komercyjnym). Za takim scenariuszem rozwoju również przemawia fakt, że w wielu uczelniach w kraju ilość komputerów włączonych do sieci Internet zbliża się do wartości maksymalnych.

2. Wykorzystanie infrastruktury technicznej środowisk naukowo-badawczych do zastosowań komercyjnych

Internet powstał w Stanach Zjednoczonych w środowisku naukowo-badawczym dla potrzeb kompleksu militarno-przemysłowego w celu zapewnienia komunikacji między jednostkami administracji rządowej a uniwersytetami i wielkimi przedsiębiorstwami pracującymi na rzecz przemysłu zbrojeniowego. Finansowanie i rozwój Internetu odbywało się z funduszy federalnych, co wykluczało wykorzystanie Internetu do celów komercyjnych. Narodowa Fundacja Nauki (National Science Fundation), agencja rządu USA finansowała utrzymanie sieci szkieletowej NFSnet. Sieć NFSnet była znaczącą częścią globalnej sieci Internet. Sieć NFSnet początkowo była przeznaczona dla środowiska akademickiego i badawczego i przesyłanie informacji dla celów komercyjnych przez tę sieć było zabronione. Narodowa Fundacja Nauki utrzymywała również połączenia transatlantyckie do kilku krajów Europy Zachodniej. Z tego powodu sieć Internet była również niedostępna dla ruchu komercyjnego w Europie. Z drugiej strony utrzymanie zakazu komercji w praktyce w pełni nie było skuteczne ze względu na pakietowy charakter sieci. Komercyjni dostawcy usług sieciowych stworzyli alternatywną sieć szkieletową o nazwie CIX (Commercial Internet eXchange). Późniejsze sieci szkieletowe jak CO + RE (Commercial plus Research and Educational) i CoREN (Corporation for Regional and Enterprise Networking) były dostępne dla użytkowników komercyjnych, badawczych i edukacyjnych.

Powstało również szereg projektów komercjalizacji Internetu takich jak CommerceNet. Prezydent Bill Clinton, wkrótce po objęciu urzędu, zapowiedział poparcie dla planu budowy Narodowej Infrastruktury Informatycznej dostępnej dla komercji, edukacji, badań, administracji. Sam Internet w USA ulega szybkiemu procesowi komercjalizacji. Stopniowe dopuszczenie użytkowników komercyjnych do sieci Internet następowało od początku lat dziewięćdziesiątych, czyli wcześniej niż zaczęła się historia polskiego Internetu. Stąd też nie pojawiły się ostre restrykcje w stosunku do środowiska komercyjnego w Polsce. Sieć szkieletowa NASK dostępna jest zarówno dla środowiska akademickiego, badawczego jak i komercyjnego.

3. Usługi sieciowe wykorzystywane przez środowisko komercyjne

Środowisko komercyjne wykorzystuje sieć Internet jako narzędzie wspomagające działalność gospodarczą. W związku z tym wykorzystuje w zasadzie tylko takie narzędzia, które ułatwiają porozumiewanie się, przesyłanie plików, prowadzenie dyskusji, prezentację firmy, prowadzenie reklamy oraz marketingu.

Środowisko komercyjne z całego repertuaru usług wykorzystuje najczęściej usługę poczty elektronicznej, przesyłanie plików oraz korzystanie z takich systemów informacyjnych jak: Gopher, WWW, Nowości Sieciowe. Możliwe jest także korzystanie z innych usług, ale są to przypadki odosobnione. Oddzielną grupę zastosowań komercyjnych stanowią tzw. dostawcy usług internetowych, którzy muszą z konieczności udostępniać pełny zestaw usług sieci Internet.

3.1. Poczta elektroniczna

Poczta elektroniczna jest najbardziej popularną publiczną usługą sieci Internet. Korzystają z niej dziesiątki milionów użytkowników na całym świecie. Użytkownicy sieci Internet mają także możliwość przesłania poczty do innych sieci komercyjnych takich jak CompuServe (użytkownik@compuserve.com), MCIMail (użytkownik@mcimail.com), America Online (użytkownik@aol.com), X400 i wielu innych.

Poczta elektroniczna staje się dominującą formą komunikacji dla celów gospodarczych. Może to być komunikacja między centralą firmy a jej placówkami terenowymi, komunikacja między kooperującymi firmami, komunikacja między firmą a jej klientami. Poczta elektroniczna jest też doskonałym narzędziem do dystrybucji informacji do wielu użytkowników. Szczególnie przydatne w tym zakresie są tzw. listy pocztowe. Łatwo tą drogą przesyłać do klientów, użytkowników informacje: o nowych produktach firmy, zasadach dystrybucji, cenach, warunkach dostawy, itp. Poczta elektroniczna może być również użyta do działań gospodarczych powodujących skutki finansowe. Należy jednak pamiętać, że poczta internetowa zapewnia niski poziom bezpieczeństwa - nie zabezpiecza tajemnicy informacji. Przesyłając pocztą elektroniczną zamówienia, np. z numerem karty kredytowej, musimy mieć pewność, że to zamówienie dotrze pod wskazany adres w postaci niezmienionej i że zamówienie to odbierze wskazany odbiorca. Taki poziom bezpieczeństwa poczty elektronicznej w sieci Internet mogą zapewnić tylko techniki kodowania.

3.2. Przesyłanie plików

Usługa przesyłania plików pozwala użytkownikom sieci Internet przesyłać i otrzymywać pliki wewnątrz sieci. Prawie każdy użytkownik dołączony do sieci Internet posiada możliwość korzystania z tej usługi, zwanej krótko FTP od angielskiej nazwy File Transfer Protocol. Dla zastosowań komercyjnych tworzy się serwery FTP dostępne dla wszystkich użytkowników Internetu lub tylko dla selekcyjnie wybranej grupy. Serwer FTP może być użyty jako narzędzie do przesyłania, odbioru zamówień handlowych, folderów, raportów. Tworząc publiczny serwer FTP, zwany serwerem anonimowym, można łatwo dystrybuować informacje takie jak: katalogi, cenniki, dokumenty związane z obsługą produktu (okresowe przeglądy, zmiany modernizacyjne) i wiele innych. W sieci Internet znajdują się tysiące publicznych serwerów FTP, które są wykorzystywane do dystrybucji wszelkiego rodzaju plików, a więc plików tekstowych i binarnych.

3.3. System informacyjny - Gopher

Gopher jest systemem informacyjnym, który pozwala na tworzenie, magazynowanie i przesyłanie informacji w sieci Internet. Zbudowany jest on według zasady "klient - serwer". Tworzenie, magazynowanie informacji przeznaczonej do dystrybucji wymaga instalacji oprogramowania typu serwer. Sam dostęp do informacji znajdującej się na serwerze wymaga instalacji tylko oprogramowania typu Klient. Informacja może być typu tekstowego, graficznego, nawet dźwiękowego. System Gopher zawiera także przejścia (interfejsy) do innych systemów informacyjnych takich jak: WAIS, Archie oraz usług typu Telnet, FTP. Jest niezwykle prosty w obsłudze, za pomocą menu pozwala łatwo odnajdować potrzebne informacje. Z punktu widzenia użytkownika można go porównać do katalogu głównego (menu główne) z wieloma podkatalogami. Wyżej przedstawione cechy tego systemu preferują go do zastosowań komercyjnych. W oparciu o system Gopher łatwo zbudować prezentację małej firmy, konsorcjum lub holdingu w świecie Internetu. Większość informacji może być zapisana w formacie tekstowym, a tym samym łatwo

dotrzeć z nią do odbiorcy. Dla zaawansowanego odbiorcy można zbudować menu z informacją graficzną lub nawet dźwiękową.

3.4. System informacyjny WWW (Word Wide Web) - Światowa Pajęczyna

System ten też jest zbudowany na zasadzie "klient - serwer". Chcąc być dostawcą informacji w tym systemie trzeba posiadać oprogramowanie typu serwer, dla odbiorcy wystarczy oprogramowanie typu Klient. Informacja w tym systemie jest zapisana w postaci "hipertekstu", czyli w formacie, który charakteryzuje się tym, że na stronach hipertekstu występują specjalne łączniki (links) umożliwiające przejście do innych stron hipertekstowych. Łączone strony mogą znajdować się na różnych serwerach. Informacja udostępniona poprzez system WWW może być w postaci tekstowej, graficznej, dźwiękowej a nawet w postaci animacji. System adresowany jest do użytkowników zaawansowanych, gdyż odbiorca informacji musi być w zasa-dzie włączony do sieci Internet, tj. posiadać własny adres IP. Użytkownicy tego systemu posługują się przeglądarkami (przeglądarkami nazywa się oprogramowanie typu Klient, które są znane jako Mosaic, Netscape, HotJava, Lynx). Ostatnia z wymienionych przeglądarek pozwala na dostęp do systemu WWW bez konieczności posiadania adresu IP. Wystarczy posiadać konto na komputerze dostawcy usług.
System WWW doskonale nadaje się do zastosowań komercyjnych. Pozwala on na prezentacje firmy w różnorodnych formach. Mogą to być informacje tekstowe o firmie, lista produktów firmy, lista cen, jak również same produkty w formie zdjęć kolorowych, czy nawet animacji (pokazanie produktu z różnych stron).

3.5. System informacyjny Nowości Sieciowe (Netnews)

Nowości Sieciowe to rozproszony system konferencyjny sieci Internet. Istnieje ponad 5000 różnych grup dyskusyjnych. Grupy są zbudowane hierarchicznie. Istnieje kilka głównych tematów dyskusyjnych takich jak: comp (nauki komputerowe), sci (wszystkie pozostałe dziedziny nauki), rec (rekreacja, hobby). Wśród tych głównych tematów znajduje się również temat biz (biznes, zastosowania komercyjne). Wokół głównego tematu mogą być utworzone podtematy dyskusyjne, np. biz.misc (biznes różnorodny). System Nowości Sieciowych daje możliwości określania dystrybucji informacji. Swym zasięgiem może obejmować region, kraj, kontynent lub świat. Istnieje także możliwość tworzenia grup dyskusyjnych filtrowanych, tj. takich, że informacja wysłana do odbiorców grup dyskusyjnych może być dopuszczona do dystrybucji lub nie. Użytkownik systemu Nowości Sieciowych korzysta ze specjalnego oprogramowania zwanego czytnikiem. Istnieje wiele znanych czytników: tin, rn, nn i inne. Także edytor poczty elektronicznej Pine pozwala na czytanie Nowości. Oprogramowanie typu czytnik pozwala na zapisanie się do grupy dyskusyjnej, czytanie informacji napływających z grupy, odpowiadanie na wybrane informacje lub wysyłanie nowych, własnych informacji.
Przedstawione cechy systemu Nowości Sieciowych preferują go do zastosowań komercyjnych. Nietrudno bowiem sobie wyobrazić utworzenie grupy dyskusyjnej o zasięgu regionalnym lub krajowym na temat jak promować firmę z wykorzystaniem sieci Internet. Promocja czy reklama firmy poprzez system Nowości Sieciowych może okazać się ryzykowną, gdyż w rezultacie może się pojawić szereg informacji szkodzących dobremu obrazowi firmy, nadawanych chociażby przez konkurencję.

4. Rodzaje dostępu do sieci Internet dla użytkowników/abonentów komercyjnych

Rodzaj dostępu do sieci Internet, jaki może wybrać firma komercyjna, zależy od wyboru usług i systemów informacyjnych z jakich zamierza ona korzystać. Na wybór rodzaju dostępu do Internetu ma również wpływ podjęcie decyzji, czy firma zamierza samodzielnie zaistnieć w sieci Internet czy też poprzez tzw. dostawcę usług sieciowych (provider'a).

4.1. Dostęp do usług sieci Internet poprzez łącza komutowane

Dostęp do wielu usług można uzyskać poprzez łącza telefoniczne komutowane. Wystarczy komputer użytkownika wyposażyć w modem analogowy i w odpowiedni program sterujący. Funkcje tego programu mogą być różne w zależności od rodzaju usług sieciowych z jakich użytkownik zamierza korzystać. Dla przykładu może to być emulator typowego terminala VT100, który gwarantuje dostęp w trybie tekstowym lub np. pakiet I-COMM (sharware software) gwarantujący dostęp w trybie graficznym.

Dostęp do usług sieci Internet poprzez łącza telefoniczne można podzielić na dwie kategorie.
Pierwsza kategoria to użytkownicy, którzy nie posiadają własnego adresu internetowego (ich adres składa się z identyfikatora (nazwy konta) i adresu internetowego dostawcy usług). Są to użytkownicy, których zalicza się do klasy biernych użytkowników.
Drugą kategorię stanowią użytkownicy posiadający własne numery (adresy) internetowe. Ich podłączenie do sieci Internet odbywa się poprzez protokoły SLIP (Serial Line Internet Protocol), PPP (Point to Point Protocol). Tych użytkowników zalicza się do klasy aktywnych użytkowników.

4.2. Dostęp do usług poprzez łącza telefoniczne trwałe

Łącza komutowane w wielu przypadkach charakteryzują się niskim poziomem jakości transmisji, małą przepustowością praktycznie nie przekraczającą 28,8 kb/s. Przy intensywnym wykorzystywaniu opłaty telefoniczne za tzw. impulsy mogą przekraczać koszty łącz trwałych.
Poprzez łącza trwałe można zapewnić dostęp do sieci Internet wielu użytkownikom sieci lokalnych, czyli zapewnia się dostęp abonentowi. Abonent sieci posiada własną klasę adresową, własny serwer nazw domenowych, serwer systemów informacyjnych. Dostęp poprzez łącza trwałe może być realizowany poprzez serwery komunikacyjne z asynchronicznym trybem transmisji i poprzez routery z synchronicznym trybem transmisji i różnymi protokołami jak HDLC, FR, ATM.

4.3. Inne sposoby dostępu do sieci Internet

W Polsce w przeważającej większości firmy komercyjne uzyskują dostęp do Internetu poprzez dzierżawione linie telefoniczne. Jednak w wielu krajach masowo wykorzystuje się inne sposoby, między innymi poprzez linie ISDN i telewizję kablową.

4.3.1. Dostęp poprzez sieć ISDN

W wielu krajach oferowana jest usługa dostępu do Internetu poprzez linie ISDN (Integrated Services Digital Network). Dla szybkiego podłączenia się do sieci Internet można wykorzystać np. kanał cyfrowy o przepustowości 64 kb/s.
Ten sposób dostępu może być oferowany w Polsce.

4.3.2. Dostęp poprzez telewizję kablową

Telewizja kablowa jako nośnik wykorzystuje kable współosiowe. Na bazie tego okablowania tworzy się sieć podobną do Ethernetu. Firma Hybrid Networks z Kaliforni udostępnia taki serwis za 100 dolarów miesięcznie. W rozwiązaniu proponowanym przez tę firmę szybkość przesyłania 10 Mb/s uzyskuje się tylko dla jednego kierunku przesyłania informacji.
W Polsce trwają prace nad udostępnieniem takiego serwisu.

4.3.3. Dostęp poprzez łącza typu Ethernet

Wykorzystując technikę światłowodową można wykonać łącza typu ethernet o długości wielu kilometrów do dostawcy usług internetowych. Koszt takiego podłączenia jest bardzo duży, opłaty miesięczne także wysokie. Sposób praktycznie nie stosowany przez środowisko komercyjne.

5. Rejestracja użytkowników/abonentów komercyjnych w Polsce

Jak już wcześniej wspomniano użytkowników komercyjnych można podzielić na dwie klasy: na użytkowników biernych (bez adresu IP) i aktywnych (z adresem IP). Rejestracja pierwszej klasy użytkowników praktycznie nie jest możliwa, gdyż trudno uzyskać wiarygodne dane od wielu dostawców usług internetowych.
W drugiej klasie użytkowników/abonentów następuje automatyczna rejestracja komputerów w odpowiednich rekordach Serwerów Nazw Domenowych. Trudność polega tylko na wyodrębnieniu nazw domenowych użytkowników komercyjnych. Znając ilości komputerów abonentów można w przybliżeniu określić ilości użytkowników komercyjnych w sieci Internet.

6. Badania wykorzystania sieci Internet do działalności gospodarczej (komercyjnej)

Badania wykorzystania sieci Internet w działalności gospodarczej można prowadzić w dwóch płaszczyznach:

- pierwsza płaszczyzna to badania ilościowe takie jak: ilość komputerów, ilość użytkowników w sektorze komercyjnym w odniesieniu do wskaźników globalnych. Tą drogą można określić wskaźnik "usieciowienia" sektora gospodarczego,
- druga płaszczyzna to badania jakościowe takie jak: sposób dostępu do Internetu, rodzaj wykorzystywanych usług, efekty (korzyści) wymierne i niewymierne uzyskiwane z wykorzystania sieci Internet, przepustowość linii wykorzystywanych przez sektor gospodarczy.

Danych do pierwszej płaszczyzny badań mogą dostarczyć Serwery Nazw Domenowych. Danych do drugiej płaszczyzny mogą dostarczyć badania ankietowe wybranej, reprezentacyjnej grupy użytkowników komercyjnych. Badania powinny być prowadzone w dość długim okresie czasu, aby na podstawie uzyskanych wyników można było postawić prognozę rozwoju na następne lata. Wyniki badań mogą być wykorzystywane do podejmowania takich przedsięwzięć jak budowa linii przesyłania danych o dużej przepustowości, czy też budowa krajowej infrastruktury informatycznej.

7. Bezpieczeństwo usług internetowych

Firma komercyjna decydująca się na włączenie do sieci Internet powinna wziąć pod uwagę fakt, że sieć Internet charakteryzuje się niskim poziomem ochrony danych. Decydując się na wybór dostawcy usług należy przede wszystkim zwrócić uwagę na poziom bezpieczeństwa oferowanego przez dostawcę. Istnieje wiele rozwiązań sprzętowo-programowych znacznie zwiększających poziom ochrony danych takich jak: jednorazowe hasła, filtracja ruchu, twierdza, kodowanie danych itp. Przed wyborem dostawcy usług potrzebna jest świadomość, które środki będą nam potrzebne i czy dostawca usług je oferuje.

8. Perspektywy wykorzystania sieci Internet dla zastosowań komercyjnych w Polsce

Dokładne trendy wykorzystania sieci Internet do działalności gospodarczej będzie można określić po przeprowadzeniu badań. Ale już dzisiaj, zdaniem autora, można stwierdzić, że już w 1996 roku w Polsce rozpocznie sie gwałtowny rozwój Internetu. Ten gwałtowny rozwój zapewnią użytkownicy komercyjni. Na ten rozwój złoży się wiele czynników:

- po pierwsze - TPSA uruchamia sieć dostępową do Internetu. Dotychczas Internet był rozpowszechniany w dużych środowiskach akademickich i w najbliższym sąsiedztwie. W niedługim czasie wraz z telefonizacją kraju Internet trafi do gmin,
- po drugie - Miejskie Sieci Komputerowe (akademickie i TPSA) oraz sieć NASK jako sieci szkieletowe stworzą możliwości dostępu do Internetu wielu abonentom komercyjnym, a atrakcyjność i użyteczność usług spowoduje ich powszechność.

Literatura

1. Ed Krol: The Whole Internet User's Guide and Catalog
2. David Angell, Brent Heslop: The Internet Business Companion

SIECI SZEROKOPASMOWE JAKO PŁASZCZYZNA REALIZACJI USŁUG MULTIMEDIALNYCH

Krzysztof Amborski, Bogdan Dreszer

Telekomunikacja Polska S.A.
00-945 Warszawa, ul. Świętokrzyska 3

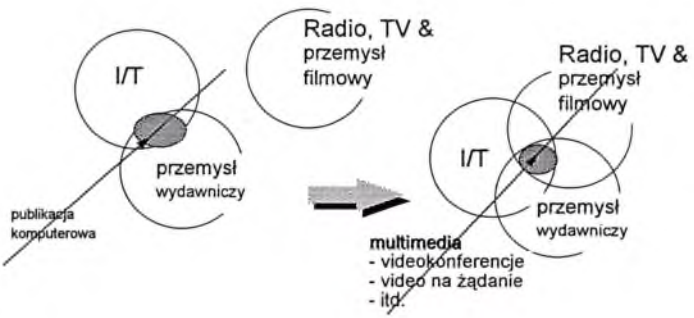
Wstęp

Realizacja usług multimedialnych jest obecnie coraz częściej omawianym zagadnieniem w aspekcie realizacji zarówno sieci pilotowych, jak i instalacji próbnych. Konkretyzują się akceptowalne komercyjnie rozwiązania techniczne w zakresie realizacji sieci dostępowych i zakresu świadczonych w początkowej fazie aplikacji usług. Panuje powszechne przekonanie, że podstawę realizacji aplikacji multimedialnych w sieciach rozległych będą stanowiły światłowodowe sieci szerokopasmowe z przesyłem sygnałów w technice ATM.

Definicja multimediów

Multimedia są uznawane za szansę rozwoju technologii w następnym stuleciu.
Zastosowania multimedialne to obszar związany z przedstawianiem, przechowywaniem, odzyskiwaniem i rozpowszechnianiem przetwarzalnych maszynowo informacji wyrażonej w wielu różnorodnych mediach takich jak tekst, głos, grafika, obraz, audio i wideo.
Powstanie komputerowych stacji roboczych, które łączą w sobie dużą moc i oszczędność, wraz z urządzeniami o wysokiej pojemności przechowywanych informacji i sieciami łączności cyfrowej o dużej szybkości przesyłu danych doprowadziło do tego, że świadczenie szerokiego zakresu usług multimedialnych jest obecnie nie tylko technicznie, ale także ekonomicznie możliwe.
W ogromnym tempie powstają nowe zastosowania multimedialne, takie jak:
- usługi wydawnicze na życzenie;
- usługi poligraficzne na życzenie;
- gazeta elektroniczna;
- telewizja responsywna;
- video na życzenie;
- videokonferencje;
- telewizja interaktywna.

Zastosowania te w nowej branży usług multimedialnych postrzegane są jako rezultat łączenia się trzech tradycyjnych sektorów i zmian związanych z integracją technologii komputerowej, telekomunikacyjnej i elektronicznej.

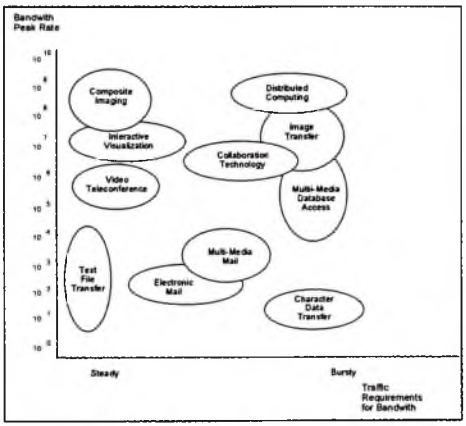


Rysunek 1: Multimedia jako wynik łączenia się trzech branż

Multimedia gwałtownie poszerzają zakres możliwości. Większość zastosowań multimedialnych nie występuje w pakietach czy systemach, lecz jest oferowana jako osobne, niezależne od siebie produkty. Multimedia wymuszają podwyższanie standardów istniejących już sieci do standardów sieci o dużej przepływności, które stanowić będą podstawę dla transmisji usług multimedialnych.
Dla określenia istoty multimediów stosuje się różne definicje i pojęcia. Niektórzy uważają multimedia za formę integracji telewizji z komputerami, inni uznają usługi interakcyjne szerokopasmowe tylko i wyłącznie za formę zarządzania pamięcią.
Multimedia definiuje się najczęściej jako zbiór co najmniej kilku z poniżej wymienionych istniejących już usług: radia, telewizji kablowej, usług interaktywnych, usług na życzenie (video, gier, muzyki) i łączności komputerowej.

Stan rynku usług multimedialnych

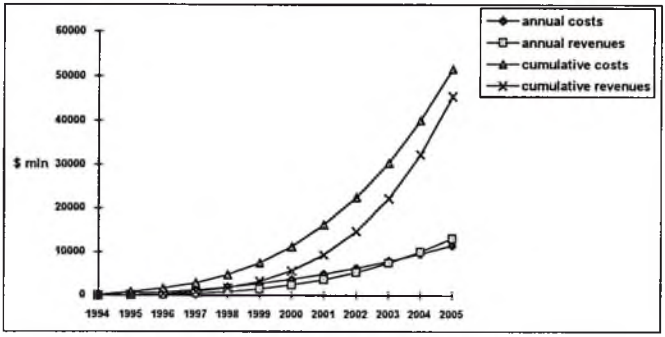
Obecnie rynek multimedialny rozwija się w coraz szybszym tempie. Równie szybko powstają nowe powiązania i nowe zastosowania. Coraz większa liczba firm działających na tradycyjnym rynku mass-mediów poszukuje sposobów wejścia na rynek multimediów.
Liczba firm działających na europejskim rynku usług multimedialnych wzrosła niemal trzykrotnie w okresie od 1991 do 1995 r. (źródło: "European Multimedia Yearbook"). Tempo tego wzrostu będzie z upływem czasu coraz większe. Według AT&T, wartość transakcji na rynku usług multimedialnych wyniesie w 1996 r. 12 mld USD, aby w roku 2000 wzrosnąć do poziomu 100 mld USD.
Wielkości te odnoszą się do rynku rozpatrywanego jako całość, włącznie ze wszystkimi operacjami związanymi z multimediami: produkcją oprogramowania i sprzętu, dostarczeniem treści programowej i telekomunikacją. Bliższa analiza wskazuje na potrzebę bilansowania wydatków na inwestycje z uzyskiwanymi dochodami. W szczególności operatorzy sieci telekomunikacyjnych i kablowych stoją przed koniecznością dokonania znacznych inwestycji związanych z podnoszeniem standardów sieci bez gwarancji szybkiego zwrotu z inwestycji.



Rysunek 2: Wymogi ruchowe dla szerokości pasma [1].

Jedyne na co mogą liczyć, to zyski w długim horyzoncie czasowym, kiedy to korzystanie z usług multimedialnych stanie się powszechne. Tymczasem napotykają na znaczne różnice w technice i zarządzaniu między nowymi usługami medialnymi i usługami telefonicznymi.
Usługi o charakterze interaktywnym i multimedialne powodują całkowicie inne wykorzystanie sieci: tworząc model ruchu o wysokiej "impulsowności" w porównaniu z innymi usługami.
Dla przykładu, zgodnie z prognozami Novum, przychody z amerykańskiego rynku kablowych usług interakcyjnych nie przekroczą ponoszonych kosztów do roku 2002, a z uwzględnieniem kosztów

skumulowanych - do roku 2004. Okres począwszy od pierwszych inwestycji do realizowania zysków będzie w przypadku projektów realizowanych w Europie jeszcze dłuższy (rys.3).



Rys.3. Koszty i przychody z działalności multimedialnej europejskich operatorów sieci kablowych [1].

Możliwe rozwiązania techniczne sieci dostępowej

Istnieje kilka alternatywnych rozwiązań technicznych, które można wykorzystać dla udostępnienia wizyjnych technik multimedialnych przesyłanych poprzez kabel współosiowy lub konwencjonalną siecią komutacyjną użytku publicznego (PSTN). Wybór możliwości zależy w dużym stopniu od punktu wyjściowego rozbudowy sieci. Tradycyjni operatorzy sieci telekomunikacyjnych są zainteresowani przede wszystkim wykorzystaniem istniejącej bazy przewodów miedzianych spoczywających już w ziemi i będą dawać pierwszeństwo rozwiązaniom, w których będą mogli wykorzystać istniejące instalacje, aniżeli budować całkowicie oddzielną sieć lub nadbudowywać istniejącą.
Wśród specjalistów zajmujących się tą dziedziną istnieje zgodność, iż nie istnieją żadne przeszkody natury technologicznej dla wprowadzenia interaktywnych usług multimedialnych. Wszystko zależy od ekonomii - a przede wszystkim od tego, czy będzie istniał wystarczająco duży popyt, aby umożliwić masową produkcję, która jest niezbędna dla obniżenia kosztów sprzętu i czy odbiorcy będą gotowi zapłacić cenę, która umożliwiłaby uzasadnione ekonomicznie świadczenie takich usług.
Sieć dostępu łączy serwer multimedialny lub łącznicę (centralę telefoniczną) z abonentem (np. przystawką, komputerem lub telefonem). Infrastruktura sieci wymaga dużych inwestycji ze strony operatora sieci dla jej udoskonalenia, rozszerzenia i transmisji usług multimedialnych.
Te inwestycje są często usprawiedliwione przez uzyskiwane oszczędności eksploatacyjne. Wymiana wielu przewodów o skręconych parach wiązek przez pojedynczą żyłę kabla światłowodowego umożliwia znaczne oszczędności dzięki zwiększeniu niezawodności i zmniejszeniu kosztów konserwacji.

Linia światłowodowa (FTTH)

Niektórzy operatorzy telewizji kablowej zainstalowali kable światłowodowe od punktu rozdzielczego do użytkownika (FTTH), obsługując kilka setek gospodarstw domowych dla poprawienia niezawodności systemu. Sieć o strukturze hierarchicznej (dendrycznej) oparta na kablu koncentrycznym jest stosowana do przenoszenia sygnału analogowego na krótsze odległości do abonentów. Kabel światłowodowy wykorzystuje ten sam wielonośnikowy wizyjny zakres częstotliwości, jaki jest używany przez telewizję kablową i dlatego nie jest wymagana złożona konwersja postaci sygnału dla wspólnego systemu kabel światłowodowy - kabel koncentryczny. System ten jest powszechnie stosowany w nowych sieciach i rozważa się go jako ważny alternatywny system dla stopniowego rozwoju istniejących sieci, gdzie główne przewody dystrybucyjne mogą zostać zastąpione przez kabel światłowodowy, ale pozostawi się

na miejscu istniejące kable koncentryczne, aby służyły jako przewody doprowadzające do odbiorców końcowych.

Struktura hybrydowa (HFC)

Nowe systemy telewizji kablowej o większej szerokości pasma lub te, w których udoskonalono zasadniczą część ich sieci przez zastosowanie kabla światłowodowego, mogą wykorzystać modulację analogową i cyfrową w różnych kanałach tego samego kabla. Technika multimedialna dla usług na żądanie może być przenoszona pomiędzy 450 a 860 MHz w modulowanych cyfrowo kanałach o szerokości 6 MHz.
Kanał analogowy 6 MHz może być modulowany dla przenoszenia do 30 Mbps lub maksymalnie piętnastu skompresowanych sygnałów 2 Mbps. Większość operatorów systemów telekomunikacyjnych uważa, iż sieci oparte na miedzianych kablach koncentrycznych są sposobem dla dostarczania usług multimedialnych, np. generatorów głosu do odbiorców domowych. Niektóre próby terenowe generatorów głosu, np. próba terenowa firmy Deutsche Telekom w Berlinie, opierają się na istniejącej sieci telewizyjnych kabli koncentrycznych, które zostały udoskonalone przez kable światłowodowe w magistralach. Użytkownicy przesyłają z powrotem sygnały sterujące, dotyczące na przykład zmiany programów, przy pomocy zwykłej telefonicznej sieci przewodów miedzianych.
Aby sieci telewizji kablowej mogły być odpowiednie dla przesyłania interaktywnych usług multimedialnych, konieczna jest łączność dwustronna oraz efektywne wykorzystanie sieci. Można to zrealizować przez wprowadzenie cyfrowego protokołu multipleksowego, takiego jak ATM (Asynchronous Transfer Mode) w połączeniu z wymienionym wcześniej udoskonaleniem sieci głównej przy pomocy kabla światłowodowego. W kierunku od sieci głównej do abonenta jest zalecane podłączenie punktów ponownej konwersji do głównej instalacji przy pomocy dwupunktowej struktury gwiaździstej.
Istnieją dwie główne możliwości dla instalacji central ATM:
a) pojedynczą centralę ATM można umieścić w głównej instalacji,
b) sprzęt ATM jest usytuowany w głównej instalacji, a także w punktach ponownej konwersji sieci telewizji kablowej (TVK).

Ponieważ sprzęt ATM w budynkach klienta może pracować przy niższych przepływnościach, wydaje się to być rozwiązaniem bardziej oszczędnym. W kierunku od abonenta do sieci głównej należy zarezerwować pasmo częstotliwości dla informacji od odbiorców do instalacji głównej. Realistyczne jest uzyskanie przepustowości u źródła równej 10-30 Mbps. Biorąc pod uwagę, że niemożliwe jest, aby około 1000 odbiorców dzieliło tę przepustowość źródłową - nawet przy użyciu nowoczesnych technik kodowania oraz najbardziej wydajnych i elastycznych technik multipleksowych - aby oferować każdemu odbiorcy oddzielny kanał o przepustowości 64 kbps. Zakłada się, że dostępna przepustowość źródłowa na odbiorcę będzie wystarczająca dla prostych informacji sterujących, np. obraz wizyjny na żądanie, ale zbyt ograniczona dla zastosowania głosu o szerokiej skali lub usług wizyjnych w dwie strony, jak w przypadku video-konferencji. Aby pokonać ograniczone zdolności instalacji centralnej obecnych sieci telewizji kablowej należy skorzystać z dwóch rozwiązań:
1) Zwiększyć analogową szerokość pasma dla kanału powrotnego w sieci telewizji kablowej do co najmniej 64 Mbps, co będzie związane z poważniejszymi inwestycjami, lub
2) porzucić ideę kanału zwrotnego poprzez sieć telewizji kablowej i zamiast tego skorzystać z sieci PSTN (sieć komutacyjna użytku publicznego) lub ISDN (sieć cyfrowa z integracją usług).

Asymetryczna cyfrowa linia abonencka (ADSL)

Technologia Cyfrowej Linii Abonenckiej (Digital Subscriber Line - DSL) uczyniła duże postępy od czasu, gdy została użyta w sieci cyfrowej z integracją usług o podstawowej szybkości ISDN na zainstalowanej sieci miedzianej. Cyfrowe systemy abonenckie o dużej przepustowości (HDSL) mogą zapewnić przepływności do 784 kbps pełnego dupleksu na skręconą parę wiązek, co w przypadku dwóch par daje przepustowość 1,5 Mbps w obrębie obszaru usług telefonicznych - maksymalnie na odległość od 2,7-do 3,6 km, zależnie od grubości drutu. Asymetryczna Cyfrowa Linia Abonencka (ADSL) może zapewnić swojej formie wstępnej - ADSL I - przepustowość równą 1,5 Mbps w jednym kierunku na pojedynczej parze skręconych wiązek, ponadto zapewniając kanał danych 16 kbps i

analogowe usługi telekomunikacyjne POTS. Późniejsza wersja - ADSL II - wykorzystuje dyskretną technologię wielotonową (DMT) dla zapewnienia przepustowości 6,4 Mbps plus pełno-dupleksowy kanał danych do 384 kbps, 16 kbps sterowania i telefonię analogową.
Odległości, które zapewnia ADSL II, stanowią tylko połowę oferowanych przez model ADSL I. Obydwa modele są atrakcyjne, ponieważ wykorzystują istniejące kable o skręconych parach wiązek, ale wiele osób uważa je jedynie za rozwiązanie tymczasowe. Jednakże w wielu przypadkach ADSL spełnia wymagania krótkoterminowe i w połączeniu ze światłowodami może stanowić sprawdzone rozwiązanie długoterminowe. Czas jego wykorzystania będzie zależał od szybkości instalacji światłowodu wzdłuż całej drogi do abonenta.
W Melbourne pod koniec ubiegłego roku, Australian Telstra rozpoczęła próby płatnej telewizji w technologii ADSL obejmującej 300 domów. Mimo, iż większość ogólnoświatowych prób obejmuje technologię ADSL, aby umożliwić dostarczanie sygnałów po kompresji cyfrowej poprzez istniejące sieci przewodów miedzianych, według opinii większości organizacji telekomunikacyjnych system ASDL jest kosztowny i stosunkowo niewypróbowany, a jakość istniejących sieci lokalnych jest niewystarczająca, aby umożliwić wykorzystanie tej technologii. Wielu operatorów wnioskuje, że stosowanie ADSL byłoby bardziej kosztowne (w przybliżeniu 1000 USD na użytkownika) i trudniejsze technicznie niż początkowo przypuszczali.
Firma AT&T Paradyne zapowiedziała powstanie GlobeSpan, nowej technologii transmisji, która według niej umożliwi użytkownikom prowadzenie rozmowy telefonicznej, wykorzystując równocześnie ten sam miedziany przewód telefoniczny do oglądania wydarzeń "na żywo" na ekranie telewizora, zdalnie ładując zbiory multimedialne wysoko-zdefiniowane z sieci Internet do mikrokomputera, lub na żądanie odbierając obraz filmowy. System GlobeSpan opracowany wspólnie przez AT&T Paradyne i AT&T Bell Laboratories, jest technologią transmisji, która wykorzystuje techniki kodowania linii CAP (Carrierless Amplitude and Phase modulation) dla współbieżnej transmisji zarówno standardowych analogowych sygnałów głosowych, jak i szybkich sygnałów cyfrowych na miedzianym przewodzie linii telefonicznej. Według opinii firmy, technologia ta umożliwi czterokrotne zwiększenie szybkości istniejących sieci telefonicznych z przewodami miedzianymi z 1,544 Mbps do ponad 6 Mbps - szybkości niezbędnej dla przesyłu obrazu na żywo oraz dostępu do szybkich Lokalnych Sieci Komputerowych (LAN).
Obecnie uważa się, że ADSL jest tylko rozwiązaniem krótkoterminowym i nie jest prawdopodobne, aby jego zastosowanie stało się powszechne. Jeżeli jednak pojawi się ogromny wzrost zainteresowania usługami multimedialnymi, istnieje większe prawdopodobieństwo zastosowania hybrydowego rozwiązania kabel światłowodowy/ADSL, które wykorzystuje istniejącą infrastrukturę.

Pasywne sieci optyczne (PON)

Gdy kabel światłowodowy jest prowadzony do domu odbiorcy, całą pracę przełączania komunikatów dla różnych abonentów można wykonać na centrali telefonicznej. Światłowód jest ostatecznym urządzeniem przesyłowym dla domowych usług szerokopasmowych i ostatnio stał się skuteczną i ekonomiczną metodą dalekosiężnych połączeń dla węzłów sieci małych społeczności. Pasywne Sieci Optyczne (PON) testowane były w Wielkiej Brytanii przez firmę British Telecom i stosowane na dużą skalę we wschodniej części Niemiec. Jednakże związane z nimi koszty, standardy i bariery techniczne uniemożliwiają powszechne wprowadzenie kabli światłowodowych do domów abonentów.

Hybrydowe połączenie sieci światłowodowej i sieci bezprzewodowej

Postęp technologii fali milimetrowej wraz z dostępnością częstotliwości przy tych długościach fali umożliwiają opracowanie hybrydowego połączenia sieci światłowodowych i dystrybucji bezprzewodowej. Takie rozwiązanie byłoby pożądane w obszarach bez żadnych przewodów miedzianych lub tam, gdzie istniejąca instalacja znajduje się w złym stanie lub tam, gdzie fizyczny dostęp dla okablowania pomiędzy lokalnym punktem rozdzielczym a budynkami użytkownika jest ograniczony lub kosztowny - tak jak w przypadku, gdy dostawca usług posiada infrastrukturę światłowodową, ale brak mu przewodów miedzianych prowadzących do użytkownika.
Próby obejmują wielokanałową, wielopunktową dystrybucję wizyjną fali milimetrowej -prowadzoną przez firmę British Telecom przy 29 GHz lub ofertę handlową firmy Cellular Vision na obszarze Nowego Jorku pod licencją pionierską US FCC w paśmie częstotliwości 27,5 do 29,5 GHz.
W przeciwieństwie do hybrydowego połączenia sieci kabli światłowodowych i koncentrycznych, nie ma obecnie sposobu utrzymania struktury sygnału przy przejściu z kabli światłowodowych na system bezprzewodowy. Zarówno system stosowany przez BT jak i przez Cellular Vision wykorzystują szerokopasmową modulację częstotliwości dla radiowo-telewizyjnej transmisji kanałowej. Żadna z nich nie zapewnia bezprzewodowego kanału powrotnego (mimo, iż firma Cellular Vision to planuje). Nie jest jasne, czy wymagane asymetryczne działanie dupleksowe będzie bardziej oszczędne w porównaniu z innymi rozwiązaniami, z wyjątkiem przypadków szczególnie trudnego dostępu i wysokich kosztów okablowania.

Szacunkowe koszty rozwiązań sieci dostępowej

Poniższa tabela podaje przegląd istniejących technologii, ich główne cechy charakterystyczne i zakres cen dla łączy abonenckich z roku 1995.

Architektura sieci	Opis	Koszt na jedno łącze
Fiber to the home (FTTH) - kabel światłowodowy od punktu rozdzielczego do użytkownika	· kabel światłowodowy do urządzeń końcowych · optymalne rozwiązanie pod kątem technologicznym, ale również najbardziej kosztowne · wysokie koszta związane z układaniem kabla i urządzeniami końcowymi	DM 5.000 do DM 8.000
Fiber to the curb (FTTC) kabel światłowodowy między centralą a punktem rozdzielczym	· kabel światłowodowy do skrzynki rozdzielczej · kabel koncentryczny pomiędzy skrzynką rozdzielczą a urządzeniami końcowymi odbiorcy; niezbędne częściowo nowe kable koncentryczne · brak wad przepustowości w porównaniu z rozwiązaniem FTTH · preferowane, gdy gęstość rozmieszczenia gospodarstw domowych jest mniejsza niż 50 na km2	DM 2.500 do DM 5.000

struktura hybrydowa HFC (kabel światłowodowy/kabel koncentryczny)	· wykorzystuje istniejącą infrastrukturę kabli koncentrycznych · analogowe kanały bazowe z kanałem głównym i kanałami dodatkowymi dla generacji głosowej skompresowanej dla adresowanych przystawek · preferowane, gdy gęstość rozmieszczenia gospodarstw domowych jest większa niż 50 na kilometr	DM 600 do DM 1.500
Asymmetrical Digital Subscriber Line (ADSL) Asymetryczna Cyfrowa Linia Abonencka	· obszerne prace badawczo-rozwojowe dla stałej poprawy szerokości pasma; · obecnie przepustowość dla * 4 skompresowane kanały wizyjne, 1.5 Mbps * 1 kanał B-ISDN (384 Kbps) * 1 kanał ISDN (16 - 44 Kbps) · ograniczone inwestycje, gdy może być stosowana istniejąca infrastruktura miedziana; tanie rozwiązania dla celów tymczasowych lub długoterminowych	DM 1.000 do DM 2.000
High Bit Rate Digital Subscriber Line (HDSL) Cyfrowy System Abonencki o Dużej Przepływności	· HDSL umożliwia połączenie w obu kierunkach, obecnie do 2Mbps na odległość do 4 kilometrów pomiędzy skrzynką rozdzielczą a urządzeniami końcowymi odbiorcy	DM 2.000 do DM 3.000
Instalacja kanału zwrotnego w sieci telewizji kablowej	· wykorzystanie dodatkowego zakresu częstotliwości dla łączności w obie strony szerokość pasma do kilku Mbps · możliwe połączenie z usługami POTS	brak danych
instalacja kanału zwrotnego w sieciach satelitarnych przy wykorzystaniu istniejącej infrastruktury POTS	· mają być instalowane tylko w domach użytkownika · szerokość pasma ograniczona przez użycie telefonu · pierwszy system jest sprzedawany w USA (DirecTV produkowana przez Hughes Aircraft) · na razie w niewielkim stopniu akceptowane przez klientów, ponieważ system trudny w obsłudze	poniżej DM 1.000

Wireless Local Loop (WLL) / Radio in the local loop (RITL) Bezprzewodowa (Radiowa) Instalacja Lokalny/ Radio w Instalacji Lokalnej	- zalety opcji bezprzewodowej: bardzo szybka rozbudowa - stosunkowo niskie koszty (w porównaniu z FTTH) - preferowany przy małej penetracji rynku lub małym zagęszczeniu gospodarstw domowych - różne technologie i standardy; prawdopodobnym zwycięzcą jest Digital European Cordless Telecommunications (DECT) - nie wszystkie technologie pracują w każdym środowisku (fizyczne ograniczenie technologii nośników informacji) - jak dotąd, za mała szerokość pasma dla zastosowań telewizji interaktywnej	brak danych

Dotychczasowe instalacje doświadczalne.

Firma konsultingowa Screen Digest doliczyła się na całym świecie ponad 90 planowanych różnego rodzaju przedsięwzięć w zakresie kablowych sieci interaktywnych, w których realizacji uczestniczy 52 różnych operatorów. Ponad połowa tych projektów ma być realizowana w USA, 18 w Europie, 9 w Japonii i 7 w Australii Azji. Ostateczne plany wprowadzenia na rynek usług interakcyjnych na zasadach komercyjnych potwierdziło 11 firm, z czego 7 to operatorzy sieci telefonicznych ze Stanów Zjednoczonych. Celem multimedialnych projektów próbnych jest podłączenie sieci oferujących usługi interakcyjne zarówno do gospodarstw domowych, jak i użytkowników biznesowych. Wśród oferowanych usług znajdują się: video na życzenie, domowe zakupy i operacje bankowe, gry, video-telefon, kształcenie interaktywne, usługi medyczne na odległość, informacje o lokalnej społeczności, bazy danych i muzyka na życzenie. Zgodnie z publicznymi wypowiedziami uczestników tych projektów, obecne działania mają za zadanie zbadanie popytu użytkowników końcowych na różnego rodzaju usługi interaktywne oferowane na zasadach komercyjnych. Zmiany w technologii pozwalają na pełne wykorzystanie szerokiej bazy twórczej i ogromnej wartości rynkowej posiadanych praw autorskich. To prawdopodobnie jest jednym z głównych powodów, dla których dostawcy informacji odgrywają dominującą rolę w próbnych projektach multimedialnych: zdobywają dzięki nim informacje dotyczące stopnia akceptacji usług mutlimedialnych. Operatorzy sieci telefonicznych uczestniczący w próbnych projektach koncentrują się na testowaniu różnych technologii. W roku 1993 r. firma Bell Atlantic przeprowadziła na próbie 300 gospodarstw domowych ze stanu Północna Virginia (USA) test techniczny w zakresie techniki video-telefonicznej (zwanej VDT od ang. Video Dial Tone). Dla przeprowadzenia tego testu firma Bell Atlantic wykorzystała technologię transmisji ADSL w ramach konwencjonalnych parowych linii telefonicznych. Cel projektu próbnego był dwojaki: z jednej strony chodziło o zbadanie popytu użytkownika końcowego na różnego rodzaju usługi interaktywne, a z drugiej strony o ocenę popytu innych dostawców informacji videofonicznych na sieć opracowaną przez Bell Atlantic. Wprawdzie firma Bell Atlantic rozpoczęła swoje badania w dziedzinie usług multimedialnych od technologii ADSL, to jednocześnie była zainteresowana rozwijaniem i zdobyciem doświadczeń w zakresie dwóch innych systemów sieciowych: HFC i FTTC. Z tego też względu firma Bell Atlantic rozpoczęła kolejny projekt próbny wraz z firmami Broadband Technologies i Philips.
"Ovum" wyróżnia cztery, czasami zachodzące na siebie, fazy opracowywania nowych usług interakcyjnych. Obecne działania w tej mierze przebiegają zgodnie z następującymi stadiami:
1. Pierwsza faza obejmuje "test techniczny", który zazwyczaj polega na dotarciu z nowymi usługami do 50 - 100 gospodarstw domowych. Głównym celem tego testu jest zademonstrowanie różnego rodzaju urządzeń technicznych z powodzeniem ze sobą współpracujących oraz zaznajomienie się z

ograniczeniami (pojemność, funkcjonalność) systemu. Wiele z tych projektów próbnych było wielokrotnie odkładanych w czasie, czego powodem były niedojrzałe jeszcze technologie i brak odpowiedniego wsparcia finansowego.
2. Kolejną fazę stanowią próbne projekty rynkowe, które mogą objąć swoim zasięgiem od 200 do 10.000 gospodarstw domowych. W trakcie tych projektów głównym obszarem zainteresowanie przestaje być technika a stają się nim usługi interaktywne. Zasadniczym celem tej fazy jest zbadanie, jakiego rodzaju usługi najbardziej zainteresują klienta i za jaką cenę.
3. W trzeciej fazie usługi świadczone są na zasadach komercyjnych. Nadawcy oferują szereg usług drogą kablową lub telefoniczną, przyjmując za podstawę transmisji urządzenia ATM i już zainstalowaną sieć światłowodową "do klienta".
4. Po zakończeniu powyższych testów i projektów próbnych, rozpoczyna się komercyjna działalność w zakresie usług interaktywnych. Za pośrednictwem powszechnie dostępnych "pełnoobsługowych" sieci, klienci mogą porozumiewać się na dużą odległość i dokonywać wyboru spośród dużego wachlarza usług.

USA
Większość działań jest prowadzona w ramach intensywnych programów podwyższania standardów i przebudowy realizowanych przez duże amerykańskie grupy sektora telekomunikacyjnego.
Rodzaje oferowanych usług i planowanych do zastosowania technologii, a także ich wyniki są utrzymywane w tajemnicy. W szczególności terminy rozpoczęcia projektów próbnych lub wdrożeniowych podlegają znacznym przesunięciom. Długi proces podejmowania decyzji przez Federalną Komisję Łączności jest czynnikiem znacznie spowalniającym realizację planów.
W przypadku wielu projektów amerykańskich ograniczono ich skalę z próbnych projektów rynkowych do testów technicznych. Szczególnie trudne we wdrożeniu okazały się plany przebadania cyfrowych urządzeń dekodujących.

Orlando, Floryda
Time Warner i US West dopiero od niedawna uruchomiły pełnoobsługową sieć multimedialną w Orlando na Florydzie. Do końca 1994 r. podłączonych zostało do niej jedynie pięć gospodarstw domowych. Wśród usług oferowanych w sieci znajdują się: filmy na życzenie, domowe zakupy, interaktywne gry video, video-konferencje i wiadomości na życzenie (wiadomości w wybranym zakresie z możliwością otrzymania wydruku). Time Warner i US West wykorzystują do swojego projektu hybrydową sieć światłowodowo-koncentryczną z centralami ATM. Dostawcą zestawów urządzeń dekodujących, z których każdy kosztuje obecnie 5.000 USD, jest firma Scientific Atlanta. Projekt otwarty jest również na nowych dostawców usług i kanałów. W roku 1994, kiedy rozpoczęto projekt próbny, dostępnych było jedynie kilka zastosowań.. W marcu 1995 r. do sieci pełno-obsługowej podłączono 50 gospodarstw domowych, a obecnie jest podłączonych łącznie 4.000 gospodarstw.

Denver, Colorado
W lipcu 1994 r. AT&T, US West i TCI zakończyły dwuletni projekt próbny z dziedziny usług video na życzenie, realizowany na próbie 300 gospodarstw domowych w Denver, Colorado. Usługi były oferowane za pośrednictwem kablowej sieci koncentrycznej z odpowiednio zmodyfikowanymi liniami telefonicznymi i urządzeniami dekodującymi, które umożliwiały użytkownikom wypożyczanie interesujących ich filmów na życzenie z biblioteki liczącej 1.500 pozycji. Rolę serwera spełniał magnetowid. W trakcie projektu, odbiorcy reprezentujący przeciętne gospodarstwo domowe obejrzeli 2.5 filmu miesięcznie, co można uznać za sukces, w porównaniu z przeciętną 2.6 filmu rocznie przypadającą na jedno amerykańskie gospodarstwo domowe posiadające dostęp do standardowych kablowych usług płatnych za pokaz.Castro Valley, Kalifornia
W połowie 1994 r. Viacom i AT&T rozpoczęły próbny projekt telewizji interaktywnej z usługami typu VOD, traktując go jako pośredni krok w kierunku bardziej zaawansowanych usług telewizji interaktywnej. Do hybrydowej sieci światłowodowo-koncentrycznej podłączonych jest obecnie 13.000 gospodarstw domowych w rejonie Castro Valley w Kalifornii. Dostawcą serwera, oprogramowania operacyjnego i urządzeń dekodujących była firma AT&T.

- Północna Virginia:
Serię próbnych projektów związanych z usługami interakcyjnymi rozpocznie Bell Atlantic. W poszczególne projekty zaangażowani są różni dostawcy serwerów, systemu operacyjnego i urządzeń dekodujących.

- Seattle:
Począwszy od kwietnia 1994 r. na ograniczonej ilości abonentów w Seattle firma TCI bada popyt na usługi zbliżone do usług video na życzenie. TCI poszukuje zyskownych zestawów łączących szereg skompresowanych kanałów. Wśród oferowanych usług znajdują się filmy płatne za pokaz i przekazy telewizyjne na życzenie. W projekcie wykorzystano hybrydową sieć światłowodowo-koncentryczną a oprogramowanie operacyjne dostarczone jest przez Microsoft.

- Chicago, Detroit, Columbus, Milwaukee i Indianapolis:
Ameritech ma zamiar rozpocząć nadawanie komercyjnej telewizji interaktywnej zaraz po otrzymaniu zgody od Federalnej Komisji Łączności. W zamierzeniach firmy jest podłączenie do sieci ok. 6 mln abonentów do roku 2000. Zastosowane technologie pochodzą:
w zakresie serwera - od DEC (Digital Equipment Corporation) i IBM,
w zakresie oprogramowania operacyjnego - od IBM, ADC Telecoms i Microware,
w zakresie urządzeń dekodujących - od Scientific Atlanta.

Europa

Paryż, Francja
W lutym 1995 r. rozpoczął się w Paryżu projekt próbny o ograniczonym zakresie, oferujący gry na życzenie dla 500 gospodarstw domowych. Zgodnie z zapewnieniami France Telecom, Lyonnaise Communications i Sony Electronic Publishing, sieć na zasadach komercyjnych rozpocznie działalność na wiosnę. W ramach projektu, zamiast grać w czasie rzeczywistym (tzw. "on-line"), abonenci muszą załadować najpierw oprogramowanie gry do pamięci komputera. Komputer osobisty połączony jest z systemem kablowym za pośrednictwem przystosowanego dekodera umożliwiającego dostęp do wizji. Fakt, że 40 procent gospodarstw domowych w Paryżu jest podłączonych do kabla i posiada jednocześnie komputery osobiste, stanowi o wysokim potencjale tego rynku. Abonament w tym systemie kosztuje 90 Ffr (16.80 USD).

Kesgrave, Anglia
British Telecom wraz z nCube, Apple i Oracle przeprowadzili test techniczny na próbie 60 gospodarstw domowych w Kesgrave w Anglii. Celem testu, który trwał od kwietnia do września 1994 roku, było przebadanie technologii asymetrycznej cyfrowej linii abonenckiej ADSL w kontekście możliwości jej wykorzystania do celów dystrybucji kaset video za pośrednictwem konwencjonalnych linii telefonicznych. Uzyskano bardzo dobre wyniki. Obszar, na którym wykorzystano technologię ADSL, charakteryzował się 92% penetracją sieci i miał dużą odporność na problemy związane z trzaskami na linii i problemy okablowania. Wykorzystano sygnały typu MPEG-1 o przepływności 2 Mbps.
Zasięg systemu ADSL określono na 6 km. Serwer multimedialny pochodził od nCube, oprogramowanie bazy danych - od Oracle a urządzenia dekodujące - od Apple.

Cholchester, Anglia
BT rozpoczął w połowie 1995 r. projekt próbny w zakresie usług video na życzenie obejmujący swym zasięgiem 2.500 gospodarstw domowych w brytyjskich miastach Cholchester i Ipswich. Widzowie będą mieli do wyboru 600 godzin programów telewizyjnych, 400 godzin filmów i 200 godzin programów muzycznych. Ponadto ma być oferowanych ok. 350 godzin programów edukacyjnych, a National Westminster ma oferować domowe usługi bankowe. W ramach istniejącej infrastruktury w ok. 80% połączeń jest stosowany system ADSL (produkcji Westell), a w pozostałej części przewody światłowodowe. Dla potrzeb projektu zostaną wykorzystane przełączniki ATM.

Berlin, Niemcy
Deutsche Bundespost Telekom planuje przeprowadzić w 1996 r. projekt próbny w zakresie telewizji interaktywnej, obejmując nim 6.250 niemieckich gospodarstw domowych. Wstępny projekt rozpoczął się w Berlinie w lutym 1995 r. na próbie 50 gospodarstw. W końcu 1995 r. rozpoczęto szereg dalszych oddzielnych projektów:

Hamburg, Niemcy
Projekt próbny dla 1.000 gospodarstw domowych, w których podwyższono standard sieci kablowych do poziomu umożliwiającego przesyłanie danych cyfrowych. Widzowie komunikować się będą z dostawcami programów za pośrednictwem istniejących linii telefonicznych (aby poprosić o wybrane programy/usługi i użyć funkcji stop/start/stopklatka), podczas gdy programy i usługi dostarczane są za pośrednictwem kabla koncentrycznego.

Köln i Bonn, Niemcy
Usługi dostarczane będą za pośrednictwem kabla o podwyższonym (HFC), pozwalającego na ruch dwukierunkowy.

Nürnberg, Niemcy
DT rozpocznie oferowanie pełnej obsługi w zakresie video na życzenie dla 1000 gospodarstw domowych za pośrednictwem normalnej miedziowej linii telefonicznej. Niektóre gospodarstwa korzystać będą z połączonych linii kablowo-telefonicznych, podobnie jak w przypadku Hamburga.

Stuttgart, Niemcy
W Stuttgarcie rozpocznie się projekt próbny obejmujący 4.000 gospodarstw domowych, w ramach którego w całości wykorzystywany będzie kabel o podwyższonym standardzie (HFC).

Leipzig, Niemcy
Pod koniec 1995 r. w 100 gospodarstwach domowych w Lipsku rozpocznie się projekt próbny w zakresie usług interaktywnych dostarczanych do każdego domu za pośrednictwem światłowodu.

Holandia
Od lipca 1994 r. rozpoczął się z inicjatywy SURFnet i holenderskiego operatora telekomunikacyjnego test pilotażowy w ramach sieci Internet i przy wykorzystaniu szerokopasmowej transmisji 34 Mbps w sieci ATM. SurfNet dostarcza usługi sieci Internet holenderskim uniwersytetom, instytutom badawczo-rozwojowym i szpitalom akademickim i sygnalizuje wzrastający popyt na usługi szerokopasmowe: szpitale chcą wymienić skanery na trójwymiarowe i oferować specjalistom możliwość telewizyjnego podglądu operacji chirurgicznych; badacze chcą uzyskać znaczną ilość informacji naukowych z instytutu CERN w Szwajcarii; ośrodki projektów graficznych chcą wymieniać między sobą obrazy o wysokiej rozdzielczości, itp.
Wdrożenie projektu na zasadach komercyjnych jest planowane na rok 1996.

Wnioski

Odnotowane projekty próbne znajdują się w różnych stadiach realizacji. Niektóre z nich są wstrzymane, inne z różnych powodów odwołane i zastąpione nowymi testami. Wyniki testów są w większości przypadków utrzymywane w tajemnicy i znane wyłącznie uczestniczącym w projektach firmom. Żadna firma nie oczekuje jednak osiągnięcia sukcesu komercyjnego od samego początku. Główne powody, dla których prowadzone są projekty próbne, to zbadanie nowych technologii i uzyskanie doświadczeń w zakresie możliwości rynkowych związanych z wprowadzeniem zastosowań multimedialnych.
Większość uczestników projektów pilotażowych dysponuje różnego rodzaju doświadczeniem technicznym (dostawcy sieci i jej wyposażenia oraz dostawcy wyposażenia dla użytkownika końcowego). Powodem uczestnictwa czy inicjowania projektów próbnych jest zainteresowanie zarówno możliwościami rynkowymi jak i postępem technologicznym. Dla firm takich jak Oracle, Micosoft, AT&T, Apple i Videotron projekty próbne stanowią istotną szansę przetestowania opracowanych przez

nie aplikacji, usług, wyposażenia lub sieci. Tym należy również tłumaczyć wysoki stopień poufności informacji wspólny dla wszystkich testów i projektów pilotażowych.

Podsumowanie

Sieci szerokopasmowe i świadczone poprzez nie usługi multimedialne stanowią przyszłościowy kierunek rozwoju telekomunikacji - zarówno w sektorze biznesowym, jak i prywatnym.
Środowisko sieci ATM wydaje się być obecnie najodpowiedniejszym medium telekomunikacyjnym, jednak do tej pory brak jednoznacznych ustaleń definiujących przesyłanie informacji w tej sieci - standaryzacja nie jest zakończona. Drugim problemem jest określenie najlepszego wyboru - technicznie i ekonomicznie - sieci dostępowej stosowanej do przesyłu sygnałów szerokopasmowych o wysokiej przepływności niezbędnej dla zapewnienia pełnej gamy usług multimedialnych. Sieć ta bowiem ma decydujące znaczenie w określeniu kosztów całego przedsięwzięcia.

Źródła:

[1] Wstępna analiza techniczno-ekonomiczna celowości projektu multimedia TP S.A. - opracowanie KPMG, wrzesień 1995
[2] Wstępne Studium Możliwości Projektu Multimedia - BTN - TPSA, grudzień 1995
[3] Audio-visual Multimedia Service Implementation Agreement, ATM Forum, 95-0012R1

W3CACHE

Wojciech Sylwestrzak

Interdyscyplinarne Centrum Modelowania, Banacha 2, 02-097 Warszawa

1 Serwer cache WWW

Cache jest nazwą używaną do określenia jednostki pośredniej między klientem a serwerem, której zadaniem jest buforowanie danych. W przypadku WWW na serwer cache wygodnie jest często patrzeć jak na serwer proxy z lokalnym dyskiem, pełniącym rolę cache. Najczęstszym powodem użycia cache'a jest szybkość dostępu - oczekuje się, że czas odpowiedzi cache'a będzie krótszy niż miałoby to miejsce w przypadku bezpośredniego użycia serwera. Niestety przestrzeń w której cache gromadzi dane jest ograniczona i nierzadko bardzo kosztowna. Dlatego zasadniczym problemem napotykanym przy użyciu cache'a jest określenie jakie dane i jak długo należy w nim przechowywać.

Bez mechanizmu cache, WWW padłoby ofiarą własnej popularności. Wraz z rozwojem usług WWW rośnie liczba klientów pobierających jednocześnie te same dokumenty, a co za tym idzie, rośnie zużycie pasma na łączach między klientami a serwerami. Konsekwencją tego jest coraz większe obciążenie serwerów oraz przede wszystkim sieci i w efekcie coraz gorsza jakość połączeń.

Niezbędnym rozwiązaniem jest oczywiście stopniowe zwiększanie przepustowości sieci oraz mocy serwerów WWW. W świetle gwałtownego wzrostu ruchu WWW okazuje się jednak ono bardzo kosztowne, a w praktyce, głównie ze względów finansowych, niemożliwe do zrealizowania w sposób pozwalający zaspokoić szybko rosnące potrzeby.

Rozwiązaniem pozwalającym zmniejszyć negatywne skutki wzrostu popularności WWW jest użycie serwerów cache. Pozwala ono przenieść kopie najczęściej żądanych obiektów znacznie bliżej populacji klientów, w wyniku czego są one łatwiej dostępne, a łącza sieciowe wykorzystywane są efektywniej. Pozytywnym skutkiem ubocznym zastosowania serwerów cache jest mniejsze obciążenie serwerów źrodłowych oraz krótszy czas oczekiwania na dokument.

Jak się okazuje, wykorzystanie serwerów WWW cache też ma wyraźne uzasadnienie ekonomiczne i temu przypuszczalnie należy przypisać gwałtowny rozwój światowej hierarchii cache w roku 1996. Inwestycja w szybki serwer WWW cache oraz dedykowane łącze do niego okazuje się często być znacznie tańsza niż ciągłe zwiększanie przepustowości sieci.

Serwer WWW cache jest to serwer HTTP, który odpowiada na żądania klientów odsyłając im dokumenty z lokalnego bufora lub pobierając je z serwerów

źródłowych. W tym ostatnim przypadku serwer WWW cache pełni rolę zwykłego serwera proxy, pośredniczącego w komunikacji między klientem, a serwerem źródłowym.

2 Światowa hierarchia serwerów cache

Najpopularniejszym obecnie na serwerach WWW cache oprogramowaniem jest *cached 1.4*, program pochodzący z projektu Harvest. Po zakończeniu projektu Harvest prace nad rozwojem oprogramowania prowadzone są w dwu niezależnych zespołach, tworzących publicznie dostępną wersję *Squid 1.0* oraz komercyjną *cached 2.0*. Obydwa produkty w pierwszej połowie maja opuściły wersję testów beta. Należy przypuszczać, ze tworzony w ramach konsorcjum NLANR *Squid* będzie następcą *cached 1.4*.

Inną, komercyjną implementacją jest cache server firmy Netscape. Mimo, iż zawiera on elementy pozwalające na tworzenie struktur hierarchicznych, nie zostały one dotąd zaimplementowane wystarczająco efektywnie.

Wreszcie jako serwerów cache używać można także na małą skalę zwykłych serwerów WWW pracujących w trybie proxy takich jak Apache 1.1[1], CERN 3.0[2] czy Spinner[3]. Również one nie są jednak zaprojektowane do pracy w dużych strukturach hierarchicznych.

Oprócz wymienionych istnieją także implementacje o charakterze bardziej eksperymentalnym, takie jak Lagoon[4] czy Ichtus[5].

Jedną z zalet serwerów cache wywodzących się z projektu Harvest jest fakt, że zostały one zaprojektowane z myślą o pracy w hierarchii, w ramach której przekazują sobie wzajemnie obiekty, tym samym dodatkowo wpływając na zmniejszenie obciążenia łącz oraz zmniejszając przeciętny czas dostępu do informacji. Przy konfiguracji serwera określa się, które inne serwery traktowane mają być jako jego *sąsiedzi* lub *rodzice*. W obecnej wersji oprogramowania wybór *rodzica* lub *sąsiada*, od którego ściągany będzie obiekt dokonywany jest na podstawie RTT (czasu powrotu) dla pakietu QUERY protokołu ICP (Internet Cache Protocol). Pakiet taki, zawierający informację o żądanym URL wysyłany jest do odpowiednich *rodziców*, *sąsiadów* i ewentualnie do źródłowego serwera WWW. Przyszłe wersje oprogramowania przy wyborze sąsiada przypuszczalnie będą także uwzględniać parametry takie, jak chwilowa przepustowość drogi między serwerami cache czy "koszt" danego odcinka. W uproszczeniu, odpowiedzią na

[1] http://sunsite.icm.edu.pl/pub/www/apache/docs/1.1/
[2] http://www.w3.org/hypertext/WWW/Daemon/User/Config/Caching.html
[3] http://sunsite.icm.edu.pl/pub/www/spinner/
[4] http://www.win.tue.nl/lagoon/
[5] http://www.gh.cs.su.oz.au/Cache/

pakiet ICP wysłany do *rodzica* lub *sąsiada* jest komunikat HIT, jeśli obiekt znajduje się w jego lokalnym cache'u i MISS jeśli go nie ma. Po wysłaniu pakietów ICP serwer czeka na:

- Pierwszą odpowiedź HIT. Wtedy natychmiast obiekt pobierany jest z serwera (*rodzica* lub *sąsiada*), który nadesłał tę odpowiedź.
- Jeśli w określonym czasie nadeszły tylko odpowiedzi MISS, serwer ściąga obiekt poprzez rodzica, który najszybciej odpowiedział. W tym wypadku serwer źródłowy traktowany jest na równi z rodzicem.
- Jeśli w określonym czasie nie nadeszła żadna odpowiedź (lub tylko odpowiedzi MISS pochodzące od sąsiadów), serwer próbuje ściągnąć obiekt bezpośrednio ze źródła.

  Obiekt może być także ściągnięty bezpośrednio ze źródła, jeśli:

  - konfiguracja serwera cache nie dopuszcza cache'owania obiektu tego typu.
  - nazwa domenowa serwera WWW, występująca w URL obiektu wskazuje, że serwer źródłowy znajduje się w pobliżu (w sensie topologii sieci) serwera cache (na przykład w tej samej domenie).
  - dla danego URL konfiguracja cache serwera nie specyfikuje żadnego rodzica ani sąsiada.
  - serwer źródłowy odpowie szybciej na pakiet ICP niż którykolwiek z rodziców lub sąsiadów. W praktyce zdarza się to bardzo rzadko.

Tak więc jedyna różnica między *rodzicem* i *sąsiadem* polega na tym, że sąsiad zwraca obiekt tylko jeśli posiada go w swoim cache'u.

Opisany wyżej algorytm gwarantuje, że obiekt będzie ściągany ze źródła w przypadku gdy nie ma komunikacji z rodzicem oraz od najszybszego rodzica (lub sąsiada posiadającego obiekt w cache'u) w przeciwnym przypadku.

Znaczenie hierarchicznych struktur serwerów cache zostało bardzo szybko dostrzeżone zarówno przez twórców oprogramowania jak i autorów specyfikacji protokołu HTTP 1.1. Nowe wersje przeglądarek Netscape (2.0 i 3.0) posiadają już możliwość automatycznego wyboru najbliższego w hierarchii serwera cache, zaś w propozycji specyfikacji HTTP 1.1 znalazło się między innymi wiele nowych rozdziałów poświęconych właśnie zaawansowanym sposobom komunikacji między klientami, serwerami źródłowymi, a serwerami WWW cache.

Szybki rozwój hierarchii WWW cache rozpoczął się pod koniec roku 1995, odkąd dostępne zaczęło być wystarczająco stabilne oprogramowanie. Obecnie

prawie wszystkie serwery cache w hierarchii używają oprogramowania pochodzącego z amerykańskiego projektu Harvest (cached 1.4) lub jego pochodnych (wspominane wcześniej cached 2.0 i Squid 1.0). Pierwotna wersja tzw. Harvest cache powstała przy amerykańskim narodowym metacentrum (skupiającym główne naukowe centra superkomputerowe USA) w ramach projektu NLANR. Głównym projektem realizowanym w 1995 proku w ramach NLANR była konstrukcja, testowanie oraz uruchomienie vBNS - szybkiej (622Mbps) sieci komputerowej łączącej działające w ramach metacentrum ośrodki superkomputerowe w różnych stanach. W ramach optymalizacji ruchu HTTP wewnątrz USA stworzono szkieletową sieć składającą się z kilku serwerów cache w silnej konfiguracji rozmieszczonych w centrach superkomputerowych. Serwery te tworzą najwyższego rzędu strukurę na poziomie krajowym i w zamierzeniu służyć mają obsłudze serwerów niższych rzędów.

Na przełomie 1995/96, niemal jednocześnie z uruchomieniem struktury amerykańskiej rozpoczął się rozwój hierarchii WWW cache w Polsce (pod nazwą W3cache) oraz w Wielkiej Brytanii, a następnie w Niemczech oraz we Francji. Obok projektu NLANR rozwijany jest także Europejski projekt DESIRE.

Najszybciej rozwinął się cache brytyjski (działający w oparciu o 6 dedykowanych serwerów SGI Challenge oraz kilkanaście mniejszych serwerów działających przy różnych uniwersytetach) oraz cache w Nowej Zelandii, gdzie bardzo szybko stał się usługą o charakterze komercyjnym.

Serwery najwyższego rzędu w hierarchiach krajowych bardzo szybko zaczęły łączyć się w strukturę międzynarodową umożliwiającą optymalną wymianę danych. Dziś światowa struktura WWW cache obejmuje oprócz serwerów w USA i Polsce także Australię, Austrię, Czechy, Danię, Nową Zelandię, Finlandię, Francję, Japonię, Niemcy, Republikę Południowej Afryki, Szwecję, Wielką Brytanię, i Włochy. Każdy z serwerów poziomu krajowego odpowiedzialny jest za dostarczanie innym dokumentów WWW z podległego sobie obszaru oraz od serwerów znajdujących się za nim w hierarchii.

Polska strukura serwerów (tzw. W3cache) budowana jest od końca 1995. Polska jako jedno z pierwszych państw rozpoczęła budowę krajowej struktury WWW cache juz pod koniec 1995. Projekt W3cache zakłada strukturę trójstopniową z centralnym serwerem krajowym obsługującym serwery miejskie. Serwery miejskie obsługują poszczególne MANy wraz z serwerami pojedyńczych instytucji zlokalizowanych na terenie danego miasta. Koordynacja w ramach struktury W3cache obejmuje tylko dwa pierwsze poziomy (serwer krajowy i serwery miejskie). Obecnie serwery miejskie działają już we wszystkich większych ośrodkach sieciowych (Gdańsk, Katowice, Kraków, Łódź, Poznań, Toruń, Warszawa, Wrocław) oraz w kilkunastu instytucjach oraz firmach komercyjnych.

W pierwszym kwartale 1996 w ślad za polskim projektem W3cache poszły Niemcy i Francja, które także próbują zbudować hierarchie krajowe.

W obrębie sieci miejskich serwery, które połączone są szybkimi łączami traktują siebie wzajemnie jako sąsiadów, zaś serwer krajowy traktują jako rodzica. Serwer krajowy z kolei współpracuje z serwerami krajowymi innych państw.

W maju 1996 struktura W3cache składa się z serwerów utrzymywanych przez następujące ośrodki:

serwer krajowy

- ICM, Warszawa

serwery miejskie

- MAN Gdańsk - Trójmiejska Akademicka Sieć Komputerowa
- MAN Katowice - Uniwersytet Śląski w Katowicach
- MAN Kraków - Akademia Górniczo-Hutnicza, Politechnika Krakowska
- MAN Łódź - Łódzka Miejska Sieć Komputerowa
- MAN Poznań - Poznańskie Centrum Superkomputerowo-Sieciowe
- MAN Toruń - Uniwersytet Mikołaja Kopernika
- MAN Warszawa - Interdyscyplinarne Centrum Modelowania
- MAN Wrocław - Politechnika Wrocławska

Większość serwerów w hierarchii W3cache używa oprogramowania *cached 1.4pl3*. W Krakowie testowany jest *Squid 1.0*, a w Warszawie *cached 2.0*. Przykładami szkół, w których uruchomiono uczelniane serwery W3cache, mogą być Uniwersytet Adama Mickiewicza w Poznaniu, SGGW lub Wyższa Szkoła Ubezpieczeń i Bankowości w Warszawie.

We wstępnym okresie eksploatacji, jeszcze przed oficjalnym udostępnieniem usługi na niektórych serwerach cache statystyki wskazują na transfer kilkuset megabajtów dziennie przy współczynniku trafień przekraczającym 40% (a czasami nawet 60%).

Stopień oszczędności cache'a zależy od "zogniskowania" serwera, tzn. przeznaczenia serwera do obsługi grup użytkowników o zbliżonych preferencjach. Dlatego należy sie spodziewać, że serwery cache obsługujące poszczególne instytucje będą miały zazwyczaj wyższy współczynnik trafień niż serwery miejskie. Stosunkowo najniższy współczynnik trafień zanotowano na cache w Warszawie. Przypuszczalnie jest to spowodowane tym, że cache warszawski i krajowy umieszczone są fizycznie na wspólnym serwerze.

Inne zebrane doświadczenia wskazują na znaczenie, jakie ma właściwy dobór czasu przechowywania dokumentów w cache. Problem jest o tyle złożony, że nie są w pełni opracowane algorytmy wykorzystania informacji zawartej w

polu *If-Modified-Since* nagłówka zapytania GET protokołu HTTP 1.0 i decyzja o czasie życia obiektu w cache podejmowana jest albo wyłącznie na podstawie zawartości pola *Last-Modified* oraz takich informacji jak rozmiar czy nazwa obiektu, albo bezwarunkowo na podstawie *If-Modified-Since*. Dłuższy czas życia obiektu oznacza większą oszczędność ruchu w sieci, ale jednocześnie zwiększa prawdopodobieństwo, że cache będzie udostępniać nieaktualne informacje.

Kolejnym zagadnieniem jest współpraca serwerów W3cache z serwerami cache komercyjnych dostawców Internetu w Polsce. O ile wydaje się że w większości przypadków nie ma tu żadnych przeciwwskazań, a nawet wykorzystanie W3cache należałoby uznać za korzystne, to w przypadku dostawców dysponujących własnymi łączami międzynarodowymi wydaje się, że współpracę między serwerami cache należy ograniczyć do zależności typu *sąsiad-sąsiad*. Ma to na celu uniknięcie sytuacji, w której ruch WWW jednego dostawcy byłby tunelowany przez łącze drugiego.

3 Przegląd innych struktur cache WWW

W większości krajów dynamiczny rozwój narodowych struktur WWW cache rozpoczął się w pierwszym kwartale 1996. Tam, gdzie jest to uzasadnione topologią sieci lub innymi względami, W3cache współpracuje ze strukturami zagranicznymi. Poniżej przedstawiamy przegląd kilku ciekawszych z nich.

3.1 Francja

Francuski projekt Renater-Cache[6] rozwija się od końca stycznia 1996. Koordynowana jest praca kilkunastu serwerów regionalnych działających w oparciu o Harvest cache w ramach struktury krajowej. W końcu maja planowany jest zakup serwera poziomu krajowego (DEC AlphaServer 1000) wyposażonego w 320 MB pamięci oraz 20 GB dysku. W międzyczasie testowane są różne konfiguracje grup sąsiadujących serwerów.

3.2 Niemcy

Działająca od stycznia 1996 w Niemczech struktura DE-cache [7] zmierza ku stworzeniu rozproszonego systemu serwerów WWW cache powiązanych wzajemnymi relacjami sąsiedztwa. W planach jest połączenie kilkunastu biorących udział w projekcie serwerów szybkimi łączami. DE-cache zmierza także do ujednolicenia nazw oraz sposobu działania serwerów.

[6] http://web.pasteur.fr/other/computer/cache/
[7] http://www.informatik.uni-bonn.de/de-cache/

3.3 Nowa Zelandia

W Nowej Zelandii hierarchia składa się z centralnego serwera cache (działającego na zasadach komercyjnych) wykorzystującego Harvest cache oraz obsługujących poszczególnych dostawców Internetu lokalnych serwerów, które traktują serwer centralny jako jedynego rodzica. Ze względu na duży koszt łącza transoceanicznego, WWW cache w Nowej Zelandii rozwija się niezwykle dynamicznie [8].

3.4 USA

Amerykański projekt NLANR Cache[9] , finansowany przez National Science Foundation stanowi część projektu vBNS rozwijanego przez narodowe metacentrum. We wstępnej fazie (przełom 1995/1996) uruchomiono 6 głównych serwerów w centrach superkomputerowych. Serwery te mają w założeniu wyłącznie obsługiwać serwery niższego rzędu oraz współdziałać z narodowymi serwerami w innych krajach. NLANR Cache wykorzystuje serwery DEC Alpha z 10 GB dysku każdy. Obecnie używane oprogramowanie, Harvest cache, przypuszczalnie zostanie w niedalekiej przyszłości zastąpione przez Squid.

3.5 Wielka Brytania

Finansowany z centralnych środków brytyjski projekt HENSA Cache[10] używa sześciu serwerow SGI Challenge w konfiguracjach 14 GB dysku i 256 MB RAM oraz 16 GB dysku i 128 MB RAM. Serwery HENSA wykorzystują komercyjne oprogramowanie firmy Netscape. HENSA szczyci się wysokim współczynnikiem trafień (powyżej 60%) oraz obsługuje ponad milion żądań dziennie.

Oprócz podanych przykładów projektow serwery WWW cache rozwijane są na mniejszą skalę m. in. w Australii, Austrii, Czechach, Danii, Estonii, Finlandii, Holandii, Japonii, Norwegii, Rosji, RPA, Szwecji, na Węgrzech oraz we Włoszech.

4 Podsumowanie

Polski Internet znalazł się w czołówce krajów, w których rozwijane są struktury WWW cache.

Korzyści wynoszone z systemu W3cache będą tym większe im większa będzie jego popularność. Dlatego należy skłaniać do współdziałania administratorów lokalnych sieci komputerowych namawiając ich do zakładania własnych serwerów cache korzystających z W3cache. Należy także namawiać poszczególnych

[8] http://www.waikato.ac.nz/harvest/www5/Overview.html
[9] http://www.nlanr.net/Cache/
[10] http://www.hensa.ac.uk/wwwcache/

użytkowników do jak najpowszechniejszego korzystania z tej usługi. Informacje o sposobie użycia W3cache dostępne są pod adresem

`http://w3cache.icm.edu.pl/`

Istnieje także lista dyskusyjna poświęcona problemom związanym z administrowaniem serwerów W3cache - `cached-admins@usk.pk.edu.pl`.

Jednocześnie należy dbać o to, aby usługa świadczona była na możliwie najwyższym poziomie, tym samym zachęcając dalszych użytkowników do korzystania z niej. W szczególności oznaczać to będzie konieczność inwestycji w serwery W3cache oraz łącza między nimi tak, aby były w stanie sprostać wzrastającemu obciążeniu.

LAN and WAN encryption

Security in a networked environment

Tommy Waszkiewicz
SECTRA AB
Teknikringen 2
583 30 LINKÖPING, Sweden

Email: tw@sectra.se

Summary

Modern computer networks offer many possibilities and threats. More and more networks are interconnected to create large organization wide networks. Today many applications rely on a combination of local and wide area networks to function properly. The information transmitted in networks is often both critically necessary to the owner and potentially very interesting to an enemy. This makes network security a worthwhile consideration for most modern organizations.

When designing a security system for today's networks it is important to realize that modern networks are very diverse. Not only do they consist of different media, they also change and grow fairly rapidly. This changing and diverse environment require flexible and manageable solutions. One way of achieving flexibility is to employ encryption at the network layer of communications (IP, IPX, etc.). Network layer security can be made independent of both physical media and applications.

Packet based encryption and filtering, possibly combined with a firewall is a very attractive way of implementing network layer security

One example of such a network security system is the KryptoLan® network encryption system. KryptoLan® work by encrypting the contents of (IP) packets and provides confidentiality, integrity and authentication. In order to simplify key and connection management the KryptoLan® system uses a centralized KeyServer.

Threats in a networked environment

Security concerns for computer networks are driven by two main trends: The move towards network-oriented applications (client-server) and the galloping growth of network interconnections. Not only is your organization's most valuable information available on the network, the network itself is also spreading in a way that is sometime hard to control.

One of the main security problems with most modern networks is that the end-users have no way of knowing how their information is transported from point A to point B. Not only is the network large and hard to overview, due to dynamic routing your network traffic may take a different route today compared to last week or even an hour ago! In reality this means that sending your information over the network is about as safe as writing it on a postcard and dropping it in the mail. Hopefully it will arrive at the intended recipient, but were it has been in between and who else may have read it is outside of your control. This situation is made worse by the increasing use of public infrastructure. Although appealing from an economical perspective, letting someone else transport your information can be a major security problem.

When dealing with security in a networked environment it is often a good idea to divide it into a number of objectives:

- Confidentiality, protecting your communications from eavesdropping.
- Integrity, make sure your messages arrive the way you sent them.
- Authentication, verify the identity of the party you are communicating with.
- Availability, make sure your network is working when you need it.

Confidentiality is traditionally archived by using encryption, normally with symmetrical methods for performance reasons. Integrity and authentication can be realized using asymmetrical cryptographic methods (e.g. RSA), or with a combination of symmetrical encryption, checksums and careful key management. Availability and robustness against communication failures is one of the main design criteria's of modern networking systems. However some precautions may be needed against hostile insertion of routing information and other denial of service attacks.

Traditionally encryption systems have been mainly of one of two types: Application level systems like file or E-mail encryption or link level systems like point-to-point and bulk encryptors, encrypting modems, etc. Application level security systems have the advantage of being virtually independent of network media and structure, however given the number of different applications in use large scale deployment of application security systems is not very practical. Link level security systems on the other hand can usually support any application but cannot provide end-to-end security and are also not very flexible in a changing network environment.

Network level encryption

One interesting type of security and encryption systems that have recently emerged is packet based network level security systems. These systems can be very flexible in the sense that they can support any application running on top of their supported protocols and at the same time being relatively independent of network media. Packet based encryption can somewhat simplified be described as encrypting only the data part of a packet leaving addresses and other header information in the clear. See figure 1.

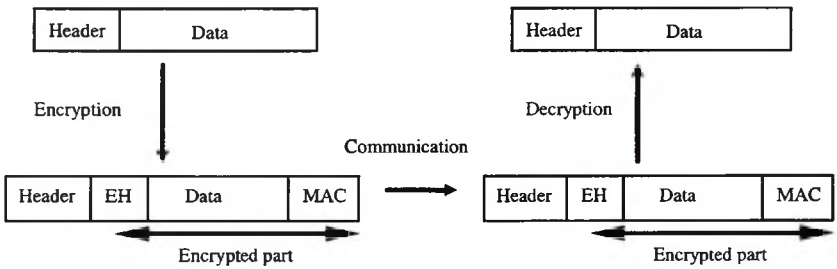


Figure 1. Packet based encryption.

As can bee seen from figure 1 an extra encryption header (EH) is inserted into the packet before the encrypted data. This header is used to carry synchronization information for use by the receiving party. Some systems also add an extra message authentication code (MAC) to the encrypted packet. This is used to detect manipulation during transit and thus provides integrity to the traffic.

During the past years a number of standards for this kind of packet oriented encryption has evolved. There are (at least) two ISO standards: ISO 10736 Transport Layer Security Protocol (TLSP) [1] and ISO 11577 Network Layer Security Protocol (NLSP) [2]. The US government have sponsored the Secure Data Network System, Security Protocol 3 (SNDS, SP3) [3] and for pure LAN networks there is the IEEE 802.10 SILS standard [4]. The Internet community recently released a series of standards on the subject in the form of the RFC's 1825 to 1829 [5] [6] [7] [8] [9]. Apart from these there are a number of commercial systems using propriety protocols or modified versions of the above standards.

Maybe the most interesting of the standards are the Internet RFC's. This is partly because they are defined for both IPv4 and IPv6 and thus cover the most interesting network protocols both today and for the future. Another reason to look into these standards is that they are very implementation oriented and clear. This makes it likely that they will be widely supported by different vendors.

As with any encryption system key management and distribution is a key issue (no pun intended) for network encryption systems. If every encryption unit in a large network is supposed to have secure communications with a number of other units the number of keys to manage can grow very large. This clearly calls for automated key management systems to be used. Two main types of automated key generation systems can be found: Peer-to-peer key generation using Diffie-Hellman or similar techniques and centralized key-server approaches. Peer-to peer key generation has the advantage of not relying on any centralized function, but on the other hand it requires strong authentication using some public key system (e.g. RSA) and established certificate chains to some trusted third party. Centralized key-servers are of course sensitive single point of failures, but this problem can be solved with redundant servers at different sites. The centralized server also provides a manageable checkpoint for all communications within the system.

One important aspect of packet based encryption is the possibility to mix encrypted and clear text traffic thru the same unit. This is often very desirable in order to access public services and network support services such as DNS. The problem however with cleartext passage is that it requires extensive filtering in order not to break the security of the system. One way of implementing this filtering is to complement the encryption equipment with a firewall.

The KryptoLan system

One example of network encryption systems is the KryptoLan® system from SECTRA AB. KryptoLan® can encrypt network traffic at both IP and Ethernet levels. The Ethernet encryption is implemented using a propriety version of the IEEE 802.10 SILS standard. IP encryption is handled in a manner very similar to RFC 1825-1829. A typical KryptoLan® system might look something like figure 2.

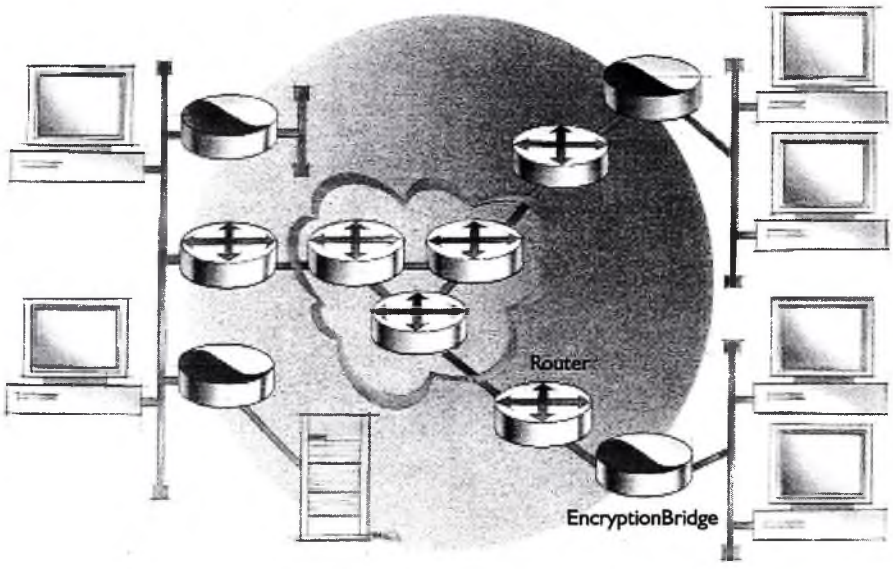


Figure 2. A typical KryptoLan® system

The main component of a KryptoLan® system is the encryption unit, called EncryptionBridge. The EncryptionBridge is placed between the protected part of the network and the rest of the network. Any traffic going between the protected network to the outside world is subject to filtering and possibly encryption. One EncryptionBridge can handle many simultaneous connections to different counterparts, some of which are encrypted and some in clear text.

Key management in a KryptoLan® system can be done in two different ways. One possibility is to manually configure the EncryptionBridges, the other alternative is to use a centralized KeyServer. Manual configuration is useful if you are designing a small system with only a few EncryptionBridges. If you have a system with more than a handful of EncryptionBridges a KeyServer will dramatically reduce the effort required to manage communications in the system. The KeyServer contains a database of allowed communications and information about which connections to encrypt and which to leave in clear text. Apart from managing allowed communication paths the KeyServer also generates and distributes encryption keys. This is all handled automatically and keys can be changed with configurable intervals.

In order to increase the robustness of the system several redundant KeyServers can be used at the same time. In this case every EncryptionBridge uses its primary KeyServer as long as it is available. If the primary KeyServer goes off line the EncryptionBridges automatically switches to the redundant spare. Redundant KeyServers can also be used for load sharing in very large networks.

Conclusion

Network encryption is a flexible and economical way to implement communications security in a networked environment. The benefits of network encryption include:

- End to end communications security. No intermediate clear text hops.
- Scaleable solution for both local and wide area networks.

- Transparent security service to all applications using the network.
- Independence of transport media and topology.
- Possibility to use public infrastructure in a secure way.
- Clear text and encrypted traffic can be mixed in the same network removing the need for multiple cabling in mixed environments.

The KryptoLan® system realizes all these benefits and also provides communications integrity, authentication and simplified key management using a KeyServer.

If a mix of clertext and encryption is desired thru the encryption equipment one should be very careful about the cleartext that is passed thru. Extensive filtering, probably in the shape of a firewall, is recommended.

References

[1] ISO/IEC, Transport Layer Security Protocol, ISO/IEC DIS 10736.

[2] ISO/IEC, Network Layer Security Protocol, ISO/IEC DIS 11577.

[3] SNDS Secure Data Network System, Security Protocol 3, SP3, Document SDN.301, Revision 1.5, 15 May 1989.

[4] IEEE, Standard for Interoperable Local Area Network Security, IEEE 802.10.

[5] Atkinson, R., Security Architecture for the Internet Protocol, RFC 1825, NRL, August 1995.

[6] Atkinson, R., IP Authentication Header, RFC 1826, NRL, August 1995.

[7] Atkinson, R., IP Encapsulating Security Payload, RFC 1827, NRL, August 1995.

[8] Metzger, P., and W. Simpson, IP Authentication with Keyd MD5, RFC 1828, Piermont, Daydreamer, August 1995.

[9] Karn, P., Metzger, P., and W. Simpson, The ESP DES-CBC Transform, RFC 1829, Qualcom, Inc., Piermont, Daydreamer, August 1995.

STRATEGIA PRZECHODZENIA DO ATM

Daniel J. Bem, Waldemar E. Grzebyk, Jarosław M. Janukiewicz

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1. Wprowadzenie

Dwa lata temu na pierwszej konferencji POLMAN autorzy postawili pytanie „Czy już nadszedł czas na ATM ?". Był to pretekst do dyskusji na temat możliwości i zaawansowania standardów Asynchronous Transfer Mode. Konkluzja była ostrożna i wyważona. ATM jest technologią, która umożliwi budowę skalowalnych jednorodnych sieci. Mimo iż wiele aspektów ATM-u jest jeszcze nie unormowanych należy rozpocząć prace związane z przygotowaniem do wdrażania tej technologii. W nowo budowanych sieciach należy uwzględniać tę technologię przy wyborze okablowania. Stan zaawansowania w technologii ATM pozwoli na powszechne jej stosowanie w perspektywie 3 do 6 lat.

W ostatnich dwóch latach nastąpiła eksplozja prac wdrożeniowych ATM-u. Znacznie zwiększyła się liczba dostawców sprzętu. W przeciągu roku 1995 gremia standaryzacyjne a głównie ATM Forum wprowadziły wiele zaleceń. Pojawił się sprzęt i oprogramowanie o stabilnych parametrach. Ceny sprzętu zmniejszyły się na tyle, że rozwiązania zgodne ze standardami ATM zbliżają się do do rozwiązań tradycyjnych. Dotyczy to głównie rozwiązań dla sieci lokalnych i miejskich.

Nadal pozostaje nierozwiązanych wiele problemów dotyczących współpracy urządzeń różnych producentów co jest podstawową barierą zastosowania ATM-u w sieciach rozległych. Wdrażanie ATM-u związane jest z wieloma problemami, różnymi w zależności od miejsca ulokowania urządzeń. Inne wymaganie są stawiane przed urządzeniami do transmisji danych a inne do transmisji wizji, inaczej powinny zachowywać się urządzenia na styku z użytkownikiem a inaczej wewnątrz sieci. Nie jest to sprawa standardu ATM ale głównie styku z innymi urządzeniami. Wiele firm proponuje swoje rozwiązania, które pozwalają na płynną ewolucję w kierunku technologii ATM. Rozwiązania te obecnie nastawione są na transmisję danych i wchłonięcie istniejących technologii (Ethernet, Token Ring, FDDI).

Można zaryzykować stwierdzenie, że ATM jest na tyle zaawansowany, że dynamika wdrażeń nie będzie limitowana rozwojem technologii a raczej szybkością wzrostu zapotrzebowania na usługi szerokopasmowe.

2. ATM w Polsce

Polska jest krajem znacznie opóźnionym w stosunku do krajów nasyconych usługami telekomunikacyjnymi. Jednak dzięki opóźnieniu paradoksalnie jesteśmy gotowi na przyjęcie najnowszych technologii telekomunikacyjnych. Obecnie działa wiele ogólnokrajowych sieci transmisji danych głównie opartych o protokół X.25 (Polpak, Telbank, Kolpak, PRONet).

W zeszłym roku NASK zaoferował - jako pierwsza w Polsce sieć - usługi transmisji w standardzie Frame Relay (FR). Sieć została zbudowana na komutatorach FR typu ER (Enterprise Router) i IAN (Integrated Access Node) firmy Ascom Timeplex.

Na początku bieżącego roku została uruchomiona sieć TP S.A. zgodna ze standardami Frame Relay (Polpak-T). Sieć jest zbudowana na urządzeniach firmy Nortel Limited serii

Magellan Passport 50 i 160. Sieć pracuje na połączeniach o szybkości 2 Mb/s. Sieć Polpak-T ma zasięg ogólnokrajowy z rozbudowaną infrastrukturą w większych miastach wojewódzkich. Na wybranych kierunkach (Gdańsk-Warszawa, Łódź-Warszawa, Katowice-Warszawa) uruchamiane są połączenia pracujące w technologii ATM na połączeniach o prędkości transmisji 34 Mb/s.

Należy wspomnieć o pierwszej w Polsce sieci budowanej od początku jako sieć ATM. Warszawski WARMAN budowany przez NASK jest największą w kraju siecią ATM obsługującą zarówno środowisko naukowe jak i użytkowników komercyjnych.

Tabela 1 Wykorzystanie urządzeń ATM w sieciach akademickich

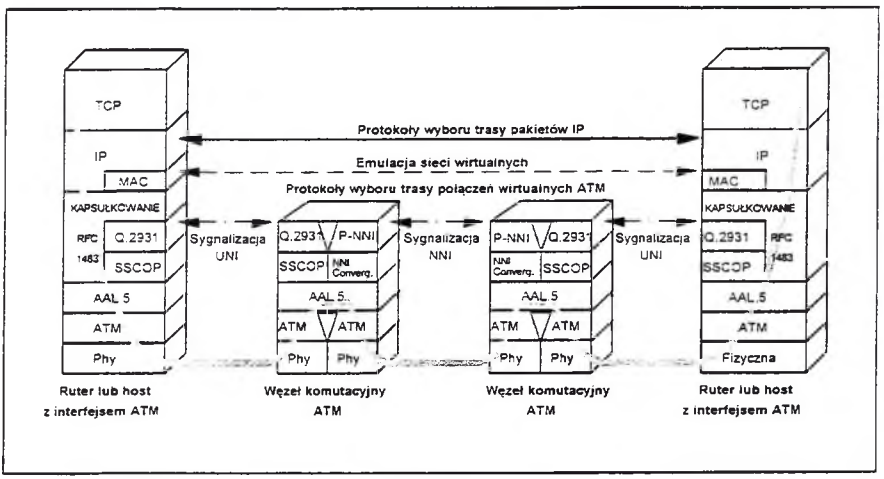
Lp.	Nazwa sieci	Typ urządzeń ATM i urządzeń dostępowych z interfejsem ATM	Uwagi:
1	**BIAMAN** - Białostocka Miejska sieć Komputerowa	**CISCO:** 2xLS100, 2xC5000, 1xC4700	Rozwój sieci planowany do końca 1996 roku.
2.	Miejska Akademicka Sieć Komputerowa w Bydgoszczy	**CISCO:** 2xLS100, 1xC7505, 1xC4700	Rozwój sieci planowany do końca 1996 roku.
3.	**KOSMAN** - Miejska Sieć Komputerowa w Koszalinie	------	Sieć pracuje w standardzie FDDI.
4.	Miejska Sieć Komputerowa w Krakowie	**CISCO:** 2xLS100, 2xC7000, 1xC7010	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.
5.	**LODMAN** - Miejska Sieć Komputerowa w Łodzi	**GDC:** 3xAPEX **CISCO:** 7x(Ruter)	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.
6.	**POZMAN** - Poznańska Akademicka Sieć Komputerowa	**FORE:** 1xASX-200WG, 2xASX200BX, 2xLAX-20 **3COM:** 2xCELLplex 7000 2xLinkSwitch 2700	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.
7.	**PULMAN** - Miejska Sieć Komputerowa w Puławach	------	Planowane wykonanie sieci w standardzie FDDI.
8.	**RAMAN** - Radomska Akademicka sieci Komputerowa	**CISCO:** LS100	Planowany zakup urządzeń na początku 1997 roku.
9.	**RMSK** - Rzeszowska Miejska Sieć Komputerowa	**CISCO:** 1xLS100, 2xC4500	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.
10.	Miejska sieć komputerowa w Szczecinie	**FORE:** 1xASX-200, 4xLAX-20	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.
11.	Regionalna Sieć Komputerowa Środowiska Śląskiego	-----	Planowany jest rozwój sieci w standardzie ATM w latach 1997-1998.
12.	**TORMAN** - Miejska Sieć Komputerowa w Toruniu	**CISCO:** 2xLS100, 1xC7010, 2xC4700	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.
13.	**TASK** - Akademicka Sieć Komputerowa Trójmiasta	**CISCO:** 8xLS100, 2xC7000, 2x7010	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.
14.	**WARMAN** - Miejska Sieć Komputerowa w Warszawie	**GDC:** 10xAPEX-DV2	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.
15.	**WASK** - Wrocławska Akademicka Sieć Komputerowa	**CISCO:** 2xLS100, 3xC5000, 2xC7000, 1xC7010	Stan obecny. Planowany jest dalszy rozwój sieci w standardzie ATM.

Od trzech lat z inicjatywy Komitetu Badań Naukowych budowane są w 15 ośrodkach miejskie sieci komputerowe (MSK) dla potrzeb nauki. Technologia ATM jest wdrażana w tych ośrodkach na dwa sposoby. Pierwszy na wzór Warszawy, który mozna określić „do ATM-u przez ATM" i drugi polegający na ewolucji w kręgosłupie sieci od technologii FDDI do ATM.

Obecnie prawie wszystkie sieci akademickie wprowadzają urządzenia ATM do swoich sieci. Przegląd rozwiązań sprzętowych stosowanych w MSK w standardzie ATM zamieszczono w tabeli (*Tabela 1*). Dane w tabeli pochodzą z materiałów opublikowanych na konferencji POLMAN'96.

3. Stan standaryzacji ATM-u

Do niedawna najczęściej stosowanym standardem transmisji danych pomiędzy sieciami LAN był „IP over ATM" wykorzystujący warstwę adaptacyjną 5 i niegwarantowany tryb transmisji danych UBR (ang. Unspecified Bit Rate) (*Rys. 1*). Implementacje tego standardu są zgodne z zaleceniami IEFT (ang. Internet Engineering Task Force) RFC 1483 i RFC 1577.



Rys. 1. Model transmisji pakietowej przez sieć ATM

Pod koniec 1995 roku ATM Forum wydało zalecenie dotyczące realizacji emulacji sieci lokalnej z wykorzystaniem sieci ATM (LANE 1.0). LANE (ang. Local Area Network Emulation) pozwala na przeniesienie poprzez sieć ATM ruchu sieci lokalnych (obecnie Ethernet) bez potrzeby modyfikacji protokołów w istniejących sieciach.

Znane są implementacje transmisji dźwięku i wizji poprzez ATM z wykorzystaniem CBR (ang. Constant Bit Rate). Zdefiniowane są klasy usług typu VBR (ang. Variable Bit Rate) dla transmisji skompresowanych sygnałów wizji i ABR (ang. Available Bit Rate) przeznaczona dla transmisji danych z ograniczoną gwarancją jakości transmisji.

Oczekiwane jest opracowanie standardu transmisji wieloprotokołowej (ang. Multiprotocol Over ATM) związanego z klasą usług ABR. Istotne dla współpracy urządzeń z różnych firm jest implementacja protokołu rutowania w ATM zgodna ze specyfikacją P-NNI Phase 1 (ang. Private Network Node Interface). Implementacja protokołów rutowania pozwala na efektywne wykorzystanie techniki przełączanych kanałów wirtualnych (SVC).

Obecnie współpraca urządzeń różnych producentów odbywa się z wykorzystaniem trwałych kanałów wirtualnych (PVC). Zdefiniowany jest cały szereg interfejsów użytkownika o prędkościach od 2 do 155 Mb/s. Od początku bieżącego roku pojawiło się wiele ofert na karty ATM przeznaczone do stacji roboczych i komputerów osobistych. Rozwój oprogramowania dedykowanego dla ATM-u w zakresie transmisji danych i usług transmisji wizji może stać się motorem dla szybkiego wzrostu zapotrzebowania na usługi transportowe ATM-u.

Poważnym problemem we wdrożeniach jest brak standardu w zakresie zarządzania komutatorami ATM. Najczęściej producenci implementują protokół SNMP i oferują oprogramowanie współpracujące z jedną z platform zarządzania. Wielu producentów stosuje własne nawzajem niekompatybilne rozwiązania systemów zarządzania.

4.Wnioski

Technologia ATM jest obecnie wprowadzana do polskiej telekomunikacji. Można zauważyć silny rozwój głównie sieci lokalnych i miejskich związany z technologią ATM. Obecnie sieci ATM przenoszą ruch pomiędzy sieciami lokalnymi i stanowią szybki kręgosłup sieci transmisji danych. W kilku ośrodkach akademickich tworzone są centra komputerowe wykorzystujące technologię ATM do realizacji usług multimedialnych.

Planowany w najbliższych latach przez TP S.A. rozwój szybkiej sieci SDH o zasięgu ogólnokrajowym stworzy warunki do wdrażania ATM-u w sieciach krajowych. Należy się spodziewać że migracja do technologii ATM jako podstawy sieci teletransmisyjnych to sprawa najbliższych 3–4 lat. Rozwój usług Frame Relay jest czynnikiem stymulującym rozwój rynku potencjalnych komercyjnych użytkowników technologii ATM. Zapotrzebowanie na komercyjne zastosowanie ATM-u przyspieszy prace standaryzacyjne.

Pierwszym klientem ogólnokrajowych systemów transmisji ATM może być środowisko akademickie dysponujące odpowiednim sprzętem i zasobami uzasadniającymi wykorzystanie tej technologii. Środowisko akademickie jest generatorem rozwoju zastosowań trasmisji szerokopasmowej. Może ono wnieść duży wkład na rzecz rozwoju ATM-u przez prace nad rozwojem usług multimedialnych. Przy ograniczonych środkach na telekomunikację współpraca środowiska akademickiego z operatorami może zaowocować opracowaniem optymalnej drogi rozwoju systemów teletransmisyjnych. Możliwe byłoby prowadzenie prac pilotażowych związanych z testowaniem współpracy urządzeń różnych producentów służące przyjęciu odpowiednich standardów.

Podsumowując:

- technologia ATM jest dojrzała na tyle aby wprowadzać ją do sieci lokalnych i miejskich,
- należy stosować urządzenia ATM gdzie jest to ekonomicznie uzasadnione i jest wyraźne zapotrzebowanie na usługi wymagające transmisji szerokopasmowych,
- wykorzystanie technologii ATM jest uzasadnione w sieciach o złożonej topologii,
- przy wyborze urządzeń do sieci należy się kierować zgodnością z istniejącymi standardami; w szczególności należy zwrócić uwagę na wykorzystanie standardowych interfejsów, implementacje LANE, P-NNI, IP over ATM, obsługę ruchu typu CBR, VBR, ABR, dostępność adapterów do transmisji wizji i fonii,

- należy sobie zdać sprawę, że na obecnym etapie rozwoju oprogramowania dla ATM-u przy budowie sieci konieczne jest stosowanie urządzeń typu ruterów (rutowanie w sieciach pakietowych)
- wskazany jest wybór urządzeń mających zaimplementowaną obsługę protokołów warstwy trzeciej (ang, multi layer switch) w zastosowaniach związanych z łączeniem LAN-ów,
- wskazane jest instalowanie interfejsów ATM w komputerach do zastosowań multimedialnych,
- w momencie pojawienia się łączy SDH korzystne byłoby nawiązanie współpracy pomiędzy ośrodkami akademickimi i TP S.A. w celu tworzenia pilotowych instalacji sieci ATM o zasięgu krajowym. Wnioski z takich doświadczeń stanowiłyby podstawę do sformułowania kierunków rozwoju ogólnopolskiej sieci szerokopasmowej.

5.Literatura

[1]. D.J. Bem, J.M. Janukiewicz, Czy już nadszedł czas na ATM, Miejskie Sieci Komputerowe w Nauce i Gospodarce POLMAN'94; Materiały z konferencji; Ośrodek Wydawnictw Naukowych, Poznań 1994, str. 50 -54.

[2]. Miejskie Sieci Komputerowe w Nauce i Gospodarce i Administracji POLMAN'96; Materiały z konferencji; Ośrodek Wydawnictw Naukowych, Poznań 1996.

SYSTEM ZASILANIA AWARYJNEGO JAKO ELEMENT ZARZĄDZANIA SIECIĄ

Waldemar E. Grzebyk, Jarosław M. Janukiewicz, Tomasz Banyś[*)]

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1. Wprowadzenie

Awarie i jakość zasilania urządzeń są krytycznym czynnikiem wpływającym na skuteczność działania sieci komputerowej. Sieć komputerowa nie jest autonomicznym systemem i jej działanie silnie zależy od stanu sieci energetycznej. Niewłaściwe zasilanie jest jedną z najczęstszych przyczyn awarii spotykanych w sieciach komputerowych. Z tego względu głównym składnikiem systemu zarządzania w sytuacjach awaryjnych powinien być przemyślany proces kontroli jakości i awarii zasilania. Brak zasilania węzła sieci oznacza brak kontroli nad węzłem zarówno w aspekcie zarządzania jak i bezpieczeństwa systemu. W artykule zostanie omówiony aspekt zarządzania siecią w sytuacjach awaryjnych. Zostanie przeprowadzona dyskusja właściwości urządzeń zasilających UPS (ang. Uninterruptible Power Supply) w sieciowym systemie zasilania awaryjnego.

2. Zarządzanie siecią w sytuacji awarii zasilania

2.1 Aspekty zarządzania według ISO

W dobie powszechnego rozwoju sieci komputerowych, problem właściwego zarządzania ich zasobami jest bardzo istotny. Systemy zarządzające powinny pracować niezawodnie i bezpiecznie. Wymagana jest efektywna transmisja dużej ilości informacji (wykorzystywanych w procesie zarządzania) na znaczne odległości. Bazując na istniejących standardach i zaleceniach możliwa jest budowa systemu zarządzania siecią. Istnieją normy (np. ISO/IEC 7498) określające składowe systemu zarządzania siecią. ISO dzieli problem zarządzania systemami otwartymi na pięć aspektów:

- zarządzanie w sytuacjach awaryjnych (ang. fault management),
- zarządzanie wydajnością (ang. performance management),
- zarządzanie rozliczeniami (ang. accounting management),
- zarządzanie konfiguracjami (ang. configuration management),
- zarządzanie zabezpieczeniami (ang. security management).

Rozróżnienie pięciu aspektów ułatwia analizę problemu zarządzania. Na realizację każdego z nich składają się trzy funkcje:

- ciągłe zbieranie informacji o stanie sieci komputerowej,
- wykonanie pewnych operacji w celu rozwiązania problemu,
- zbieranie doświadczeń i planowanie właściwych rozwiązań na przyszłość.

Niezależnie od pięciu aspektów zarządzania, ISO wyróżnia trzy stany systemu zarządzania:

- monitorowanie (ang. monitoring) - pozwalające na zbieranie informacji wykorzystywanych w procesie zarządzania,

[*)] Instytut Telekomunikacji i Akustyki Politechniki Wrocławskiej

- kontrolowanie (ang. control) - czyli manipulacja stanem urządzeń,
- raportowanie (ang. reporting) - urządzenie alarmuje o określonych zdarzeniach.

Mimo dużych nakładów jakie zostały poniesione na prace standaryzacyjne i wypracowanie kompletnego rozwiązania OSI, nie jest ono powszechnie implementowane. Ogromną popularnością cieszy się Internet i związany z nią system zarządzania zdefiniowany w ramach standardu Internet-standard Network Management Framework korzystający z protokołu SNMP (ang. Simple Network Management Protocol). System zarządzania dla sieci Internet jest rozwiązaniem ograniczonym funkcjonalnie w stosunku do proponowanego standardu OSI. Posiada jednak podstawową przewagę - jest skutecznie implementowany.

2.2 Zarządzanie w sytuacjach awaryjnych

Zajmuje się zapobieganiem skutkom awarii w sieciach komputerowych. Ten składnik systemu zarządzania NMS (ang. Network Management System) jest szczególnie ważny i dostrzegany przez ISO. Awarie w sieciach komputerowych powodują poważne ograniczenie jakości usług oferowanych użytkownikowi.

Skuteczne rozwiązanie zarządzania w sytuacjach awaryjnych wymaga systemu powiadamiającego administratora o awarii i narzędzi umożliwiających podjęcie odpowiednich działań. W systemie zarządzania w sytuacjach awaryjnych można wyróżnić kilka funkcjonalnych kroków:

- analiza sygnałów związanych z awariami poszczególnych składników sieci komputerowej. Pozwala ona na izolację danego problemu do poszczególnych elementów sieci komputerowej (np. urządzenie, system operacyjny, oprogramowanie, medium itd.),
- diagnostyka prowadząca do precyzyjnego określenia przyczyny awarii i sposobów jej usunięcia,
- zapewnienie poprawnego działania sieci komputerowej w okresie usuwania przyczyn awarii - obejście przyczyn awarii,
- powiadamianie operatora,
- zdalne usunięcie przyczyn awarii - jeżeli jest to możliwe,
- gromadzenie informacji opisującej aktualny stan otoczenia awarii.

2.3 Zasilanie urządzeń

Opisane wcześniej założenia systemu zarządzania siecią są poprawne jeżeli stan urządzeń jest niezależny od stanu sieci energetycznej. Założenie to jest konieczne ponieważ w rzeczywistych systemach informacja o stanie urządzeń nie może być przesłana po zaniku zasilania urządzeń. Analiza otoczenia miejsca awarii sprowadza się w przypadku sieci komputerowej zazwyczaj do stwierdzenia, że węzeł sieci przestał pracować nie dociera natomiast informacja wskazująca co było jej przyczyną . Rozwiązaniem tego problemu może być realizacja systemu awaryjnego zasilania. W praktyce spotyka się dwa typy systemów awaryjnego zasilania (UPS): centralny dla wszystkich urządzeń lub rozproszony obejmujący poszczególne urządzenia. Pierwszy jest rozwiązaniem dobrym dla pojedynczych urządzeń lub urządzeń umieszczonych na niewielkim obszarze. W sieciach miejskich i rozległych duża odległość pomiędzy węzłami wymusza stosowanie systemów rozproszonych. Jeżeli system jest rozproszony to najwygodniejszą formą sterowania i monitorowania UPS-a jest wykorzystanie tych samych mechanizmów jakie stosowane są do zarządzania urządzeń sieciowych. Obecnie będzie to przede wszystkim protokół SNMP i jedna z platform zarządzania ulokowana na stacji roboczej.

3. Modele działania UPS-a i stacji zarządzającej

Typowy UPS filtruje zakłócenia zasilania w trybie ciągłym. W przypadku znaczących spadków lub wzrostów napięcia zasilania UPS zapewnia niezależne zasilanie z baterii. W odróżnieniu od filtracji zakłóceń, przejście na zasilanie awaryjne wiąże się z wykorzystywaniem skończonego zasobu UPS-a jakim jest energia elektryczna zgromadzona w bateriach.

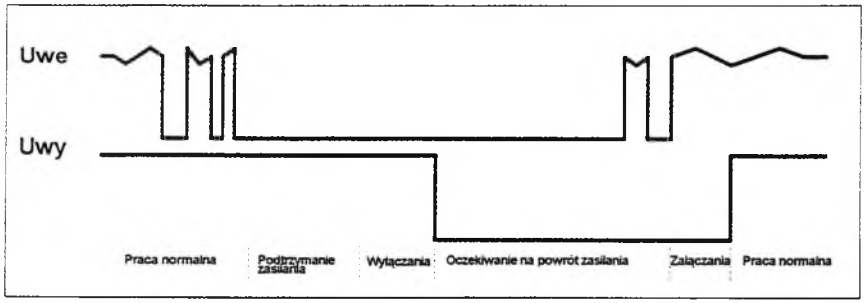
Można zamodelować działanie UPS-a przy następujących założeniach:

- zasilanie na wejściu UPS-a jest dwustanowe: prawidłowe lub nieprawidłowe,
- zasilanie na wyjściu UPS-a jest dwustanowe: włączone lub wyłączone.
- jeżeli na wyjściu jest zasilanie to ma ono optymalną charakterystykę.
- zasilanie stacji roboczej powinno być utrzymane do czasu poprawnego zatrzymania systemu operacyjnego,
- zasilanie bezdyskowych urządzeń sieciowych może zostać przerwane w dowolnym momencie po przesłaniu informacji o awarii.

Istotne jest określenie maksymalnego czasu podtrzymania zasilania. Przy długim czasie podtrzymania istnieje szansa powrotu zasilania w sieci energetycznej - co oznacza, że UPS zapewni poprawne zasilanie urządzenia przez cały okres awarii. Przy ustalonej pojemności akumulatorów wydłużanie czasu powoduje rozładowanie akumulatorów. W efekcie seria awarii zasilania może spowodować, że kolejna awaria nie zostanie zneutralizowana.

Włączanie i wyłączanie napięcia na wyjściu UPS-a jest związane z pewną histerezą zapobiegającą niestabilności systemu w przypadku szybkich zmian napięcia na wejściu UPS-a. Typowy przebieg zmian napięcia podczas awarii zasilania został przedstawiony na rysunku (*Rys. 1*).

W zależności od stanu napięcia podczas awarii zasilania, system zarządzania podejmuje działania sterujące UPS-em. Model działania UPS-a w sieci zarządzania przedstawiono na rysunku (*Rys. 2*), natomiast model działania stacji zarządzającej na rysunku (*Rys. 3*).



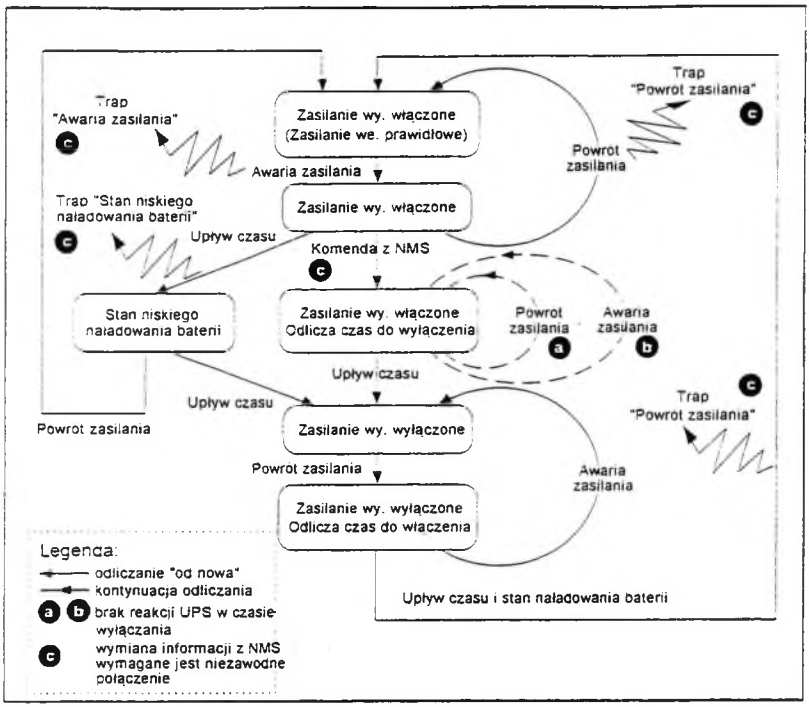
Rys. 1. Przebieg zmian napięcia na wejściu i wyjściu UPS-a w czasie awarii zasilania

Na rysunku (*Rys. 2*) małymi literami alfabetu oznaczono sytuacje modelu działania UPS-a w sieci zarządzania, które wymagają stosownego komentarza:

a) jak wspomniano wcześniej UPS w stanie odliczania czasu do wyłączenia obwodów wyjściowych ignoruje powrót zasilania na wejściu,

b) podobnie jak w punkcie a) - cykl powrotu i ponownej awarii zasilania nie jest w stanie przerwać procesu odliczania, który nieuchronnie zakończy się wyłączeniem zasilania na wyjściu UPS-a.

c) przekazanie komendy UPS-owi przez NMS jak i wysłanie alarmu (ang. trap) wymaga zapewnienia poprawnej łączności między tymi elementami.



Rys. 2. Model działania UPS-a w sieci zarządzania

Na rysunku (*Rys. 3*) małymi literami alfabetu oznaczono sytuacje modelu działania stacji zarządzającej wymagające komentarza:

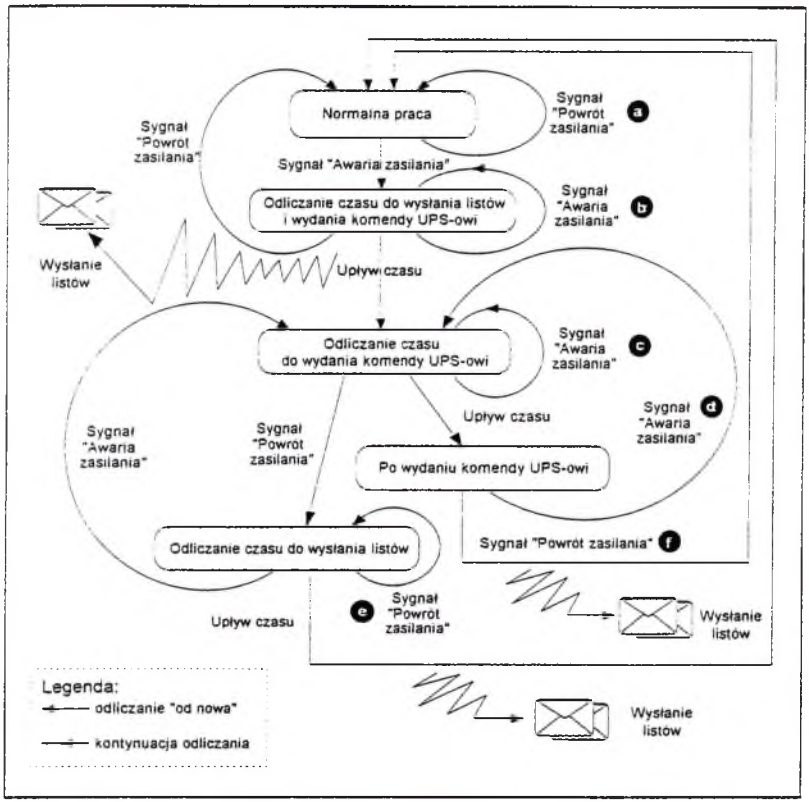
a) system zarządzania nie otrzymał wcześniej sygnału o awarii zasilania. Pojawienie się sygnału o powrocie zasilania w tym stanie systemu zarządzania powinno być ignorowane. Odpowiednio częste odpytywanie UPS-a o jego stan pozwoli na wykrycie braku łączności lub awarii zasilania.

b) i c) system zarządzania nie otrzymał wcześniejszej informacji o powrocie zasilania. Traktując nową awarię (o której sygnał nadszedł) jako kontynuację starej, system powinien kontynuować stosowny proces odliczania. Częste odpytywanie UPS-a o jego status pozwoliłoby na wykrycie powrotu zasilania lub braku łączności,

d) złożony wypadek w którym wcześniej nie dotarła informacja o powrocie zasilania. Przy założeniu, że komenda wydana przez stację zarządzającą została wykonana przez UPS (co oznacza, że UPS wyłączył zasilanie na wyjściu) sygnał taki powinien być traktowany jako nowa awaria i uruchomić rutynową procedurę jej obsługi. Należy podkreślić, że nie jest uzasadnione wysyłanie listów informujących o nowej awarii zasilania. Z punktu widzenia administratorów domen poprzednia awaria zasilania trwa bowiem nadal. Wysłanie nowego listu zakłóciłoby spójność korespondencji,

e) nie dotarła wcześniejsza informacja o awarii zasilania. System zarządzania powinien zacząć liczyć od początku wymagany czas poprawności zasilania na wejściu UPS-a,

f) sposób podłączania adaptera SNMP do sieci oznacza, że w przypadku wcześniejszego wyłączenia zasilania na wyjściu UPS-a po jego odtworzeniu alarm (trap) wysłany przez adapter SNMP nie dotrze do NMS. Wynika to wprost z większego czasu inicjalizacji rutera niż opóźnienie wysłania alarmu przez adapter SNMP UPS-a. Z tego względu niezbędne jest istnienie procesu, który będzie odpytywał okresowo UPS-y o status zasilania na ich wyjściu. Aby ograniczyć obciążenie sieci proces ten powinien odpytywać UPS-y uprzednio wyłączone lub te, których nie udało się wyłączyć (ze względu na brak łączności).



Rys. 3. Model działania stacji zarządzającej

Scenariusze pracy systemu zarządzania w sytuacjach awarii zasilania pracują w trybie predykcyjnym. Na podstawie przebiegu historii zasilania i jego aktualnego stanu przewidują optymalne zachowanie się UPS-a przy jego określonych zasobach energetycznych. Informacją niezbędną do opracowania scenariuszy działań jest charakterystyka statystyczna awarii zasilania w danej sieci energetycznej. Podstawowymi parametrami zasilania wejściowego modelu UPS-a są:

- czas trwania awarii zasilania,
- czas poprawnego stanu zasilania między awariami.

Bazując na opisanym modelu rozważano następujące warianty czasu podtrzymania zasilania urządzeń przez UPS:

- równego połowie maksymalnego czasu podtrzymania przy aktualnym stanie parametrów: pojemność baterii i obciążenie. To rozwiązanie oznacza, że w przypadku serii powtarzających się awarii zasilania czas podtrzymania będzie się stopniowo zmniejszał,
- stałego, określonego na podstawie możliwości podtrzymania zasilania przez UPS w stanie "pełnych" baterii.

W przypadku serii powtarzających się awarii rozważano zasadę wyłączenia UPS-a na dłuższy okres. Detekcja serii awarii może być oparta o analizę aktualnego stanu baterii UPS-a. Tak więc osiągnięcie przez energię elektryczną zgromadzoną w bateriach UPS-a określonego minimalnego poziomu powinno być sygnałem do wyłączenia UPS-a na dłuższy okres. Dłuższy okres wyłączenia był tutaj rozpatrywany w dwóch kategoriach:

- stałego interwału czasowego, określanego w chwili wydania komendy wyłączenia. UPS zostaje wyłączony na ten okres czasu niezależnie od stanu zasilającej go sieci energetycznej,
- skonfigurowania warunku minimalnej pojemności baterii przy której UPS może zostać włączony. Proszę zauważyć, że w tym przypadku okres dłuższego wyłączenia UPS-a jest zależny od czasu trwania awarii i czasu prawidłowego zasilania, które pozwoli na ewentualne doładowanie baterii. W chwili wyłączenia nie jest więc możliwe określenie czasu jego trwania.

Kolejnym zagadnieniem jest scenariusz odtwarzania zasilania na wyjściu UPS-a w zależności od stanu zasilania na wejściu. Przyjęto tutaj zasadę włączania (wcześniej wyłączonych) obwodów wyjściowych UPS-a pod warunkiem, że stan zasilania na wejściu (po jego powrocie) będzie prawidłowy przez określony kwant czasu. Wprowadzone "opóźnienie" jest podyktowane przede wszystkim zakłóceniami jakie mogą się pojawić w momencie powrotu zasilania w sieci energetycznej (chociażby z powodu jednoczesnego włączania wielu urządzeń). Warto podkreślić, że opóźnienie to eliminuje także możliwość powstania na wyjściu UPS-a krótkotrwałych zaników zasilania. W tym wypadku minimalny czas zaniku zasilania na wyjściu UPS-a jest bowiem równy omawianemu czasowi opóźnienia.

3.1. Weryfikacja modeli działania UPS-a i stacji zarządzającej

Zweryfikowano modele działania UPS-a i stacji zaradzającej w oparciu o scenariusze działania systemu zarządzania w sytuacjach awarii zasilania. Wykorzystano w tym celu fragment sieci eksperymentalnej zawierający:

- dwa UPS-y Smart-UPS® 600RM podtrzymujące zasilanie dwóch ruterów,
- UPS Smart-UPS® 2000RM podtrzymujący zasilanie stacji roboczej.

Na rysunku (*Rys. 4*) przedstawiono sposób realizacji podłączenia systemu zasilania awaryjnego węzła sieci.

Opracowane scenariusze działania systemu zarządzania w sytuacjach awarii zasilania ruterów i stacji roboczej zostały zaimplementowane w postaci skryptów systemu operacyjnego UNIX. Ze względu na wykorzystywane mechanizmy wysyłania listów i uruchamiania programów z opóźnieniem, zastosowano koncepcję przechowywania aktualnej informacji o stanie zasilania w plikach - unikalnych dla każdego urządzenia.

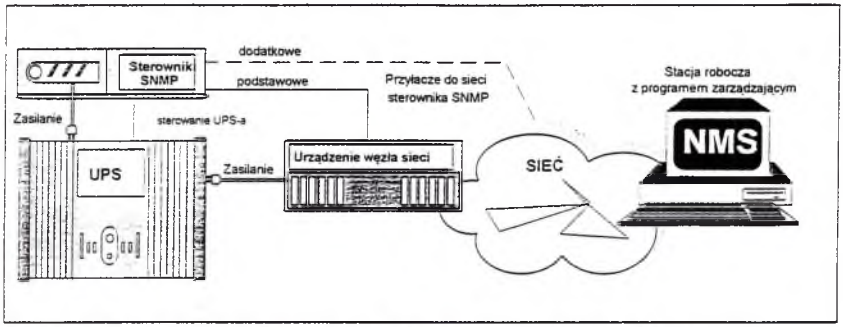
Testy poprawności proponowanych scenariuszy działań systemu zarządzania w sytuacjach awarii zasilania zostały przeprowadzone dla różnych wariantów stanów łączności miedzy NMS a UPS-em:

- łączność NMS-UPS zapewniona,

- brak łączności NMS-UPS.

Przeprowadzone testy programów wypadły pozytywnie. Na rysunku (*Rys. 1*) zaprezentowano przykładowy przebieg stanu napięcia na wejściu i wyjściu UPS-a dla kolejnych awarii zasilania.

W przeprowadzonych testach nie uwzględniono aspektu sekwencyjnego wyłączania ruterów. Ten aspekt działania systemu zarządzania nie został praktycznie zweryfikowany.



Rys. 4. Sposób realizacji podłączenia systemu zasilania awaryjnego węzła sieci

4.Wnioski

Zarządzanie w sytuacji awarii zasilania w sieci komputerowej jest ważnym elementem zarządzania w sytuacjach awaryjnych. Opisane modele były opracowane dla sieci miejskiej można je łatwo adaptować dopasowując do wymogów różnych sieci. Wykorzystanie protokołu SNMP do monitorowania, kontrolowania i raportowania stanu zasilania pozwala na integrację z systemem zarządzania siecią. Sterowniki wykorzystane w eksperymentach mogą być wyposażone w przystawkę pozwalającą monitorować otoczenie UPS-a. Możliwy jest pomiar temperatury i wilgotności. Dwustanowe wejścia pozwalają na integrację z systemami alarmowymi po zainstalowaniu czujek przeciwpożarowych czy też przeciwwłamaniowych.

Uwzględnienie topologii sieci poprzez ustalenie sekwencji wyłączeń UPS-ów oraz stosowanie dynamicznych protokołów rutowania pozwala na budowę sieci odpornej na awarie zasilania.

5.Literatura

[1]. W. E. Grzebyk, J. M. Janukiewicz, "System zasilania awaryjnego w miejskiej sieci komputerowej we Wrocławiu", Materiały z konferencji POLMAN'95, Ośrodek Wydawnictw Naukowych, Poznań 1995, (str. 136÷140).

[2]. K. McCloghrie, M. Rose, Management Information Base for network management of TCP/IP-based Internets: MIB-I, RFC 1066, 1988.

[3]. K. McCloghrie, M. Rose, Structure and Identification of Management Information for TCP/IP-based Internets, RFC 1155, 1990.

[4]. M. Schoffstall, M. Fedor, J. Davin, J. Case, A Simple Network Management Protocol (SNMP), RFC 1157, 1990.

[5]. K. McCloghrie, M. Rose, Concise MIB Definitions, RFC 1212, 1991

[6]. K. McCloghrie, M. Rose, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, RFC 1213, 1991.

[7]. M. Rose, A Convention for Defining Traps for use with the SNMP, RFC 1215, 1991.

KOMPATYBILNOŚĆ ELEKTROMAGNETYCZNA W SIECIACH STRUKTURALNYCH

Waldemar E. Grzebyk, Jarosław M. Janukiewicz

Naukowa i Akademicka Sieć Komputerowa
Zakład Telekomunikacji
50-327 Wrocław, ul. Janiszewskiego 7/9, tel./fax: 219529

1. Wprowadzenie

Powstanie koncepcji systemu okablowania strukturalnego było odpowiedzią na szybki rozwój sieci komputerowych. W Europie obowiązuje norma ISO/IEC DIS 11801 dotyczącą zasad tworzenia takiego systemu. Dotyczy ona przemysłowego okablowania budynków i określa wymagania odnoszące się do okablowania budynków przeznaczonego do przesyłania sygnałów akustycznych i transmisji danych. Norma ISO/IEC DIS 11801 ma charakter zaleceń ogólnych. Określa ona jakie funkcjonalnie kryteria techniczne mają spełniać instalowane połączenia kablowe i złącza oraz podaje wytyczne dotyczące dopuszczalnych technik instalowania oraz pomiarów. Oddzielne zagadnienie stanowi kompatybilność elektromagnetyczna sieci strukturalnych.

Zakład Naukowy Telekomunikacji NASK od ponad roku prowadzi badania dotyczące kompatybilności elektromagnetycznej mediów transmisyjnych stosowanych w sieciach komputerowych. Do tego celu wykorzystywane są techniki i metody pomiarowe zalecane przez odpowiednie normy. Jedną z metod badania są pomiary odporności na zakłócenia impulsowe. Ten typ zakłóceń ze względu na krótkotrwałe czasy narostu sygnałów zakłócających oraz ich szerokie pasmo częstotliwości ma zastosowanie w badaniach urządzeń informatycznych.

Badając poszczególne elementy sieci strukturalnych z punktu widzenia kompatybilności elektromagnetycznej (np. media transmisyjne, urządzenia aktywne) należy pamiętać, że z chwilą ich połączenia mogą się pojawić duże zakłócenia elektromagnetyczne będące wynikiem źle wykonanej instalacji a nie materiałów i urządzeń.

Włączając się do trwającej dyskusji - Ekranować czy nie ? - na temat okablowania w sieciach strukturalnych przedstawiamy w artykule fragment naszej pracy badawczej dotyczącej kompatybilności elektromagnetycznej mediów transmisyjnych stosownych w sieciach komputerowych.

2. Europejskie standardy kompatybilności elektromagnetycznej

Pod pojęciem kompatybilności elektromagnetycznej EMC systemu (ang. Electromagnetic Compatibility) rozumiemy jego zdolność do poprawnej pracy w swoim otoczeniu.

Kompatybilność elektromagnetyczna obejmuje dwa aspekty pracy systemu:

- emisja (ang. emission) - poziom zakłóceń elektromagnetycznych generowanych przez system nie może zakłócać otoczenia,
- odporność (ang. immunity) - pole elektromagnetyczne otaczające system nie może powodować jego wadliwej pracy.

Tabela 1

Wytyczna	Oznaczenie wytycznej	Uwagi:
Dyrektywa EMC	89/336/EEC	Kompatybilność elektromagnetyczna
Uzupełnienie 1 Dyrektywy EMC	92/31/EEC	Powołano normę: EN 55022.
Uzupełnienie 2 Dyrektywy EMC	93/68/EEC	EN 50082-1

Tabela 2

Kompatybilność elektromagnetyczna / Pomieszczenia i urzadzenia	Emisja		Odporność	
powszechnego użytku, **komercyjne,** **środowisko przemysłu lekkiego**	**EN-50081-1;1992 Standard źródłowy**		**EN 50082-1;1995 Standard źródłowy**	
	Normy szczegółowe stowarzyszone		Normy szczegółowe stowarzyszone	
	Normy IEC	Normy EN	Normy EN	Normy EN
	IEC 50(161)	-	IEC 50(161)	-
	IEC 555-1	EN 60555-1	IEC 1000-4-2	EN 61000-4-2: 1995
	IEC 555-2 (mod)	EN 60555-2	IEC 1000-4-4	EN 61000-4-4: 1995
	IEC 555-3	EN 60555-3	IEC 1000-4-5	EN 61000-4-5: 1995
	CISPR 14 (mod)	EN 55014	IEC 1000-4-8	EN 61000-4-8: 1993
	CISPR 22 (mod)	EN 55022	IEC 1000-4-11	EN 61000-4-11: 1994
			-	ENV 50140: 1993
			-	ENV 50141: 1993
			-	ENV 50204: 1995
środowisko przemysłu ciężkiego	**EN-50081-2;1993 Standard źródłowy**		**50082-2;1994 Standard źródłowy**	
	Normy szczegółowe stowarzyszone		Normy szczegółowe stowarzyszone	
	Standardy IEC	Standardy EN	Standardy IEC	Standardy EN
	IEC 50(161)	-	IEC 50(161)	-
	CISPR 11 (mod)	EN 55011	IEC 801-4	-
	CISPR 14	EN 55014	IEC 1000-4-4	EN 61000-4-4
	CISPR 22;1985 (mod)	EN 55022: 1987	IEC 1000-4-8	EN 61000-4-8
			CISPR 11 (mod)	EN 55011
			CISPR 22: 1985	EN 55022: 1987
			-	ENV 50140: 1993
			-	ENV 50141: 1993

(mod) - modyfikacja standardu

W chwili obecnej nie ma standardów dotyczących kompatybilności elektromagnetycznej dedykowanych specjalnie dla sieci strukturalnych. W Europie Zachodniej podstawę w dziedzinie kompatybilności elektromagnetycznej stanowi wytyczna (ang. directive) 89/366/EEC (*Tabela* 1) opublikowana w Oficjalnym Dzienniku Unii Europejskiej (ang. Official Journal on the European Union). Na podstawie tej wytycznej wraz z uzupełnieniem 92/31/EEC oraz na bazie normy CISPR 22 (ang. Internacional Special Committee of Radio Interference) powstał harmonizowany standard EN 550022 (tzn. zwierający harmonizowane procedury testowe i wzorce odniesienia). Określa on wartości graniczne oraz opisuje metody pomiaru charakterystyk interferencji radiowych urządzeń technologii informatycznej.
Ponad to Europejska Komisja CENELEC (ang. European Committee for Electrotechnical Standardisation) opracowała i ratyfikowała dwa źródłowe standardy (ang. generic standard) dotyczące kompatybilności elektromagnetycznej *(Tabela 2)*:

- **EN 50081-1; 1992** - Kompatybilność elektromagnetyczna - Źródłowy standard emisji
  Część. 1 Pomieszczenia i urządzenia powszechnego użytku, komercyjne i środowisko przemysłu lekkiego
  EN 50081-2; 1993 - Część. 2 Pomieszczenia i urządzenia środowisko przemysłu ciężkiego
- **EN 50082-1; 1995** - Kompatybilność elektromagnetyczna - Źródłowy standard odporności
  Część. 1 Pomieszczenia i urządzenia powszechnego użytku, komercyjne i środowisko przemysłu lekkiego
  EN 50082-2; 1994 - Część. 2 Pomieszczenia i urządzenia środowisko przemysłu ciężkiego

Obydwie normy mają głównie zastosowanie dla urządzeń elektronicznych i elektrycznych oraz do systemów i instalacji wytwarzających zakłócenia elektromagnetyczne lub narażonych na ich działanie. Sieci strukturalne należy traktować jako składowe technologii informatycznej IT (ang. Information Technology) i telekomunikacyjnego wyposażenia końcowego TTE (ang. Telecommunication Terminal Equipment). Muszą one spełniać wymagania odpowiednich standardów stowarzyszonych z normami **EN 50081 i EN 50082.**

W chwili obecnej są opracowywane standardy dotyczące zasad wykonywania okablowania z punktu widzenia kompatybilności elektromagnetycznej. Przykładem może być norma EN 50174 określająca zasady instalacji okablowania dla telekomunikacji i techniki informatycznej.

*Tabela 3. Zakres norm stowarzyszonych z normą **EN 50081-1; 1992***

Standard IEC	**Standard europejski EN**	**Zakres**
IEC 50(161)	-	Międzynarodowy Słownik Elektrotechniczny Rozdział 161: Kompatybilność elektromagnetyczna
IEC 555-1	EN 60555-1	Rozkłady emisji w systemach zasilania powodowane przez urządzenia domowe oraz podobny sprzęt elektryczny Cześć 1: Definicje
IEC 555-2 (mod)	EN 60555-2	Część 2: Harmoniczne
IEC 555-3	EN 60555-3	Część 3: Fluktuacje napięcia
CISPR 14 (mod)	EN 55014	Wartości graniczne i metody pomiaru charakterystyk interferencji radiowych elektronicznych urządzeń domowych, urządzeń przenośnych oraz podobnych urządzeń elektrycznych
CISPR 22 (mod)	EN 55022	Wartości graniczne i metody pomiaru charakterystyk interferencji radiowych urządzeń technologii informatycznej

Tabela 4. Zakres norm stowarzyszonych z normą EN 50081-2: 1993

Standard IEC	Standard europejski EN	Zakres
IEC 50(161)	-	Międzynarodowy Słownik Elektrotechniczny Rozdział 161: Kompatybilność elektromagnetyczna
CISPR 11 (mod)	EN 55011	Wartości graniczne i metody pomiaru charakterystyk zakłóceń radiowych urządzeń przemysłowych , badawczych, i medycznych (ISM) pracujących w zakresie częstotliwości radiowych
CISPR 14	EN 55014	Wartości graniczne i metody pomiaru charakterystyk zakłóceń radiowych od silników elektrycznych i urządzeń ciepłowniczych przeznaczonych dla domowych i podobnych potrzeb, maszyn elektrycznych, oraz podobnego sprzętu elektrycznego.
CISPR 22:1985 (mod)	EN 55022:1987	Wartości graniczne i metody pomiaru charakterystyk interferencji radiowych urządzeń technologii informatycznej

*Tabela 5. Zakres norm stowarzyszonych z normą **EN 50082-1; 1995***

Standard IEC	Standard europejski EN	Zakres
IEC 50(161)	-	Międzynarodowy Słownik Elektrotechniczny Rozdział 161: Kompatybilność elektromagnetyczna
IEC 1000-4-2	EN 61000-4-2:1995	Kompatybilność elektromagnetyczna (EMC) Część 4: Testowanie i techniki pomiarowe Sekcja 2:Wymagania dotyczące wyładowań elektrostatycznych
IEC 1000-4-4	EN 61000-4-4:1995	Sekcja 4:Wymagania dotyczące szybkich wyładowań elektrycznych
IEC 1000-4-5	EN 61000-4-5:1995	Sekcja 5: Testowanie odporności na przeciążenia
IEC 1000-4-8	EN 61000-4-8:1993	Sekcja 8: Testowanie odporności na pola magnetyczne o częstotliwości zasilania
IEC 1000-4-11	EN 61000-4-11:1994	Sekcja 11: Spadki napięcia, krótkie zaniki i zmiany napięcia
-	ENV 50140:1993	Testowanie odporności na promieniowane zakłócenia elektromagnetyczne o częstotliwościach radiowych
-	ENV 50141:1993	Testowanie odporności na przewodzone zakłócenia elektromagnetyczne o częstotliwościach radiowych
-	ENV 50204:1995	Testowanie odporności na promieniowane zakłócenia elektromagnetyczne pochodzące od radiotelefoni cyfrowej

*Tabela 6. Zakres norm stowarzyszonych z normą **EN 50082-2; 1994***

Standard IEC	Standard europejski EN	Tytuł
IEC 50(161)	-	Międzynarodowy Słownik Elektrotechniczny Rozdział 161: Kompatybilność elektromagnetyczna
IEC 801-4	-	Kompatybilność elektromagnetyczna sprzętu pomiarowego kontrolnego związanego z procesami przemysłowymi Sekcja 4:Wymagania dotyczące szybkich wyładowań elektrycznych
IEC 1000-4-2	EN 61000-4-2	Kompatybilność elektromagnetyczna (EMC) Część 4: Testowanie i techniki pomiarowe Sekcja 4:Wymagania dotyczące szybkich wyładowań elektrycznych

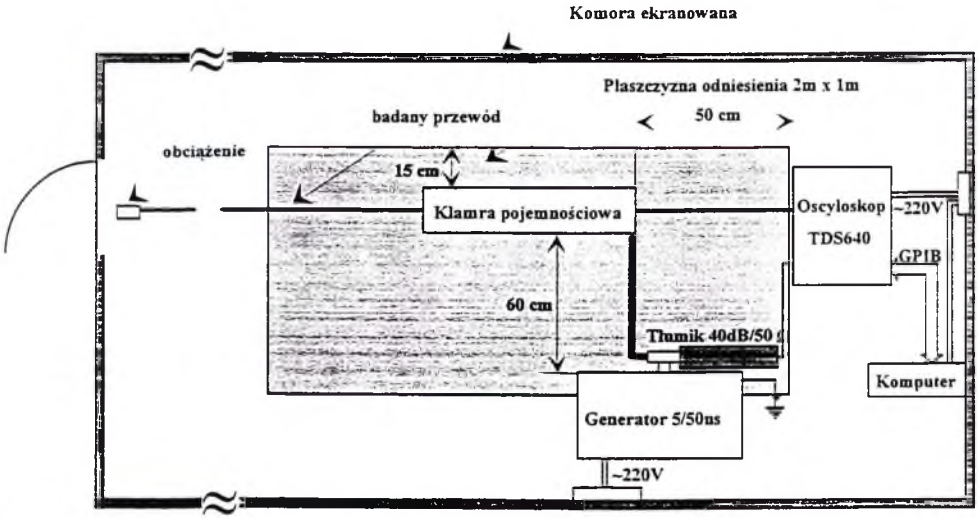
Tabela 6. cd. Zakres norm stowarzyszonych z normą EN 50082-2: 1994

Standard IEC	Standard europejski EN	Tytuł
IEC 1000-4-8	EN 61000-4-8	Sekcja 8: Testowanie odporności na pola magnetyczne o częstotliwości zasilania
CISPR 11 (mod)	EN 55011	Wartości graniczne i metody pomiaru charakterystyk zakłóceń radiowych urządzeń przemysłowych . badawczych. i medycznych (ISM) pracujących w zakresie częstotliwości radiowych
CISPR 22:1985	EN 55022:1987	Wartości graniczne i metody pomiaru charakterystyk interferencji radiowych urządzeń technologii informatycznej
-	ENV 50140:1993	Testowanie odporności na promieniowane zakłócenia elektromagnetyczne o częstotliwościach radiowych
-	ENV 50141:1993	Testowanie odporności na przewodzone zakłócenia elektromagnetyczne o częstotliwościach radiowych

3.Badania odporności torów na zakłócenia impulsowe

3.1 Stanowisko do badania odporności na impulsy typu "burst"

W badaniach wykorzystano stanowisko wyposażone w generator udarowy typu "burst" wytwarzający paczkę impulsów 5/50 ns o amplitudzie do 2 kV na obciążeniu 50Ω. Stanowisko to umożliwia prowadzenie badań zgodnie z wymaganiami: VDE 0843-4, VDE 0846-11, PN-86-06600, IEC-801-4. Jako element sprzęgający zastosowano klamrę pojemnościową.



Rysunek 1. Schemat układu pomiarowego

Zestawiony został układ pomiarowy jak na rysunku 1. W układzie tym dokonano jakościowego porównania napięć indukowanych w kablach symetrycznych. Porównano trzy typy kabli symetrycznych:

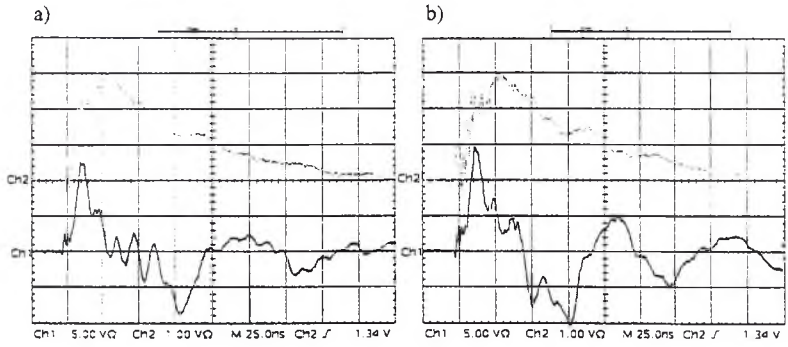
- kabel typu cztery pary „skrętki" nieekranowanej poziomu 3 (UTP),
- kabel typu cztery pary „skrętki" nieekranowanej poziomu 5 (UTP).
- kabel typu cztery pary „skrętki" w ekranie poziomu 5 (S/UTP).

3.2 Opis i wyniki badań

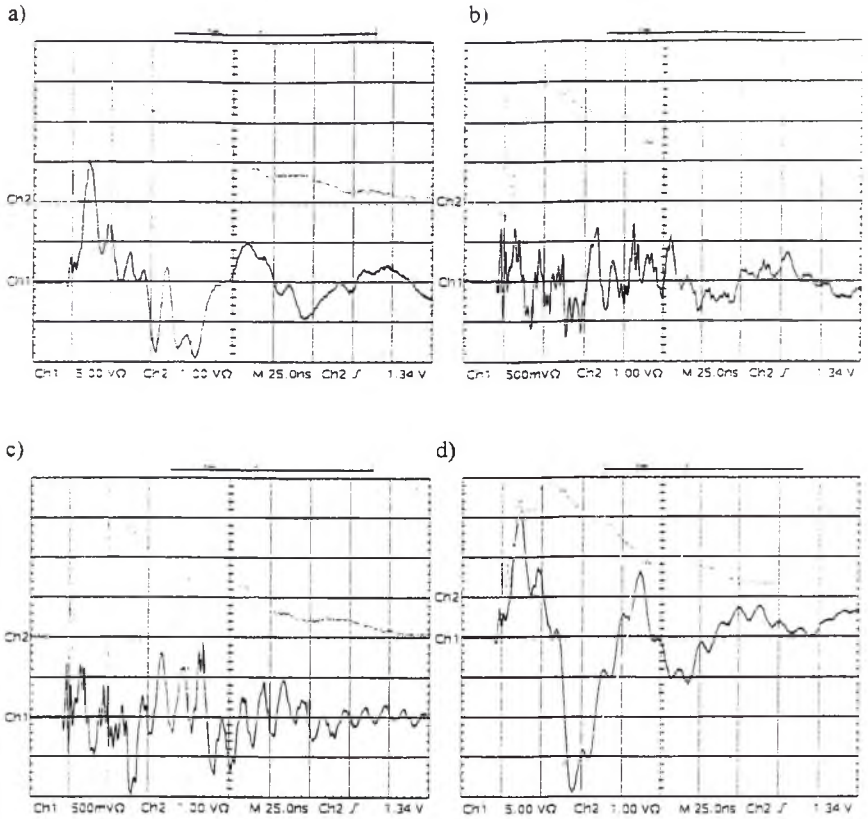
Dokonano pomiaru dla każdej z par przewodów w kablu. Napięcie na oscyloskopie było mierzone przez układ dopasowujący (100 Ω / 50 Ω). Wszystkie pary przewodów były zakończone rezystorami dopasowanymi do impedancji 100 Ω. Układ dopasowujący charakteryzował się słabym zrównoważeniem względem masy (~ 10 dB). W tym przypadku amplituda wyindukowanego napięcia jest dużo większa niż w układach o dobrym zrównoważeniu. Ponieważ wszystkie kable były mierzone w tym samym układzie nie zmienia to charakteru zjawisk. Na oscylogramach przedstawiono napięcia wyindukowane w wybranej parze przewodów dla każdego kabla.

Napięcie wyindukowane w kablu typu S/UTP było mierzone dla czterech przypadków:
- ekran nieuziemiony (rys. 3a),
- ekran uziemiony przy oscyloskopie (rys. 3b),
- ekran uziemiony przy oscyloskopie i obciążeniu (rys. 3c),
- ekran uziemiony przy obciążeniu (rys. 3d).

Uziemienie od strony obciążenia było wykonane cienkim przewodem o długości ok. 1,5 m.
Oscylogram napięcia wyindukowanego w kablu typu UTP poziomu 3 przedstawiono na rysunku 5a, w kablu typu UTP poziomu 5 na rysunku 2b.
Napięcia wyindukowane były mierzone w kanale 1 oscyloskopu (Ch1). W kanale 2 (Ch2) zarejestrowano kształt impulsu pobudzającego.



Rysunek 2. Pobudzenie i napięcie wyindukowane w parze przewodów kabli symetrycznych nieekranowanych a) UTP poziomu 3, b) UTP poziomu 5



Rysunek 3. Pobudzenie i napięcie wyindukowane w parze przewodów kabla symetrycznego ekranowanego typu S/UTP poziomu 5:

a) ekran nieuziemiony
b) ekran uziemiony przy oscyloskopie
c) ekran uziemiony przy oscyloskopie i obciążeniu
d) ekran uziemiony przy obciążeniu

4. Wnioski

Podatność na zakłócenia impulsowe kabli UTP poziomu 3 i 5 oraz kabla S/UTP poziomu 5 (bez uziemionego ekranu) było tego samego rzędu (rys. 2a, 2b, 3a). Uziemienie ekranu kabla S/UTP w znacznym stopniu wpływa na wielkość indukowanego napięcia. W przypadku prawidłowo wykonanego uziemienia ekranu można zauważyć zmniejszenie podatności kabla na zakłócenia impulsowe (rys. 3b, 3c). Nieprawidłowe uziemienie ekranu kabla powoduje wzrost podatności na zakłócenia w stosunku do kabla nieekranowanego (rys. 3d , 2b).

1. Stosowanie ekranowania wymaga spełnienia wielu warunków (dobre uziemienie, brak „petli prądowych", mała impedancja połączeń ekranów) a w praktyce jest trudne do wykonania.
2. Odporność torów symetrycznych na zakłócenia impulsowe jest szczególnie istotna w przypadku braku dobrze zdefiniowanego uziemienia.
3. Ekranowanie torów symetrycznych zmniejsza podatność na zakłócenia lecz źle wykonane może je zwiększyć.

5.Literatura

[1]. Grzebyk W.E., Janukiewicz J.M., Badnaia kabli symetrycznych z punktu widzenia kompatybilności elektromagnetycznej metodą impulsową, Materiały konferencyjne V Sympozjum Wojskowej Techniki Morskiej SWTM'95 (Tom 2, str. 65-71), Gdynia 24-25 października 1995.

[2]. Więckowski T.W., Badanie odporności urządzeń elektronicznych na impulsowe narażenia elektromagnetyczne, Prace Naukowe Instytutu Telekomunikacji i Akustyki Politechniki Wrocławskiej, Seria: Monografie, nr 37, Wrocław 1993.

[3]. Polska Norma PN-86/E-0600. Automatyka i pomiary przemysłowe. Kompatybilność elektromagnetyczna urządzeń. Ogólne wymagania i badania.

[4]. European Standard EN 50081-1, Electromagnetic compatibility - Generic emission standard Part. 1 Residential, commercial and light industry; January 1992.

[5]. European Standard EN 50081-2; Electromagnetic compatibility - Generic emission standard Part. 2 Industrial environment, August 1993.

[6]. European Standard EN 55082-1; Electromagnetic compatibility - Generic immunity standard Part. 1 Residential, commercial and light industry, September 1995.

[7]. European Standard EN 55082-2; Electromagnetic compatibility - Generic immunity standard Part. 2 Industrial environment, August 1994.

X.900 - Model odniesienia systemów przetwarzania rozproszonego

Jerzy Brzeziński, Włodzimierz Konopka

Naukowa i Akademicka Sieć Komputerowa JBR
Instytut Informatyki Politechniki Poznańskiej

1. Wstęp

Rozproszony system informatyczny (*system rozproszony*) jest zbiorem autonomicznych *jednostek przetwarzających* (*węzłów*) zintegrowanych *siecią komunikacyjną* (*łączami transmisyjnymi*) w celu realizacji wspólnego, globalnego celu przetwarzania. Systemy rozproszone charakteryzują się brakiem pamięci wspólnej i dlatego komunikacja między węzłami odbywa się w nich tylko za pomocą *wymiany wiadomości* (*komunikatów*). Czas transmisji wiadomości jest przy tym w ogólności skończony lecz nie znany. Każda z jednostek przetwarzających jest wyposażona w *procesor*, *lokalną pamięć* i *własne oprogramowanie zarządzające*. Wyróżnia się systemy rozproszone synchroniczne i asynchroniczne. W *systemach synchronicznych* działanie wszystkich procesorów jest zsynchronizowane wspólnym zegarem, natomiast w *systemach asynchronicznych* - poszczególne procesory wykonują operacje z różnymi prędkościami w takt niezależnych zegarów.

W ostatniej dekadzie nastąpił gwałtowny rozwój asynchronicznych systemów rozproszonych - w tym sieci komputerowych, systemów przetwarzania równoległego z rozproszoną pamięcią, rozproszonych środowisk programowania, rozproszonych systemów baz danych. Rozwój ten był w istocie naturalną konsekwencją ważnych własności systemów rozproszonych, charakteryzujących się potencjalnie:

- *skalowalnością* - w znaczeniu możliwości ciągłego i nieograniczonego rozwoju systemu bez negatywnego wpływu na jego efektywność i sprawność - wynikającą z modularności systemu i otwartości sieci komunikacyjnej;
- *dużą wydajnością* (*efektywnością*) - w sensie dostępnej mocy obliczeniowej, maksymalnej przepustowości, czasu odpowiedzi - wynikającą z możliwości jednoczesnego udziału wielu jednostek i systemów w realizacji wspólnego celu przetwarzania rozproszonego;
- *relatywnie niskimi kosztami* - w sensie kosztów niezbędnych do pozyskania wymaganej wydajności systemu - wynikającymi z niekorzystnego dla scentralizowanych systemów dużej mocy, wykładniczego wzrostu cen tych systemów w funkcji wydajności;
- *wysoką sprawnością wykorzystania zasobów* - w sensie stopnia (współczynnika) wykorzystania zasobu, względnego czasu zajętości, współczynnika jednoczesności - wynikającą z możliwości współdzielenia stanowisk usługowych, specyficznych urządzeń, programów i danych przez wszystkich użytkowników systemu, niezależnie od fizycznej lokalizacji użytkownika i zasobu;

- *podwyższoną niezawodnością* - w sensie odporności na błędy - wynikającą z możliwości użycia zasobów alternatywnych w przypadku wykrycia niesprawności;
- *elastycznością i otwartością funkcjonalną* - w sensie łatwości realizacji nowych, atrakcyjnych usług komunikacyjnych, informatycznych i informacyjnych (w tym usług multimedialnych) - wynikającą z integracji otwartej sieci komunikacyjnej i efektywnych, uniwersalnych jednostek przetwarzających.

Praktyczne osiągnięcie wymienionych potencjalnych możliwości systemów rozproszonych wymaga jednak efektywnego rozwiązania wielu nowych problemów (por. [1]). Podstawowa trudność wynika tu z konieczności stosowania w tym środowisku *algorytmów* (*programów*) *rozproszonych*, które składają się ze zbioru *procesów* (*zadań*) wykonywanych równolegle w różnych węzłach systemu. Procesy te komunikują się przez asynchroniczne kanały i współdziałają w realizacji globalnego, wspólnego celu przetwarzania. Charakterystyczny dla systemów rozproszonych asynchronizm komunikacji i działania procesorów implikuje *niedeterminizm wykonania programu* (przetwarzania). Dodatkowo brak wspólnej pamięci ogranicza dostępne wprost *mechanizmy synchronizacji*. Dlatego też konstrukcja i weryfikacja algorytmów rozproszonych ma swoją istotną specyfikę i rodzi szereg trudnych problemów, takich jak:

- optymalne zrównoleglenie programu przetwarzania;
- ocena poprawności i efektywności programu rozproszonego;
- alokacja zasobów rozproszonych;
- synchronizacja;
- detekcja stanu globalnego;
- transformacja modeli przetwarzania;
- niezawodność;
- bezpieczeństwo.

Jak wiadomo, *problem zrównoleglenia* sprowadza się do takiej transformacji algorytmu rozwiązywania zadania obliczeniowego na zbiór wzajemnie powiązanych procesów wykonywanych równolegle albo sekwencyjnie, by zminimalizować najdłuższą ścieżkę obliczeń sekwencyjnych, abstrahując od ograniczeń fizycznych i funkcjonalnych rzeczywistego środowiska przetwarzania.

Trudność *problemu oceny poprawności i efektywności* związana jest z koniecznością analizy wszelkich możliwych realizacji niedeterministycznego, w ogólności, programu rozproszonego.

Problem alokacji zasobów polega na takim przydziale (alokacji) dostępnych zasobów (procesorów, pamięci, urządzeń wejścia/wyjścia, danych, programów itd.) do procesów (zadań), by przy spełnieniu przyjętych bądź narzuconych warunków podzielności i ograniczeń kolejnościowych, zoptymalizować wybrane kryterium efektywności (zwykle, czas wykonania zbiory procesów).

Problem synchronizacji procesów, związany w ogólności z kooperacja procesów lub ich współzawodnictwem o dostęp do wspólnych zasobów, polega na realizacji w asynchronicznym środowisku rozproszonym mechanizmów umożliwiających wzajemne oddziaływanie procesów na ich względne prędkości przetwarzania, w celu dochowania ograniczeń kolejnościowych i zagwarantowania poprawności obliczeń (spójności).

Problem detekcji stanu globalnego polega natomiast na wyznaczaniu wartości parametrów lub predykatów globalnych związanych ze stanami procesów tworzących

obliczenia rozproszone. W asynchronicznym środowisku rozproszonym wyznaczanie stanu globalnego jest trudne i w ogólności niemożliwe bez wstrzymywania przetwarzania.

Problem transformacji modelu przetwarzania sprowadza się do realizacji na bazie modelu komunikacyjnego (podstawowego dla środowiska rozproszonego), modelu przetwarzania stosowniejszego do danego zastosowania lub wygodniejszego z punktu widzenia użytkownika (np. modelu pamięci współdzielonej, przetwarzania synchronicznego czy przetwarzania transakcyjnego).

Problemy niezawodności i bezpieczeństwa związane są z potrzebą zagwarantowania wymaganego poziomu jakości pracy systemu niezależnie od nieuniknionych błędów przypadkowych, lub celowych prób zniszczenia systemu czy naruszenia poufności i autentyczności informacji.

W wyniku prowadzonych od lat intensywnych badań w zakresie systemów rozproszonych dopracowano się szeregu praktycznych rozwiązań alternatywnych wymienionych problemów. Wobec braku, po części, rozwiązań w pełni satysfakcjonujących lub powszechnie akceptowanych, uzyskane wyniki prowokowały w rzeczywistości dynamiczny rozwój systemów rozproszonych różniących się często znacznie pod względem konstrukcyjnym. To zróżnicowanie doprowadziło wkrótce do nowych, trudnych problemów związanych z integracją *systemów niejednorodnych* (*heterogenicznych*) i dalszym ich rozwojem. Ujawniła się tym samym pilna potrzeba ustanowienia zasad (standardów), których przestrzeganie dawałoby możliwość efektywnego łączenia tworzonych niezależnie systemów heterogenicznych w sfederowane systemy rozproszone charakteryzujące się dalej skalowalnością, dużą wydajnością, wysoką sprawnością wykorzystania zasobów, podwyższoną niezawodnością, bezpieczeństwem i wygodą użytkowania.

Prace standaryzacyjne w zakresie *Otwartych Systemów Przetwarzania Rozproszonego ODP* (*Open Distributed Processing*) podjęto w *ISO* i *ITU* pod koniec lat osiemdziesiątych. Aktualnym efektem tych prac jest następująca seria dokumentów ([3], [4], [5], [6]) przedstawiających *Model Odniesienia Otwartych Systemów Przetwarzania Rozproszonego RM-ODP* (*Reference Model of Open Distributed Processing*):

1 ITU-T X.901 | ISO/IEC 10746-1 *Overview*. Przegląd ten określa podstawowe cechy systemu rozproszonego, definiuje ogólne wymagania stawiane systemom ODP i określa cele standaryzacji RM-ODP w kontekście wprowadzonych perspektyw (ang. *viewpoints*).

2. ITU-T X.902 | ISO/IEC 10746-2 *Fundations*. Dokument ten, mający charakter normatywny, wprowadza podstawowe koncepcje oraz pojęcia służące precyzyjnemu i uporządkowanemu opisowi systemu rozproszonego.

3. ITU-T X.903 | ISO/IEC 10746-3 *Architecture*. Dokument ten, mający również charakter normatywny, opisuje podstawowe elementy systemu, ich miejsce w architekturze oraz wzajemne powiązania.

4. ITU-T X.904 | ISO/IEC 10746-4 *Architectural semantics*. Dokument ten, wprowadza pojęcia i języki specyfikacji przy użyciu wybranych metod formalnych.

Powyższe dokumenty miały w grudniu 1995 roku status *Draft International Standard* (*DIS*).

2. Cel i ogólna charakterystyka RM-ODP

Model RM-ODP ma na celu przedstawienie spójnej koncepcji dotyczącej budowy systemów rozproszonych (por. [2], [7]). Przyjęto, że środowisko rozproszone powinno się charakteryzować skalowalnością, otwartością, przenośnością oprogramowania, wieloma poziomami transparentności.

Transparentność w systemach rozproszonych jest kluczowym problemem, który twórcy takich środowisk muszą rozwiązywać aby zapewnić użytkownikom złudzenie jednakowego dostępu do zasobów niezależnie od rozproszenia oraz heterogeniczności środowiska. Na tym polu model RM-ODP pełni rolę systematyzującą, definiując poziomy transparentności.

Twórcy środowisk rozproszonych stają też przed problemem wyposażenia go w zestaw niezbędnych funkcji. Rekomendacja serii X.900 definiuje zestaw funkcji ODP, grupując je w zależności od zastosowania.

Oprócz funkcji typowo systematyzujących, model RM-ODP wnosi nowe elementy do koncepcji systemów rozproszonych. Nowością jest wyróżnienie pięciu zasadniczych *perspektyw* widzenia systemu ODP (ang. *viewpoints*). Perspektywy znajdują zastosowanie w procesie tworzenia systemu rozproszonego, zwłaszcza na etapie analizy, specyfikacji i projektowania. Twórcy systemów rozproszonych uzyskują dzięki wyróżnionym perspektywom bazę koncepcyjną dla swoich projektów sprawiającą, że powyżej wymienione etapy powstawania systemu daje się ująć w rutynowo powtarzalne ramy, niezależnie od strony merytorycznej przedsięwzięcia.

Mianem nowoczesnej można określić również szkielet architektury (ang. *architectural framework*) systemów ODP zaproponowany przez twórców rekomendacji X.900. Można tu dostrzec pewną analogię do modelu CORBA (ang. *Common Object Request Broker*) zaproponowanego przez grupę OMG (ang. *Object Management Group*). Analogia ta wynika z faktu, że RM-ODP wykorzystuje modelowanie obiektowe na każdym poziomie opisu systemu rozproszonego i w związku z tym nawiązuje do problemów zarządzania w rozproszonych środowiskach zorientowanych obiektowo. Obiektowość systemów ODP wynosi je na wyższy poziom abstrakcji, gdzie istotny jest problem interakcji między kooperującymi obiektami, reprezentującymi *byty* rzeczywiste.

W części rekomendacji X.901 (ang. *Overview*) zwrócono też uwagę na zasadnicze cechy systemów rozproszonych:

- *rozproszenie* (ang. *remoteness*) - komponenty systemu (jednostki przetwarzające) są odległe od siebie w przestrzeni;
- *współbieżność* (ang. *concurency*) - komponenty systemu działają współbieżnie;
- *nieobserwowalność stanu globalnego* (ang. *lack of global state*) - wyznaczenie stanu globalnego systemu rozproszonego w zadanym momencie nie jest w ogólności możliwe;
- *cząstkowość awarii* (ang. *partial failures*) - poszczególne elementy sprzętowo-programowe mogą ulegać awariom, co nie musi uniemożliwiać funkcjonowania systemu jako całości;
- *asynchroniczność* (ang. *asynchrony*) - komunikacja i współbieżne przetwarzanie nie są synchronizowane globalnym zegarem.

Systemy rozproszone realizowane są przy użyciu wielu, różnych technologii informatycznych. Ze względu na ten fakt można wyróżnić kolejne cechy tych systemów:

- *heterogeniczność* (ang. *heterogenity*) - platformy sprzętowo-programowe węzłów systemu rozproszonego mogą się różnić, co nie powinno wykluczać możliwości ich współpracy;
- *autonomiczność* (ang. *autonomy*) - komponenty systemu rozproszonego mogą autonomicznie zarządzać środkami i zasobami pozostającymi w ich dyspozycji;
- *ewolucyjność* (ang. *evolution*) - możliwość dynamicznej zmiany konfiguracji systemu rozproszonego przez włączanie nowych elementów oraz ewolucyjny rozwój istniejących;
- *mobilność* (ang. *mobility*) - możliwość migracji elementów programowych (dane, procesy, obiekty) w ramach systemu rozproszonego.

Powyższa charakterystyka systemów rozproszonych implikuje konieczność postawienia szeregu postulatów odnośnie ich projektowania i realizacji. Norma X.901 wymienia następujące:

- *otwartość* (ang. *openness*) - w odniesieniu do dwóch aspektów:
  - *przenośności* (ang. *contribution of portability*) elementów programowych na różne węzły systemu rozproszonego bez potrzeby modyfikacji kodu,
  - *możliwości współdziałania elementów systemu rozproszonego poprzez sieci informatyczne* (ang. *internetworking*);
- *integralność* (ang. *integration*) - możliwość łączenia heterogenicznych środowisk informatycznych w jeden, spójny system rozproszony;
- *elastyczność* (ang. *flexibility*) - możliwość dynamicznej konfiguracji i modyfikacji systemu;
- *modularność* (ang. *modularity*) - poszczególne elementy systemu rozproszonego mogą działać autonomiczne, a połączone - współdziałać ze sobą poprzez wyspecyfikowane interfejsy;
- *zarządzalność* (ang. *manageability*) - możliwość monitorowania i zarządzania konfiguracją systemu rozproszonego;
- *bezpieczeństwo* (ang. *security*) - zabezpieczenie zasobów przed nieautoryzowanym dostępem;
- *transparentność rozproszenia* (ang. *transparency*) - przesłanianie faktu rozproszenia, przez oferowanie użytkownikom jednolitości operacji lokalnych i zdalnych.

Skupienie się na cechach i założeniach systemów rozproszonych potwierdza systematyzującą rolę rekomendacji RM-ODP.

3. Perspektywy systemów ODP.

Zgodnie z tradycyjnymi metodami analizy i projektowania wyróżnia się *specyfikację użytkową* (obejmującą cechy istotne z punktu widzenia użytkowników systemu), *specyfikację danych* (zawierającą struktury gromadzenia informacji i ich wzajemne powiązania), *specyfikację projektową* (określającą moduły oprogramowania) oraz *model przepływu informacji*.

Twórcy modelu RM-ODP określili pięć komplementarnych *perspektyw* (ang. *viewpoints*), składających się na pełny obraz systemu ODP. Każda perspektywa określa system ODP jako zespół obiektów wzajemnie na siebie oddziałujących. Perspektywy są istotne we wszystkich fazach powstawania systemu: analizie, specyfikacji, projektowaniu i implementacji.

3.1. Perspektywa przedsięwzięcia

Perspektywa przedsięwzięcia (ang. *Enterprise viewpoint*) jest odpowiednikiem specyfikacji użytkowej. Określa ona zakres i cel systemu, wyróżnia obiekty aktywne i pasywne na poziomie użytkowym. *Obiekty aktywne* to takie, które podejmują pewne działania modyfikujące inne obiekty, natomiast *obiekty pasywne* to te, na których takie działania są przeprowadzane. Obiekty aktywne grupowane są we *wspólnoty* (ang. *communities*) działające na rzecz osiągnięcia wspólnego celu. Specyfikacja, oprócz określenia obiektów i wspólnot, definiuje zestaw reguł odnoszących się do tych bytów. *Reguły* podzielone są na trzy grupy i określają procedury (ang. *bussiness activities*) jakie *mogą*, *muszą* lub *nie mogą* być wykonywane (ang. *permission, obligations, prohibition*).

Przykładem *obiektu przedsięwzięcia* (ang. *enterprise object*), występującego w specyfikacji przedsięwzięcia każdego z systemów, jest użytkownik, reprezentowany jako obiekt aktywny.

3.2. Perspektywa informacyjna

Z punktu widzenia *perspektywy informacyjnej* (ang. *Information viewpoint*), system ODP reprezentuje się jako zespół atomowych obiektów służących do gromadzenia informacji (ang. *information objects*) oraz wyróżnia się zależności między nimi. Specyfikacja abstrahuje od faktu rozproszenia.

Wyróżnia się dwa rodzaje obiektów informacyjnych: atomowe (ang. *values*) oraz złożone (ang. *composite information objects*). *Obiekty atomowe* reprezentują prostą informację, natomiast *obiekty złożone* - wyrażają relacje między prostymi obiektami informacyjnymi.

Reguły dotyczące zmian wartości w czasie obejmują trzy rodzaje *schematów* (ang. *related schemata*):

- *schematy niezmiennicze* (ang. *invariant schema*) - wyrażają związki, które muszą być spełnione podczas każdego zachowania się systemu (ujęte są tu więc wszystkie ograniczenia dotyczące wyjścia wartości poza dopuszczalny zakres);
- *schematy statyczne* (ang. *static schema*) - wyrażają warunki, które muszą być spełnione w wyróżnionych stanach (używane są zazwyczaj do określania wartości początkowych obiektów oraz stanów charakterystycznych, w których obiekt informacyjny powinien osiągnąć konkretnie zadaną wartość);
- *schematy dynamiczne* (ang. *dynamic schema*) - określają jak informacja może się zmieniać w czasie funkcjonowania systemu (definiują zasady wzajemnego oddziaływania obiektów na ich wartości, mogą określać sposób tworzenia i usuwania obiektów informacyjnych).

3.3. Perspektywa obliczenia

Perspektywa obliczeniowa (ang. *Computational viewpoint*) koncentruje się na cechach funkcjonalnych systemu. Wyróżnione tutaj *obiekty obliczeniowe* (ang. *computational objects*) mogą być elementami aplikacji użytkowej środowiska ODP, jak również elementami jego infrastruktury. Wyróżnione byty odpowiadają autonomicznym częściom systemu świadczącym pewne usługi poprzez swoje interfejsy.

3.4. Perspektywa inżynierska

Perspektywa inżynierska (ang. *Engineering viewpoint*) umiejscawia obiekty obliczeniowe w architekturze systemu ODP. Obiekty obliczeniowe uzyskują reprezentację w postaci *podstawowych obiektów inżynierskich* (ang. *basic engineering objects*) i są umieszczane w takich strukturach obiektowych jak *grona* (ang. *clusters*) i *kapsuły* (ang. *capsules*). Postulaty odnośnie tej specyfikacji stanowią sedno rekomendacji RM-ODP jeśli chodzi o architekturę, zestaw podstawowych usług oraz poziomy transparentności środowiska rozproszonego. Dlatego tej części poświęcimy więcej miejsca w kolejnych punktach niniejszej pracy.

3.5. Perspektywa technologiczna

Perspektywa technologiczna (ang. *Technology viewpoint*) definiuje system ODP jako zbiór obiektów reprezentujących zarówno elementy sprzętowe jak i programowe. Ma ona typowo implementacyjny charakter i w swojej treści musi odnosić się do konkretnych technologii i narzędzi informatycznych zastosowanych do tworzenia systemu ODP. Poziom abstrakcji w przypadku tej specyfikacji znacznie odbiega od pozostałych. Uwypuklają się tu wszystkie ograniczenia związane z kosztami i dostępnością poszczególnych elementów systemu. Specyfikacja technologiczna stanowi połączenie między specyfikacjami wysokiego poziomu, dotyczącymi poszczególnych perspektyw systemu ODP, a rzeczywistymi technologiami informatycznymi.

4. Szkielet architektury RM-ODP

Norma X.903 w części poświęconej *językowi perspektywy inżynierskiej* (ang. *engineering language*) wprowadza szereg rodzajów obiektów składających się na architekturę systemu. System ODP stanowi zespół obiektów współdziałających ze sobą poprzez swoje interfejsy.

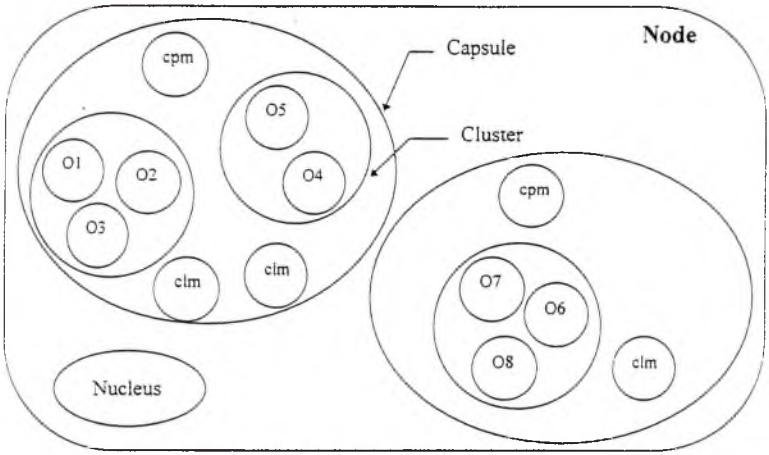
Można wyróżnić trzy schematy organizacji, zależności i współdziałania między obiektami:

- schemat węzła systemu ODP;
- schemat kanału komunikacyjnego między obiektami;
- schemat aplikacji rozproszonej.

W ramach schematu węzła ODP wyróżnia się następujące typy obiektów:

- *węzeł* (ang. *Node*) - autonomicznie zarządzany element sprzętowo-programowy, reprezentujący na poziomie obiektowym jednostkę przetwarzającą systemu rozproszonego wraz z jej zasobami;
- *jądro* (ang. *Nucleus*) - obiekt zarządzający węzłem, odpowiedzialny za alokację zasobów, zarządzanie obiektami i komunikację, reprezentujący oprogramowanie operacyjne jednostki przetwarzającej;
- *kapsuła* (ang. *Capsule*) - najmniejsza chroniona część systemu, grupująca obiekty współdziałające ze sobą w ramach konkretnej dziedziny przedmiotowej, najczęściej reprezentowana przez proces z własnym obszarem adresowym i wątkiem wykonania;
- *zarządca kapsuły* (ang. *Capsule manager*) - pełni funkcje zarządzające w stosunku do obiektów zawartych w kapsule;

- *grono* (ang. *Cluster*) - grupa obiektów wewnątrz kapsuły, dająca się wspólnie manipulować, tzn. składować, wykonywać operacje zapamiętywania punktów kontrolnych, odtwarzania stanu itp.;
- *zarządca grona* (ang. *Cluster manager*) - obiekt zarządzający wewnątrz grona;
- *podstawowy obiekt inżynierski* (ang. *Basic engineering objects*) - najmniejsza autonomiczna część systemu oferująca określone usługi poprzez wyspecyfikowany interfejs.



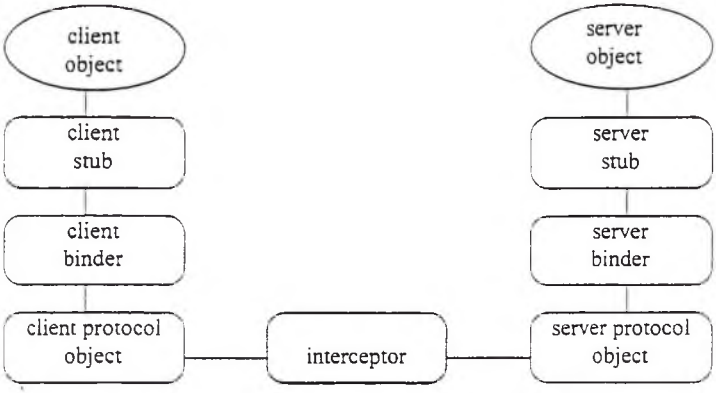
Rys.1. Schemat węzła systemu ODP

Rysunek 1 obrazuje relacje między podstawowymi rodzajami obiektów, pomijając odwołania między nimi. Odwołania możliwe są między dwoma lub większą liczbą autonomicznych obiektów poprzez specjalnie do tego celu zestawiane *kanały komunikacyjne* (ang. *channels*). Są to odwołania typu klient-serwer (ang. *client-server*). Kanały są jedyną formą komunikacji między podstawowymi obiektami inżynierskimi nawet jeśli dotyczą interakcji w ramach jednego grona. Oczywistym jest fakt, że koszty komunikacji w ramach grona będą najniższe, wyższe w ramach kapsuły i węzła, a najwyższe w ramach całego systemu ODP. Nie mniej jednak interakcja między obiektami będzie przebiegała zawsze według tego samego schematu.

Ze względu na schemat kanału komunikacyjnego możemy wyróżnić kolejne rodzaje obiektów:

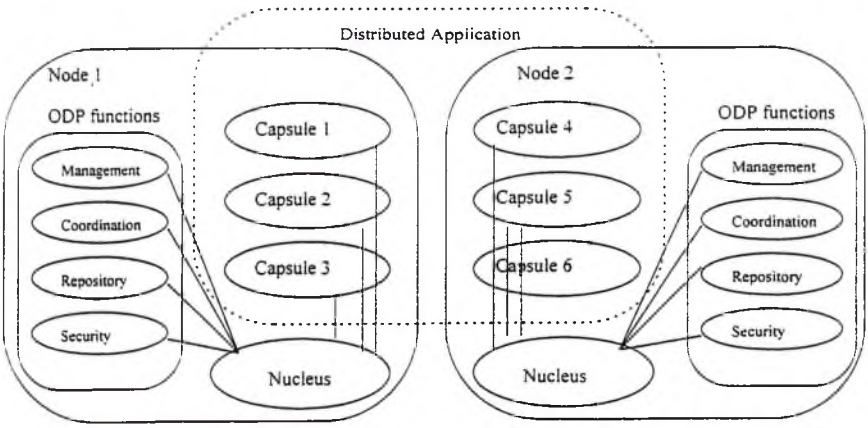
- *obiekty dopasowujące* (ang. *Stub*) - są odpowiedzialne za udostępnianie interfejsu podstawowego obiektu inżynierskiego i wprowadzają poziom niezależności między interfejsem obiektu a jego zachowaniem (ang. *behaviour*);
- *obiekty łączące* (ang. *Binder*) - rozwiązują problemy związane z rozproszeniem i są odpowiedzialne za nawiązanie łączności i utrzymanie kanału komunikacyjnego;
- *obiekty do obsługi protokołów komunikacyjnych* (ang. *Protocol object*) - są odpowiedzialne za obsługę komunikacji na poziomie protokołów komunikacyjnych;

- *obiekty translacji protokołów* (ang. *Interceptor*) - są odpowiedzialne za ewentualną translację protokołów komunikacyjnych w środowiskach, gdzie występuje zróżnicowanie protokołów.



Rys. 2. Schemat kanału interakcji między obiektami

Na rysunku 2 przedstawiono odwołanie typu klient-serwer jedynie między dwoma obiektami. Kanał komunikacyjny może być jednak zestawiany między większą ich liczbą. Również w zależności od sytuacji, niektóre warstwy mogą być pominięte, np.: obiekt translacji protokołów (w sytuacji, gdy środowisko rozproszone obsługiwane jest przez jeden protokół komunikacyjny), obiekt do obsługi protokołu komunikacyjnego (w sytuacji, gdy odwołania występują w obrębie węzła). Obiekty łączące pełnią rolę najwyższej warstwy komunikacyjnej i nie są nigdy pomijane, gdyż to one przeprowadzają proces odwołań między podstawowymi obiektami inżynierskimi.



Rys. 3. Schemat rozproszonej aplikacji ODP

Trzeci z rysunków obrazuje model działania aplikacji rozproszonej. Na aplikację może składać się wiele kapsuł rozproszonych po wielu węzłach. Usługi systemowe ODP zapewnia jądro, które jednocześnie obsługuje niskopoziomową komunikację w ramach systemu rozproszonego.

5. Funkcje ODP

Jak już wspomniano, model RM-ODP systematyzuje funkcje systemowe ODP. Są to usługi, z których (jak pokazano na Rys. 3) korzystają obiekty jądra w celu zarządzania zasobami węzłów.

Norma X.903 wyróżnia cztery podstawowe grupy funkcji:

- *grupa funkcji zarządzania* (*Management functions*) - obejmująca zarządzanie:
  - węzłami (zarządzanie wątkami, zegarami i licznikami, tworzeniem kanałów i lokalizacją interfejsów, tworzeniem i usuwanie kapsuł),
  - obiektami,
  - gronami (tworzenie punktów kontrolnych, usuwanie, dezaktywacja grona, obsługa awarii, reaktywacja grona, start po awarii, migracja),
  - kapsułami (tworzenie gron obiektów, usuwanie kapsuł);
- *grupa funkcji koordynacyjnych* (ang. *Coordination functions*):
  - zgłaszanie zdarzeń (ang. *Event notification functions*),
  - tworzenie punktów kontrolnych i odtwarzanie stanu po awarii (ang. *Checkpoint and recovery function*),
  - dezaktywacja i reaktywacja kapsuł i gron (ang. *Deactivation and reactivation functions*),
  - operacje grupowe (ang. *Group function*),
  - replikacja obiektów (ang. *Replication function*),
  - migracja obiektów (ang. *Migration function*),
  - transakcje (ang. *Transaction function*),
  - monitorowanie interakcji między obiektami (ang. *Engineering interface reference tracking function*);
- *grupa funkcji magazynowania* (ang. *Repository functions*):
  - składowania (ang. *Storage function*),
  - organizacji informacji (ang. *Information organization function*),
  - relokacji (ang. *Relocation function*),
  - składowania typów (ang. *Type repository function*),
  - udostępniania interfejsów (ang. *Trading functions*);
- *grupa funkcji bezpieczeństwa* (ang. *Security functions*):
  - kontroli dostępu (ang. *Access control function*),
  - monitorowania i gromadzenia informacji o realizowanych dostępach (ang. *Security audit function*),
  - identyfikacji i uwierzytelniania (ang. *Authentication function*),
  - zabezpieczania przed nieautoryzowanym utworzeniem, modyfikacją lub usunięciem danych (ang. *Integrity function*).

6. Poziomy transparentności w systemach ODP

Wyróżniono następujące poziomy transparentości:

- *dostępu* (ang. *Access transparency*) - oferowanie jednolitego dostępu do zasobów niezależnie od reprezentacji danych i faktu rozproszenia;
- *awarii* (ang. *Failure transparency*) - ukrycie dla poziomu obiektów samej awarii jak i mozliwej do wykonania sekwencji odtwarzającej, w celu wywołania złudzenia bezawaryjnej pracy systemu;
- *lokalizacji* (ang. *Location transparency*) - przesłanianie lokalizacji obiektów;
- *migracji* (ang. *Migration transparency*) - podejmowanie decyzji o najkorzystniejszej lokalizacji obiektu;
- *de- i reaktywacji* (ang. *Persistence transparency*) - ukrywanie przed obiektem efektu de- lub reaktywacji obiektów;
- *relokacji* (ang. *Relocation transparency*) - ukrywanie efektów relokacji;
- *replikacji* (ang. *Replication transparency*) - ukrywanie faktu replikacji zasobów w celu zwiększenia efektywności dostępu do nich;
- *transakcji* (ang. *Transaction transparency*) - ukrywanie zmian w konfiguracji obiektów w celu zachowania spójności działania systemu.

7. Podsumowanie

Zasadniczym celem prac nad modelem RM-ODP była standaryzacja zagadnień związanych z przetwarzaniem rozproszonym na poziomie konceptualnym. W tym kontekście uwidacznia się rola systematyzująca modelu w takich kwestiach jak cechy, funkcje oraz transparentność środowisk rozproszonych. Tym co wyróżnia koncepcje zawarte w modelu RM-ODP od innych, jest wprowadzenie pięciu perspektyw postrzegania systemu ODP, istotnych na etapie analizy, specyfikacji i projektowania systemu. Ważnym elementem modelu jest też zdefiniowanie szkieletu architektury systemów otwartego przetwarzania rozproszonego. O zgodności modelu RM-ODP z najnowszymi trendami w dziedzinie wytwarzania oprogramowania decyduje wykorzystywanie technik obiektowych.

W niniejszej pracy omówiono głównie zagadnienia zebrane w dokumentach X.901 i X.903. Dokument X.902 wprowadza bazę pojęciową dla X.903, natomiast dokument X.904 zawiera szereg formalizmów dotyczących języków specyfikacji poszczególnych perspektyw. Ze względu na ograniczone ramy niniejszej pracy, dokumenty X.902 i X.904 nie zostały tu szerzej omówione.

Literatura

[1] Jerzy Brzeziński „Problemy przetwarzania rozproszonego"
Materiały konferencyjne „Miejskie Sieci Komputerowe w Nauce i Gospodarce"
POLMAN'94, Poznań, 1994, str. 173-187

[2] Zbigniew Huzar „Wprowadzenie do norm dotyczących modelu odniesienia ODP (Otwartego Przetwarzania Rozproszonego)"
FTP serwer: ftp.ci.pwr.wroc.pl/apps/network/odp

[3] ITU-T X.901 IOS/IEC 10746-1 ODP Reference Model Part 1. Overview
Draft International Standard (DIS) output from the Editing meeting in Helsinki (Finland), 15-18 May 1995
dokumenty HTML: http://www.dstc.edu.au

[4] ITU-T X.902 | ISO/IEC 10746-2 ODP Reference Model Part 2. Fundations
International Standard. ITU-T Recomendation. 1995
dokumenty HTML: http://www.dstc.edu.au

[5] ITU-T X.903 | ISO/IEC 10746-3 ODP Reference Model Part 3. Architecture
International Standard. ITU-T Recomendation. Geneve. 1995
dokumenty HTML: http://www.dstc.edu.au

[6] ITU-T X.904 ISO/IEC 10746-4 ODP Reference Model Part 3. Architectural Semantics Amendment
Working Document ISO/IEC CS21 N9818. 1995
dokumenty HTML: http://www.dstc.edu.au

[7] Kerry Raymond „Reference Model of Open Distributed Processing (RM-ODP): Introducion"
University of Queensland. Brisbane, Australia
e-mail: kerry@dstc.edu.au

Zastosowanie technologii magazynów danych do zarządzania sieciami komputerowymi

Jerzy Brzeziński, Tomasz Koszlajda

Naukowa i Akademicka Sieć Komputerowa JBR

1. Wprowadzenie

Współcześnie konstruowane sieci komputerowe stają się coraz bardziej złożone i w konsekwencji nabiera znaczenia problem efektywnego zarządzania nimi. Podstawą poprawnego i efektywnego zarządzania siecią jest pełna i rzetelna informacja o bieżącym stanie sieci i zachodzących w niej procesach. Efektywny dostęp do informacji o wszystkich elementach sieci wymaga ich gromadzenia w systemie bazy danych, nazywanej *bazą informacji zarządzania*, w skrócie *MIB* (ang. *Management Information Base*). Jakość zarządzania jest zależna od wierności i pełności opisu zasobów sieci komputerowej przez dane w bazie danych oraz poprawności i efektywności mechanizmów gromadzenia i dostępu do tych danych [1], [6], [15].

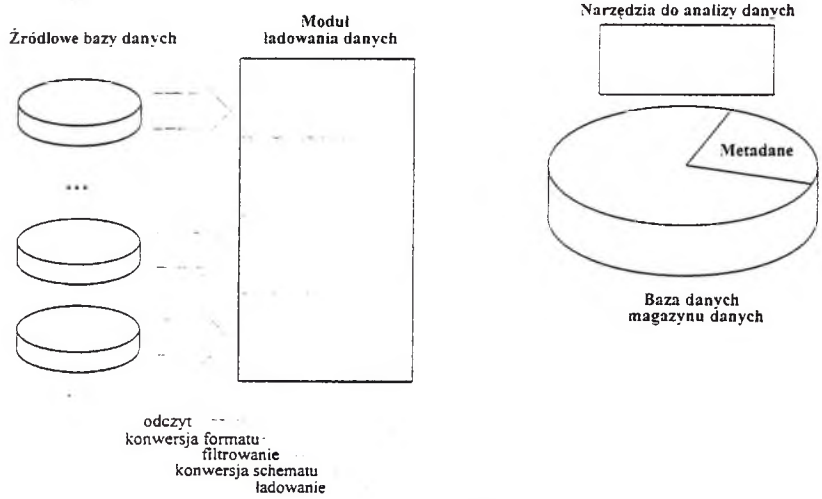
Architektura bazy danych MIB jest w pełni rozproszona, a ze względu na równoległe stosowanie kilku standardów określających architekturę, strukturę i funkcje danych MIB, jest to również heterogeniczna baza danych. Procesy zarządzania siecią komputerową muszą więc wykorzystywać rozproszone algorytmy pozyskiwania informacji o stanie różnych elementów sieci. Ponadto dostęp do danych zarządzania wymaga bezustannej translacji między różnymi standardami danych. Przyczynia się to do skomplikowania i spowolnienia procesów zarządzania.

Problemy związane z przetwarzaniem rozproszonych i heterogenicznych baz danych MIB mogą zostać rozwiązane przez zastosowanie technologii magazynowania danych. Zreplikowanie i integracja danych zarządzania różnych elementów sieci komputerowej w scentralizowanym magazynie danych pozwolą na uproszczenie algorytmów pozyskiwania danych zarządzania. Ponadto, zastosowanie w pełni funkcjonalnego systemu bazy danych zwiększy wydajność procesu przetwarzania tych danych, na przykład dzięki zastosowaniu bardziej wydajnych fizycznych struktur danych, lub wykorzystaniu narzędzi do wielowymiarowej statystycznej analizy danych.

2. Technologia magazynowania danych

Magazynowanie danych (ang. *warehousing*) jest techniką stosowaną do integrowania danych z rozproszonych, autonomicznych i najczęściej heterogenicznych źródeł informacji. *Magazyn danych* (ang. *data warehouse*) jest kolekcją zintegrowanych danych i zbiorem programowych modułów służących do przetwarzania i zarządzania tymi danymi [7], [16]. Magazyny danych są szczególnym rodzajem systemów baz danych, wyspecjalizowanych w złożonej analizie bardzo dużych wolumenów danych. Do implementacji magazynów danych najczęściej są wykorzystywane odpowiednio zmodyfikowane wersje relacyjnych systemów baz danych [17].

Architektura magazynu danych obejmuje źródłowe bazy danych, moduł przetwarzania i ładowania danych, właściwy magazyn danych, oraz zbiór narzędzi przeznaczonych do analizy danych. Architektura magazynu danych została zilustrowana na rysunku 1.



Rys. 1. Architektura magazynu danych

Rolę źródłowych baz danych dla magzynu danych pełnią zarówno w pełni funkcjonalne systemy baz danych, jak również proste aplikacje pozbawione zewnętrznego programowego interfejsu dostępu do danych. Przeznaczeniem modułu przetwarzania i ładowania danych jest:

- automatyczne pozyskiwanie danych z różnych źródłowych baz danych;
- konwersja wewnętrznej reprezentacji pozyskanych danych do formatu danych w magazynie danych;
- odfiltrowanie nadmiarowych i błędnych danych;
- przetworzenie danych do postaci zgodnej z modelem pojęciowym i logicznym magazynu danych;

- załadowanie danych do magazynu danych z uwzględnieniem ograniczeń integralnościowych zdefiniowanych w magazynie danych.

Baza danych magazynu danych oprócz danych pozyskanych ze źródłowych baz danych zawiera również zbiór *metadanych*. Metadane są to informacje opisujące:

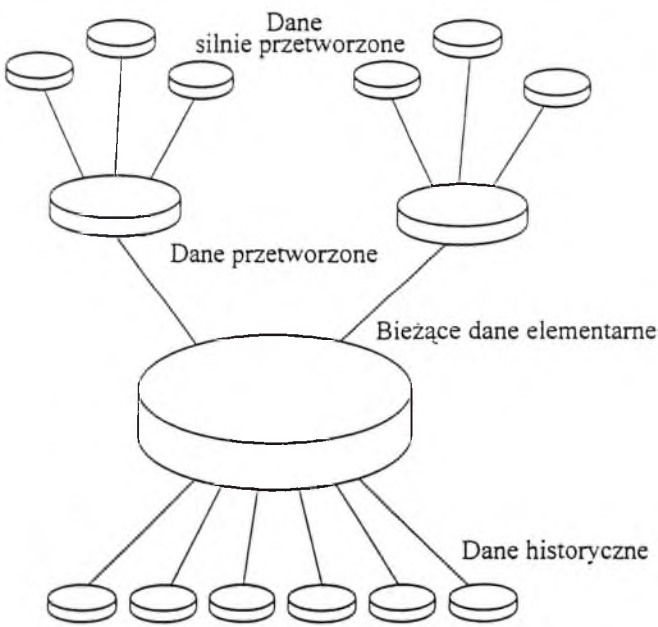
- strukturę danych magazynu danych;
- algorytmy przetwarzania danych źródłowych do postaci zgodnej z modelem pojęciowym i logicznym magazynu danych;
- algorytmy służących do tworzenia danych sumarycznych.

Narzędzia analizy danych służą do przetwarzania danych magazynu danych: ich graficznej wizualizacji, tworzenia raportów, wspomagania procesu podejmowania decyzji.

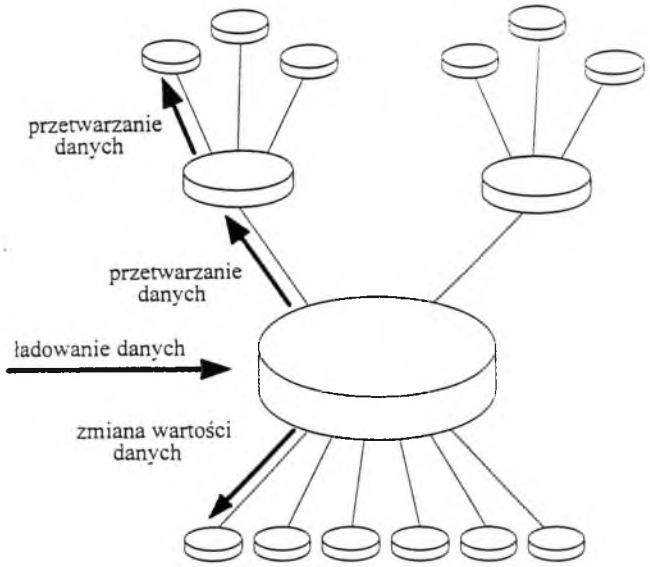
W magazynie danych przechowywane są trzy podstawowe kategorie danych [4]:

- dane elementarne równoważne pozyskiwanym danym źródłowym;
- dane historyczne tworzone w momencie pojawiania się nowych wartości już przechowywanych danych;
- dane sumaryczne o różnym stopniu przetworzenia.

Dane raz umieszczone w magazynie danych nie są usuwane, lecz podczas swojego pobytu w magazynie danych przechodzą różne fazy istnienia, w wyniku przesuwania ich między wymienionymi powyżej kategoriami danych. Strukturę danych magazynu danych zilustrowano na rysunku 2 ([4]), a cykl życia tych danych przedstawiono na rysunku 3.



Rys. 2. Struktura danych w magazynie danych



Rys. 3. Przepływ danych w magazynie danych

W klasycznych zastosowaniach baz danych powszechnie stosuje się *model bezpośredniego przetwarzania transakcji* (ang. *On-Line Transaction Processing - OLTP*). W modelu tym zbiór operacji przetwarzania danych obejmuje: wstawianie, modyfikowanie, usuwanie i odczytywanie danych. Konsekwencją przyjęcia takiego modelu jest stosowanie w klasycznych systemach baz danych określonych algorytmów zarządzania współbieżnością transakcji, na przykład algorytmów blokowania dwufazowego. W magazynach danych przyjęto odmienny model przetwarzania danych - *bezpośredniej analizy danych* (ang. *On-Line Analytical Processing - OLAP*). Zbiór operacji przetwarzania danych w tym modelu, zawiera jedynie dwie operacje: wstawiania i odczytu danych. Upraszcza to znacznie algorytmy zarządzania współbieżnością transakcji i w konsekwencji zwiększa wydajność przetwarzania danych.

3. Baza informacji zarządzania

Baza informacji zarządzania (MIB) zawiera dane opisujące stan oraz stałe i modyfikowalne parametry zasobów sieciowych podlegających procesowi zarządzania. Na bazę tę składają się dane związane z poszczególnymi elementami sieci, przeznaczone do lokalnego zarządzania tymi elementami. Można wyróżnić trzy kategorie danych przechowywanych w MIB: dane konfiguracyjne, dane sterujące i dane pomiarowe [3].

- *Dane konfiguracyjne* są kolekcją statycznych lub rzadko modyfikowanych informacji o bieżącej konfiguracji sieci. Opisują one na przykład: topologię sieci, łącza (ang. trunks), przełącznice (ang. switches), usługi sieciowe (ang. network services) lub klucze kodowania danych. Ze względu na złożoną strukturę sieci dane konfiguracyjne również charakteryzują się dużą złożonością strukturalną. Ta kategoria danych jest podstawą dla zarządzania konfiguracją sieci, kontrolą dostępu i usługami sieciowymi.

  Dla rozbudowanych rozległych sieci komputerowych wolumen danych konfiguracyjnych może osiągać rozmiar do kilku gigabajtów ([13]). Większość danych konfiguracyjnych jest składowana w MIB w momencie inicjacji systemu i jest modyfikowana w odpowiedzi na takie zdarzenia jak dodanie (lub usunięcie) nowego węzła sieci, połączenia lub usługi sieciowej.

- *Dane sterujące* są kolekcją danych opisujących bieżące nastawy parametrów umożliwiających strojenie sieci. Do tej grupy danych należą na przykład parametry określające maksymalne przepływy na poszczególnych łączach, proporcje podziału obciążenia sieci na wyjściach przełącznic lub tablice marszrutyzacji. Oprócz bieżących nastaw parametrów, ta kategoria danych obejmuje również alternatywne zestawy nastaw dla różnych obciążeń i konfiguracji sieci. Na przykład, MIB może zawierać dwa zestawy nastaw: dla obciążenia dziennego i nocnego.

  Dane sterujące są wykorzystywane do zarządzania wydajnością pracy i obsługą awarii sieci. W związku z tym, dane te mogą być modyfikowane wielokrotnie w ciągu dnia w celu uwzględnienia charakteru *ruchu* w sieci lub występujących awarii.

- *Dane pomiarowe* opisują dynamicznie zmieniający się stan sieci. Przykładem takich danych są długości kolejek na poszczególnych węzłach sieci, stany łączy lub współczynniki retransmisji danych. Wszystkie te dane są zbierane przez procesy monitorowania sieci. Są one podstawą do określenia stopnia wykorzystania i operacyjnej jakości sieci. Dane pomiarowe są podstawowymi danymi wejściowymi dla modułów zarządzania wydajnością pracy sieci, obsługą awarii i rozliczaniem obsługi klientów sieci. Szacuje się, że w rozbudowanych sieciach wolumen danych pomiarowych może przyrastać o 20 do 30 gigabajtów dziennie ([13]).

  Dane pomiarowe można podzielić na dwie grupy ze względu na czas ich utrzymywania w bazie danych. Do danych trwałych, to jest danych utrzymywanych przez okres wielu tygodni lub miesięcy, należą informacje o sumarycznym obciążaniu sieci przez poszczególnych klientów, o próbach naruszenia autoryzacji dostępu lub innych sytuacjach alarmowych. Z kolei do danych krótkotrwałych, to jest utrzymywanych w ciągu godzin lub pojedynczych dni, należą dane opisujące dynamiczną charakterystykę pracy sieci. W danym momencie oprócz bieżącego zbioru danych pomiarowych utrzymywane są również historyczne wersje tych danych, dla celów analizy efektywności pracy systemu i występujących w nim awarii.

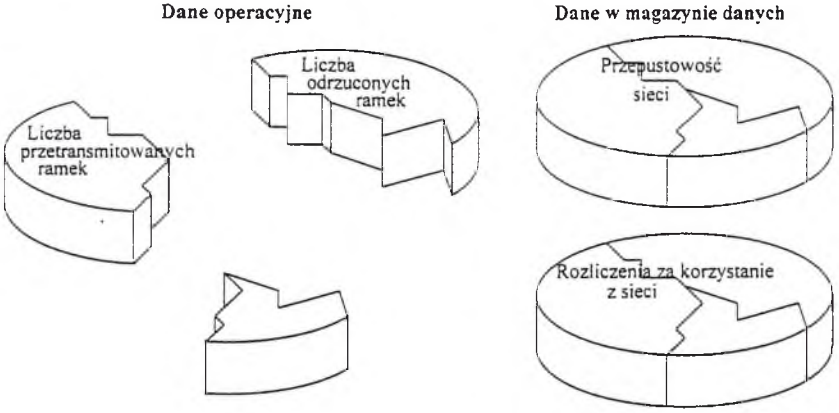
Mimo daleko posuniętej standaryzacji, rozległe sieci komputerowe są zazwyczaj systemami heterogenicznymi. Elementy składowe poszczególnych podsieci pochodzą często od różnych dostawców, co powoduje, że różnią się one często protokołami komunikacyjnymi, architekturą i implementacją poszczególnych warstw lokalnego systemu zarządzania. W związku z tym, dla uproszczenia architektury globalnego

systemu zarządzania postuluje się wprowadzenie wspólnego modelu danych dla opisu danych zarządzania. Szerzej rozpowszechnione są dwie propozycje takiego standardu. Bazują one na pojęciu tak zwanych *obiektów zarządzania*, które są abstrakcyjną reprezentacją fizycznych zasobów sieci komputerowej. Pierwszy z proponowanych modeli został opracowany przez komitet standaryzacyjny *ISO*. Model ten jest w pełni obiektowo-zorientowany. Obiekty zarządzania są w nim obiektami w rozumieniu paradygmatu obiektowego. Drugi model został opracowany przez *Internet Activity Board* (*IAB*). W modelu tym obiekty zarządzania są implementowane przez zmienne atomowe lub strukturalne, takie jak listy lub tablice ([2], [5]).

4. Zastosowanie magazynu danych do zarządzania siecią komputerową

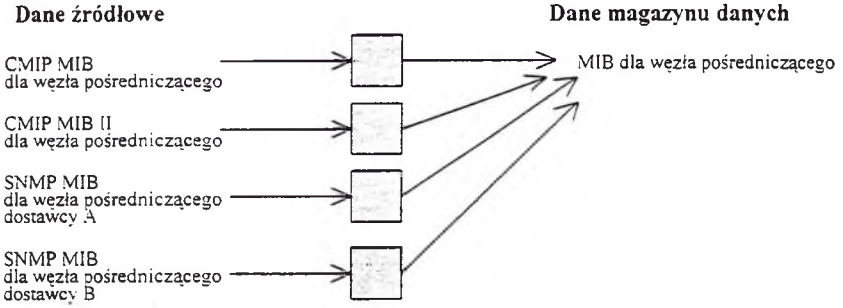
Specyficzne własności magazynów danych, takie jak integrowanie danych pochodzących z heterogenicznych źródłowych baz danych, tematyczne zorientowanie przechowywanych danych lub możliwość składowania danych wielowymiarowych obejmujących na przykład charakterystykę czasową danych, pozwalają na uwzględnienie podstawowych wymagań procesu globalnego zarządzania sieciami komputerowymi.

Dane zarządzania związane z poszczególnymi elementami sieci komputerowej mają charakter operacyjny. Służą one do lokalnego zarządzania danym urządzeniem. Dane te muszą być odpowiednio odfiltrowane i przetworzone przed ich wykorzystaniem przez procesy globalnego zarządzania siecią. Moduły ładowania magazynów danych umożliwiają wstępne odfiltrowanie i przetworzenie danych zarządzania pobieranych z tych urządzeń. Zastosowanie mechanizmu perspektyw (ang. view) i dalsze przetworzenie tych danych pozwala przygotować dane do postaci właściwej dla procesów globalnego zarządzania siecią. Mówimy, że dane w magazynie danych są ukierunkowane tematycznie.



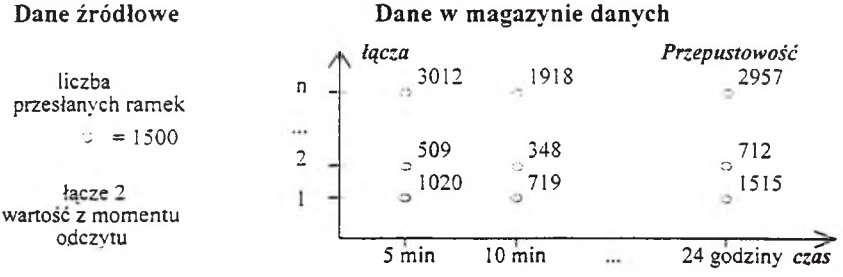
Rys 4. Tematyczne ukierunkowanie magazynu danych

Informacje zarządzania związane z różnymi elementami sieci komputerowej, pochodzącymi często od różnych dostawców, różnią się sposobem prezentacji na poziomie pojęciowym, logicznym i fizycznym ([9], [10], [11], [12]). Bezpośrednie odwoływanie się do tych danych przez procesy zarządzania wymaga nieustannej translacji między różnymi standardami reprezentacji. Zastosowanie magazynu danych pozwala na sprowadzenie tych danych źródłowych do wspólnej reprezentacji przed ich wykorzystaniem przez procesy zarządzania.



Rys. 5. Integracja heterogenicznych i rozproszonych źródeł danych

Lokalne bazy danych MIB związne z poszczególnymi urządzeniami sieciowymi opisują zazwyczaj jedynie bieżący stan danego urządzenia. Natomiast dla podjęcia racjonalnych decyzji zarządzania dotyczących na przykład wydajności sieci, usunięcia skutków awarii, lub związanych z rozliczeniami za korzystanie z sieci, niezbędna jest informacja nie tylko o aktualnym stanie sieci, ale również o dynamice zmian podstawowych parametrów sieci. Zastosowanie technologii magazynów danych umożliwiającej definiowanie danych wielowymiarowych, uwzględniających wymiar czasu, lokalizacji, użytkowników sieci, udostępni procesom zarządzania lepszą jakościowo i pełniejszą informację o stanie sieci komputerowej.



Rys. 6. Wielowymiarowość danych

5. Podsumowanie

Celem zastosowania technologii magazynów danych do reprezentacji danych zarządzania jest dostarczenie procesom zarządzania sieciami komputerowymi bogatszej, pełniejszej i bardziej dostępnej informacji o stanie podstawowych parametrów sieci. Umożliwia to bardziej racjonalne podejmowanie decyzji zarządzania. Ponadto, zastąpienie rozproszonej i heterogenicznej bazy danych MIB przez jednorodny i scentralizowany magazyn danych pozwala na znaczne uproszczenie algorytmów dostępu do danych zarządzania, co ułatwia konstrukcję programów zarządzania, pozwala na bardziej wydajny dostęp do danych i ogranicza źródła powstawania błędów.

Otwartym problemem do rozwiązania pozostaje zdefiniowanie modelu spójności danych w magazynie danych właściwego dla problemów zarządzania sieciami komputerowymi. Dotychczasowe zastosowania magazynów danych są adresowane do wspomagania procesu podejmowania decyzji ekonomicznych, gdzie model spójności danych jest bardzo uproszczony. Zdefiniowanie nowego modelu spójności wiąże się również z potrzebą zaprojekowania odpowiednich algorytmów zapewnienia spójności.

Literatura

1 Bapat, S., *OSI Management Information Base Implementation*, Integrated Network Management, II, eds. I. Krishnan i W. Zimmer, Elsevier Science Publishers B.V. (North-Holland), 1991.

2 Chernick, M., et al, *A survey of OSI network management standards activities*, Tech. Report NMSIg87/16 ICST-SNA-87-01, National Bureau of Standards, 1987.

3 Haritsa J., et al, *Design of the MANDATE MIB*, Integrated Network Management, III, eds. H. Hegering i Y. Yemini, Elsevier Science Publishers B.V. (North-Holland), 1993.

4 Inmon W.H. *What is Data Warehouse ?*. PRISM Volume 1 No.1 1995

5 Klerer, S., *The OSI Management Architecture: an Overview*, IEEE Network Magazine, 2(2), March 1988.

6 Koszlajda T., Brzeziński J. *Analiza związków modelu zarządzania OSI z systemami obiektowych baz danych*, seminarium NASK - Miedzeszyn, maj 1995

7 Koszlajda T., Morzy T. *Integracja heterogenicznych rozproszonych baz danych z zastosowaniem magazynu danych*, Materiały konferencji: Miejskie Sieci Komputerowe w Nauce, Gospodarce i Administracji POLMAN'96, Poznań, kwiecień 1996

8 Nakai S., *MIB Design for Network Management Transaction Processing*, Integrated Network Management, III, eds. H. Hegering i Y. Yemini, Elsevier Science Publishers B.V. (North-Holland), 1993.

9 Network Management Forum, Forum 026: *Translation of Internet MIBs to ISO/CCITT GDMO MIBs*, Issue 1.0, October 1993

10 Network Management Forum, Forum 029: *Translation of Internet MIB-II to ISO/CCITT GDMO MIBs*, Issue 1.0, October 1993

11 Network Management Forum, Forum 030: *Translation of ISO/CCITT GDMO MIBs to Internet MIBs*, Issue 1.0, October 1993

12 Network Management Forum. Forum 026: *ISO/CCITT to Internet Management Proxy*. Issue 1.0. October 1993
13 SPRINT Network Management Center. Virginia. Site Visit. Aprii 1992.
14 Terplan. K.. *Communications Network Management*. Prentice-Hall. 1992.
15 Valta. R.. *Design concepts for a Global Network Management Database*. ntegrated Network Management. II. eds. I. Krishnan i W. Zimmer. Elsevier Science Publishers B.V. (North-Holland), 1991.
16 Zhuge Y.. Garcia-Molina H., et al *View Maintenance in a Warehousing Environment*. ACM 1995
17 *Specialized Requirements for Relational Data Warehouse Servers*. Red Brick Systems. September 1995

DOSTOSOWANIE BAZY X.500 DO SPECYFIKI JĘZYKA LOKALNEGO *

Maja Górecka
Maja.Gorecka@cc.uni.torun.pl

Ogólnouczelniany Ośrodek Obliczeniowy

Tomasz Wolniewicz
twoln@mat.uni.torun.pl

Wydział Matematyki i Informatyki

1 Wstęp

Celem niniejszego artykułu jest przedstawienie problemów związanych z eksploatacją bazy danych o międzynarodowym zasięgu. Od kilku lat koordynujemy usługę X.500 Directory w Polsce i przedstawiamy doświadczenia i przemyślenia zdobyte w trakcie tej pracy.

Artykuł prezentuje założenia teoretyczne, jak również opisuje sposób zaimplementowania ich w praktyce w interfejsie WWW.

2 Specyfika bazy międzynarodowej

Baza typu X.500 jest systemem pozwalającym na gromadzenie szeroko rozumianej informacji adresowej o osobach i instytucjach. W założeniach informacja jest udostępniana całemu światu (w pewnych sytuacjach z ograniczeniami narzuconymi m.in. koniecznością ochrony lokalnych danych). Główny problem związany z dostępem do bazy pojawia się po zauważeniu, że użytkownicy dzielą się na dwie kategorie: użytkowników posługujących się tym samym językiem co obszar, którego dotyczą dane (język ten nazywamy lokalnym) i użytkowników obcojęzycznych.

Podstawowe zagadnienie, z którym mamy do czynienia to język udostępnienia danych. Problemem jest zarówno sam język, jak i specyficzne znaki stosowane w pisowni.

2.1 Udostępnianie informacji w języku lokalnym

Dane w języku lokalnym są zazwyczaj wystarczające w celu zaadresowania listu lub wybrania innej formy kontaktu. Dotyczy to zarówno użytkownika lokalnego jak i obcojęzycznego. Problemem może być jednak graficzna prezentacja informacji (znaków diakrytycznych). Użytkownik obcojęzyczny na ogół zakłada, że znaki diakrytyczne są zbędnym balastem, utrudniają mu odczytanie, napisanie i zapamiętanie nazwy. Użycie nazwy bez tych znaków zazwyczaj

*Autorzy pragną w tym miejscu podziękować mgr. inż. Jerzemu Żenkiewiczowi, który z ramienia NASK koordynuje prace w zakresie X.500, za kilkuletnią współpracę i wsparcie naszych działań. Panu prof. Jerzemu Brzezińskiemu dziękujemy za pomoc w zakresie teorii baz danych i uspójnienie naszej wiedzy. Poparcie NASK umożliwiało nam prowadzenie prac oraz branie udziału w europejskich spotkaniach koordynacyjnych X.500

i tak pozwoli na skomunikowanie sie. Powodów takiego stanu rzeczy należy szukać w niedostatecznym rozwoju technik komputerowych, przyczynia się do tego dominacja języka angielskiego. Stosowanie stron kodowych o pojemności zaledwie 256 znaków i kodowanie znaków zgodnie z rozkładem wybranej strony doprowadza do sytuacji, w której prawidłowa interpretacja tekstu może być niemożliwa. Brak odpowiedniej standaryzacji, na przykład wielość formatów Latin II, wprowadza dodatkowe utrudnienia.

Niewatpliwie docelowo komputerowe środowisko pracy będzie udostępniało pełny zestaw znaków, służa temu różne metody kodowania niezależne od strony kodowej (Unicode, SGML entities, standard T.61). Wydaje się jednak, że chwila ta jest od nas odległa jeszcze o kilka lat i należy starać się, aby już teraz poprawić sytuację tam, gdzie to jest możliwe za pomocą dostępnych środków.

Pamiętając o specyfice wymagań użytkownika obcojęzycznego, musimy jednocześnie zwrócić uwagę, że dla użytkownika lokalnego znaki diakrytyczne są absolutnie niezbędne. Baza danych, która będzie myliła nazwiska *Makowski* i *Mąkowski* nie będzie mogła być w Polsce uznana za profesjonalne narzędzie. Uznacza to, że baza musi niezbędnie zawierać informacje w prawidłowym formacie, ale być może niekoniecznie udostępniać je wszystkim, gdyż, przykładowo, generowanie znaków zakodowanych w Latin II na ekranie Latin I, produkuje dane zafałszowane bardziej niż gdyby zostały one po prostu pozbawione znaków diakrytycznych.

2.2 Udostępnianie informacji obcojęzycznej

Poza nazwami własnymi, baza zawiera również informacje opisowe. Zresztą nawet same nazwy własne niosą na ogół pewną informację typu opisowego. Ta informacja musi być udostępniana użytkownikowi obcojęzycznemu, nie chodzi tutaj o sposób kodowania, a o język. Prowadzone są prace nad internacjonalizacją X.500 w taki sposób, aby serwery, wyposażone w odpowiednie oprogramowanie same generowały informację we właściwym języku. U postaw tego projektu leży założenie, ze dane byłyby wprowadzone w jednym formacie, prezentacja byłaby generowana na ich podstawie przez serwer. Wydaje się, że jest to interesujący pomysł, ale po pierwsze jest on dopiero w trakcie opracowywania, a po drugie nie jest oczywiste, czy oferowane przez niego rozwiązania będą zadowalające. Na przykład dowolne tłumacznie nazwy firmy na obcy język może być niedopuszczalne dla danej firmy, gdyż na ogół posiada ona ustalona nazwę nie tylko lokalną, ale i w kilku obcych językach.

Wydaje się, że w obecnej sytuacji praktycznym rozwiązaniem jest dublowanie informacji w języku lokalnym i języku angielskim. Takie założenie zostało zaimplementowane w polskiej bazie X.500.

3 Specyfika struktury bazy danych X.500 a nazewnictwo

3.1 Hierarchia

Obiekty bazy X.500 uporządkowane są w strukturę hierarchiczną. Na szczycie tej struktury typowo umieszcza się państwa, na niższym poziomie instytucje, następnie ich podjednostki itd, aż do poziomu osób, pojedynczych obiektów (np. aplikacji komputerowych) itp.

3.2 Nazewnictwo

Każdy obiekt opisywany jest przez zestaw atrybutów, na ogół wielowartościowych. W typowej sytuacji jedna z wartości pewnego atrybutu jest wyróżniana jako właściwa nazwa obiektu. Taka nazwa musi być jedyna na danym poziomie hierarchii, ale może się pojawiać ponownie na innych poziomach. Obiekt opisywany jest za pomocą ciągu nazw kolejnych poziomów hierarchii bazy. W taki sposób pełna nazwa jest unikalna i zapewnia szybką lokalizację obiektu w bazie. Tak skonstruowaną nazwę określa się terminem *nazwy wyróżnionej*.

3.3 Sposoby dostępu do danych a język prezentacji

Typowy dostęp do adresowej bazy danych realizowany jest na jeden z dwóch sposobów:

1. przeglądanie
2. wyszukiwanie

Pierwsza metoda jest bardzo często preferowana. Użytkownik przegląda kolejne poziomy hierarchii organizacji aż dojdzie do danych, które go interesują. W tym podejściu użytkownik nie zawsze wie co chce znaleźć, przegląda informację, zatrzymując się w miejscach, które go zaciekawią.

Metoda przeszukiwania stosowana jest przez użytkownika, który stosunkowo dobrze wie czego szuka i zależy mu na szybkim otrzymaniu wyniku. Jeżeli dane do przeszukania są niedokładne, to możemy mieć do czynienia z połączeniem metody wyszukiwania i przeglądania, gdyż użytkownik będzie przeglądał listę wyników przeszukania, próbując odnaleźć dane, których potrzebuje.

Użytkownik stosujacy metodę przeglądania ma dostęp jedynie do głównych nazw obiektów i na ich podstawie musi sobie wyrobić zdanie o kolejnym etapie poszukiwań. W sytuacji kiedy mamy do czynienia z użytkownikiem obcojęzycznym, a nazwy główne są prezentowane w języku lokalnym, można spodziewać się problemów w zrozumieniu nazw, a prezentowanie ich z uwzględnieniem znaków diakrytycznych i za pomocą nieznanej strony kodowej może całkowicie uniemożliwić korzystanie z bazy.

Stosowanie metody przeszukania daje dostęp do większej gamy atrybutów, przykładowo Uniwersytet Mikołaja Kopernika w Toruniu jest reprezentowany przez wartość główną atrybutu o nazwie `organizationalName` równą `Uniwersytet Mikolaja Kopernika w Toruniu`, ale atrybut ten posiada również wartości:
`Uniwersytet Mikolaja Kopernika w Toruniu`, `Uniwersytet Mikolaja Kopernika`, `UMK`, `University of Torun`, `Nicholas Copernicus University in Torun`, `Nicholas Copernicus University`.
Oznacza to, że przeszukanie ze względu na `organizationalName=umk` odnajdzie ten obiekt, pomimo, że wartość `UMK` nigdy nie pojawi sie przy listach otrzymywanych z przeglądania.

Jako wynik wypisywania obiektów danego poziomu hierarchii lub przeszukania poddrzewa zaczynającego się od pewnego obiektu bazowego otrzymujemy listę zawierającą ciąg nazw wyróżnionych znalezionych obiektów. Na ogół z nazw wyróżnionych odcina się przedrostek będący nazwą obiektu bazowego. Wyprowadzenie ciągu nazw zwracanych przez operacje przeszukania lub wypisywanie danych bieżącego poziomu jest realizowane na podstawie algorytmów wbudowanych w eksploatowany system, bardzo to ogranicza możliwości stosowania różnych sposobów nazewnictwa, czy przetworzenia tej listy na zestaw odpowiednich łańcuchów czytelnych lokalnie.

4 Dostosowanie bazy X.500 do pracy dwujęzycznej

4.1 Założenia

Polski projekt usługi X.500 bazuje na oprogramowaniu QUIPU, które należy do pakietu ISODE, będącego implementacją protokołów OSI. QUIPU realizuje wszystkie protokoły zdefiniowane w ramach standardu X.500, dostarcza serwer bazy danych oraz oprogramowanie dające użytkowy dostęp do X.500.

Dopuszcza się pracę polskich serwerów X.500 w oparciu o oprogramowanie QUIPU w wersji ISODE-8.0 (edycja *public domain*) oraz IC (edycja dystrybuowana przez organizację Isode Consortium, udostępniana instytucjom akademickim na podstawie nieodpłatnej licencji). Wymaganie to jest niezbędne m.in. z powodu konieczności modyfikacji oprogramowania obsługi X.500 (serwer DSA oraz moduły biblioteczne) do potrzeb obsługi strony kodowej Latin II.

Zakłada się, że w celu dostosowania bazy X.500 do pracy w języku polskim stosowane będą wspólne tablice definiujące obiekty w ramach polskiego poddrzewa.

Dodatkowo przyjmujemy, że polscy użytkownicy będą korzystać z bazy za pomocą specjalnie przystosowanych interfejsów.

4.2 Struktura bazy

4.2.1 Model informacyjny

W bazie X.500 stosuje się specyfikacje CCITT ASN.1 (*Abstract Syntax Notation*) do definiowania struktur danych. Obiekty grupowane są w klasy i opisywane za pomocą ustalonych administracyjnie atybutów. W momencie definiowania atrybutu określa się reguły syntaktyczne, którym dany atrybut podlega. Pozwala to na kontrolę typu informacji przechowywanej w danym atrubucie, jak również właściwe jej interpretowanie.

Elementy bazy X.500, takie jak klasa obiektu czy atrybut, definiowane są w ASN.1 za pomocą typu zwanego identyfikatorem obiektu (`OBJECT IDENTIFIER`), który określa autorytatywnie nazwany obiekt. Identyfikatory te uporządkowane są w strukturę drzewa, mają postać ciągu nieujemnych liczb całkowitych, z których każda jest etykietą kolejnego węzła drzewa na drodze od korzenia do bieżącej pozycji. Postaci numerycznej opisującej węzeł towarzyszy na ogół krótki opis tekstowy.

System przyporządkowania identyfikatorów jest zestandaryzowany. Obecnie drzewo identyfikatorów obiektów ma trzy podstawowe gałęzie:

- `ccitt(0)`, administrowany przez CCITT;
- `iso(1)`, administrowany przez ISO/IEC;
- `joint-iso-ccitt(2)`, administrowany wspólnie przez ISO/IEC i CCITT.

co ASN.1 opisuje następująco:

```
ccitt           OBJECT IDENTIFIER ::= { 0 }
iso             OBJECT IDENTIFIER ::= { 1 }
joint-iso-ccitt OBJECT IDENTIFIER ::= { 2 }
```

Dalej np. na gałęzi `ccitt` zdefiniowano:

```
data            OBJECT IDENTIFIER ::= { ccitt 9 }
pss             OBJECT IDENTIFIER ::= { data  2342}
quipu           OBJECT IDENTIFIER ::= { pss 19200300 }
```

System taki pozwala na jednoznaczne przyporządkowanie identyfikatorów i delegowanie odpowiedzialności za administrowanie gałęziami drzewa identyfikatorów do organizacji krajowych i dalej do instytucji.

Po przydzieleniu gałęzi drzewa, instytucja lub kraj, ma pełną swobodę w definiowaniu swoich własnych elementów. Oczywiście lokalnie dodane klasy (czy atrybuty) nie będą interpetowane przez użytkowników nie mających dostępu do właściwych definicji (dzięki jednoznaczności nie zachodzi jednak niebezpieczeństwo interpretacji fałszywej). W standardzie X.500 (88) podstawowe identyfikatory rozpowszechniane są za pomocą statycznych tablic, w wersji 93 przewiduje się umieszczenie definicji w samym drzewie informacji. Takie rozwiązanie spowoduje, że niezdefiniowane obiekty nie będą się w ogóle pojawiały.

4.2.2 Standard T.61

Jedną z reguł syntaktycznych stosowanych w X.500 jest wykorzystanie standardu telekomunikacyjnego T.61 do kodowania wszelkich znaków diakrytycznych. Łańcuchy zawierające wyłącznie znaki czytelne mają przypisany syntaks `PrintableString`, takie w których dopuszcza się znaki specjalne określa się jako `T61String`. Tego typu łańcuch charakteryzuje się nagłówkiem w postaci identyfikatora {T.61} i zawiera, poza standardowymi znakami ASCII kody znaków diakrytycznych. Rozszerzeniem syntaksu `T61String` jest `CaseIgnoreString`, który dopuszcza pełne łańcuchy T.61, a jednocześnie zakłada, że przy porównaniach nie będzie się rozróżniać małych i wielkich liter. Jest to jeden z najszerzej stosowanych syntaksów.

Narodowe znaki specjalne z akcentami mają w standardzie T.61 postać dwóch bajtów: pierwszy to kod akcentu, drugi kod znaku podstawowego, inne są reprezentowane jako jeden bajt i występują w tabeli na pozycjach powyżej 127. Bardzo istotne jest, że T.61 jednoznacznie koduje znaki bez wykorzystania pojęcia strony tabeli kodowej.

Poniżej przedstawiono fragment tabeli kodów T.61:

Kod (hex)	Opis	Znak
c1	grave accent	`
c2	accute accent	´
c3	circumflex	^
c4	tilde	~
c5	macron	¯
c7	dot	˙
c8	diaresis	¨
c9	umlaut	¨
ca	ring	°
cb	cedilla	¸
cc	underline	_
cd	umlaut	¨
ce	ogonek	˛
e8	L z kreską (Ł)	Ł
f8	l z kreską (ł)	ł

4.2.3 Rozszerzenia w celu dostosowania bazy do lokalnych potrzeb

W celu przystosowania bazy X.500 do zapamiętywania w niej polskich nazw zostały ustalone niezbędne rozszerzenia, związane z definicją nowych klas obiektów i atrybutów.

Do tablic konfiguracyjnych wprowadzono polskie identyfikatory:

```
nask:                   data.2602
umk:                    nask.1
polishQuipu:            umk.1
polishObjectClass:      polishQuipu.1
polishAttributeType:    polishQuipu.2
```

Zdefinowano nowe atrybuty, m.in.:

```
polishCnName:   polishAttributeType.1 :caseIgnoreString (imie i nazwisko)
polishOName:    polishAttributeType.3 :caseIgnoreString (nazwa instytucji)
polishRDN:      polishAttributeType.19:caseIgnoreString (polska nazwa wyróżniona)
```

Atrybuty te zwierają łańcuchy w poprawnej polskiej pisowni, zapisane przy pomocy standardu T.61.

Konieczne było również zdefiniowanie nowych klas obiektów dopuszczających polskie atrybuty.

Polskie klasy obiektów i atrybuty powstały w celu umożliwienia wprowadzenia podwójnego nazewnictwa obiektów. Przyjęto, że jako wyróżnioną nazwę obiektu stosować się będzie określenia pozbawione znaków diakrytycznych, natomiast dodatkowo lokalne dane będą opisywane za pomocą specjalnych atrybutów, uwzględniających polskie znaki specjalne. Mamy wówczas do czynienia z pewnego rodzaju dublowaniem informacji, ale jednocześnie realizowane jest nazywanie obiektów zgodnie z potrzebą polskich użytkowników i w taki sposób, że odbiorca niezainteresowany narodową pisownią danych może ją bez problemu zaniedbać.

Dzięki oparciu definicji nowych atrybutów o istniejące syntaksy nie było potrzebne tworzenie dodatkowych funkcji obsługi struktur danych.

Przyjęte rozwiązanie nazywania polskich obiektów wymusiło wprowadzenie polskiej nazwy wyróżnionej, tak by na każdym poziomie można było jednoznacznie wybrać prawidłową lokalną nazwę, atrybut `polishRDN` jest obowiązkowy dla każdego polskiego obiektu, reprezentowanego jako `newPolishObject`.

4.3 RFC 1617

Polska baza X.500 jest fragmentem projektu PARADISE-NameFlow koordynowanego przez DANTE i mającego na celu tworzenie bazy X.500 dla środowiska naukowego. Sprawna praca takiej międzynarodowej bazy danych wymaga ustaleń co do sposobu nazewnictwa. Krajowe systemy X.500 działające w ramach PARADISE powinny stosować zalecenia zawarte w RFC 1617. Jednym z zaleceń jest zakaz stosowania łańcuchów T.61 w głównych nazwach obiektów. Wynika to z konieczności zapewnienia czytelnego wyświetlania nazw wyróżnionych.

Zalecenie RFC 1617 przewidujące wpisywanie nazw w poprawnej pisowni do kolejnych wartości atrybutów jest całkowicie nie do przyjęcia w przypadku, gdy chcemy stworzyć system, który polskiemu użytkownikowi będzie wyświetlał **wyłącznie** prawidłowe formy nazw.

Stosowanie wielokrotnych wartości atrybutów powoduje, że nie ma żadej możliwości automatycznego decydowania o tym, która wartość powinna być wyświetlona, a która nie.

Na podstawie doświadczeń z polską bazą przedstawiliśmy PARADISE projekt nazewnictwa uwzględniający pracę dwujęzyczną, w sposób nie ograniczony do pojedynczego kraju ([4]). W projekcie tym przewidujemy stosowanie atrybutów w wersji lokalnej i miedzynarodowej, pozostawiając interfejsowi użytkownika decyzję o tym, z której wersji korzystać. Przyjęcie tego typu zaleceń jest sprawą nadzwyczaj trudną, gdyż wymaga znacznych modyfikacji bazy danych. W tej sytuacji na razie zmuszeni jesteśmy korzystać z mniej optymalnych rozwiązań lokalnych.

4.4 Prezentacja wyników

Wiekszość aktualnie funkcjonujących aplikacji komputerowych stosuje pojęcie strony kodowej. W ten sposób użytkownik ustala, z jakiego zestawu czcionek będzie korzystał. Zmiana strony kodowej powoduje wyświetlanie innych symboli na wysokich miejscach (powyżej 127) tabeli kodów. Bezpośrednim efektem takiego podejścia jest niemożność wyświetlania na jednym ekranie jednocześnie znaków z różnych języków. Stosowanie tabeli kodowych jest szczególnie uciążliwe w przypadkach niejednoznaczych standardów (np. tabela Latin II (852) stosowana przez Microsoft i tabela ISO8859-2)

Wykorzystanie w X.500 standardu T.61 pozwala na jednoznaczne zakodowanie znaków łacińskich wszystkich języków europejskich, problemem pozostaje jednak ich wyświetlanie. Oczywiście nic nie stoi na przeszkodzie, aby aplikacja stosowała różne czcionki w ramach jednego ekranu i w ten sposób była całkowicie uniwersalna, ale nie jest to jak na razie powszechne podejście. Głównym powodem takiego stanu jest najprawdopodobniej fakt, że większość zachodnioeuropejskich języków mieści się w ramach podstawowej tabeli ISO8859-1.

Ponieważ obecnie typowy użytkownik na świecie ma do dyspozycji interfejs wyświetlający znaki zgodnie z tabelą Latin I należy założyć, że nie ma on dostępu do czcionek prezentujących polskie znaki i zostaną one zastąpione znakami nieczytelnymi. Dlatego niezbędne jest, by użytkownik obcojęzyczny bazował na nazwach pozbawionych polskich akcentów, a więc w podstawowych atrybutach bazy X.500 należy stosować nazwy bez polskich znaków diakrytycznych.

Interfejsy użytkowe muszą mieć wbudowaną możliwość wyboru strony kodowej, z którą współpracują. Takie też było założenie twórców oprogramowania QUIPU, rodzaj stosowanego zestawu znaków może zostać określony poprzez zmienną środowiskową lub za pomocą odpowiednich ustawień w użytkowych plikach konfiguracyjnych, przy czym, jak dotychczas, QUIPU dopuszcza wyłącznie ASCII i Latin I. Dokonana przez nas modyfikacja oprogramowania QUIPU w tym zakresie dopuściła stosowanie również strony Latin II w aplikacjach użytkowych.

4.5 Problemy efektywnościowe

Podstawowym problemem, z którym mamy do czynienia przy przyjętym rozwiązaniu realizacji dwujęzycznej bazy X.500 jest wydajność systemu. Nieuchronną konsekwencją proponowanego modelu jest konieczność wielokrotnego odczytu danych w celu dotarcia do informacji zgodnej z prawidłowa polską pisownią. Jak wcześniej wspomnieliśmy, obiekty w bazie X.500 są jed-

noznacznie identyfikowane poprzez swoje nazwy wyróżnione (*Distinguished Names*). Nazwy te występują w wersji międzynarodowej, w której polskie znaki diakrytyczne są pozbawione akcentów.

Użytkownik podając wzorzec przeszukania lub na podstawie przeglądania kolejnych poziomów drzewa informacji dociera do interesujących go danych. Niestety, hasło odczytywane posiada wyłącznie atrybut będący relatwną polską nazwą wyróżnioną, nie są znane polskie odpowiedniki nazw obiektów leżących na ścieżce drzewa informacji prowadzącej do docelowego obiektu. Oznacza to m.in., że wyszukując osobę reprezentowaną w bazie pod nazwą podstawową: `Wladyslaw Lopuszanski` jesteśmy w stanie odczytać lokalną nazwę obiektu: `Władysław Łopuszański`. Przyjmijmy, że nazwa wyróżniona obiektu ma postać:
`Wladyslaw Lopuszanski, Dzial Techniczny, Wydzial Chemii,`
`Wyzsza Szkola Inzynierska w Zielonej Gorze, Polska`

Chcąc wyprowadzić informację dotyczącą nazwy organizacji (zgodnie z polską pisownią), w których zlokalizowano obiekt konieczne jest odczytanie danych dotyczących lokalnych nazw haseł powyżej bieżącego (a wiec haseł trzech poziomów), tak by dotrzeć do polskich relatywnych nazw wyróżnionych i móc wyświetlić pełne dane o obiekcie:
`Władysław Łopuszański, Dział Techniczny, Wydział Chemii,`
`Wyższa Szkoła Inżynierska w Zielonej Górze, Polska`

Oczywiście taka technika znacznie wydłuża proces docierania do całości interesującej użytkownika informacji. W rozdziale 5 przedstawimy, w jaki sposób można zminimalizować koszt przedstawionej propozycji dostępu do lokalnych danych.

5 Implementacja

W bieżącym rozdziale opisujemy implementację modyfikacji interfejsów użytkowych X.500 w celu ich dostosowania do wykorzystania polskich danych umieszczonych w bazie.

Prace związane z tym tematem rozpoczęliśmy dwa lata temu. Początkowo zajęliśmy się programem de, który był w tym czasie najczęściej stosowanym interfejsem użytkowymi X.500. Następnie, gdy dynamicznie rosnąca popularność usługi World Wide Web przyczyniła sie do powstania programu umożliwiającego korzystanie z bazy X.500 poprzez interfejs kliencki WWW (tzw. WWW-browser, jak np. *Lynx, Netscape, Mosaic*), przedmiotem prac stał się moduł `web500gw`, pełniący funkcję tzw. *gateway'a* pomiędzy WWW a bazą X.500, obecnie jeden z powszechnie wykorzystywanych interfejsów X.500.

5.1 Program de

`DE` (*Directory Enquiries*) to bardzo prosty interfejs użytkowy X.500, rozwijany w ramach europejskich projektów COSINE i VALUE, autorstwa P. Barkera z Uniwersytetu Londyńskiego. Program oferuje dane X.500 Directory poprzez terminal liniowy. Dostępne są dwie wersje de:

1. działająca według standardowego dla X.500 protokołu DAP (*Directory Access Protocol*), zapewniającego komunikację pomiędzy aplikacją użytkową X.500 a serwerem DSA,
2. oparta o uproszczony protokół LDAP (*Lightweight Directory Access Protocol*), w którym kontakt z serwerem X.500 następuje poprzez serwer LDAP, komunikujący się następnie z DSA.

Prace modyfikacyjne polegały na dołączeniu w programie odczytu, w przypadku dostępu do obiektów polskiego poddrzewa X.500, wartości lokalnych atrybutów oraz prezentacji wyników zgodnie z obowiązującą strona kodową.

W programie de wybór zestawu znaków odbywa się przy starcie aplikacji, decydują tu parametry konfiguracyjne interfejsu użytkowego, które są pobierane ze specjalnego pliku użytkownika, albo z pliku systemowego.

W przypadku de opartego na protokole DAP dostosowanie interfejsu do współpracy ze stroną Latin II wymagało zmian w oprogramowaniu QUIPU. W modułach bibliotecznych QUIPU dołączono interpretację kodów znaków w ramach obsługi syntaksów konkretnych atrybutów.

W LDAP de było możliwe ograniczenie zmian do samego kodu źródłowego programu, w którym zostały dołaczone funkcje translujące zestaw T.61 do postaci Latin II.

„Spolszczone" de wykorzystuje polskie opisy umieszczone w lokalnych atrybutach i prezentuje je na ekranie. Uzyskanie pełnej informacji na temat hasła, zgodnie z tym co opisaliśmy w rozdziale 4.5, pociąga za sobą odczyt polskich danych obiektów położonych na ścieżce prowadzącej do bieżącego hasła w drzewie informacji, co zostało zaimplementowane w programie.

De pozwala również wyszukiwać informacje z bazy X.500 za pomocą wzorców zawierających polskie znaki diakrytyczne.

Modyfikacja programu de odegrała bardzo ważna rolę w zrozumieniu wielu problemów związanych z interpretacją i prezentacją znaków narodowych w aplikacjach X.500. Prace te zmusiły nas do poznania tajników oprogramowania QUIPU i znacznie usprawniły dalsze działania dotyczące polskich interfejsów X.500.

5.2 Program `web500gw`

Autorem *gateway'a* pomiędzy WWW a X.500 jest Frank Richter z Uniwersytetu w Chemnitz-Zwickau.

Modyfikacja tego programu zmierzała w dwóch kierunkach. Podstawowym celem było wykorzystanie do prezentacji informacji zawartej w ramach dodatkowych, lokalnych atrybutów i „spolszczenie" programu poprzez zastąpienie angielskich tekstów objaśniających polskimi. Kolejnym zadaniem było wbudowanie w program możliwości wysyłania formularza zawierającego dane aktualizujące informacje zamieszczone w X.500.

`Web500gw` pozwala uzyskać dostęp do danych X.500 Directory. Jego działanie bazuje na protokole LDAP, będącym uproszczoną wersją standardowego protokołu X.500, zwanego DAP (*Directory Access Protocol*), zapewniającego komunikację pomiędzy aplikacją użytkową X.500 a serwerem.

Zgodnie z przyjętym założeniem uwzględniono możliwość stosowania następujących stron kodowych: ASCII, Latin I, Latin II, IBM (CP852), Windows-EE. Wybrany zestaw znaków może zostać zmieniony w trakcie korzystania z programu, przekodowanie do odpowiednigo formatu następuje dynamicznie.

Ponieważ program `web500gw` jest typową aplikacją kliencką World Wide Web, jego dokumenty, czyli teksty wyświetlane przez program, są przygotowywane w języku HTML (*HyperText Markup Language*). HTML jest podzbiorem bardziej ogólnego języka — SGML (*Standard Generalized Markup Language*). Znaki specjalne są przedstawiane w HTML'u, podobnie jak w SGML'u, jako tzw. *SGML-entities.*

Oto przykładowe odpowiedniki:

> — `>`
> Ą — `&Aogon;`
> Œ — `&OElig;`

Program `web500gw` zmodyfikowano w taki sposób, że wszelkie znaki o kodach powyżej 127 zapamiętywane są wewnętrznie jako tzw. *SGML-entities*, również informacje pobrane z bazy X.500 translowane są z kodu T.61 do postaci SGML. Następnie, w trakcie wyprowadzania danych na ekran następuje konwersja do postaci aktualnej strony kodowej poprzez zastosowanie odpowiedniego filtru przekodowującego. Obecnie graficzne programy klienckie WWW akceptują wyłącznie *SGML-entities* z zakresu alfabetu Latin I, ale ponieważ sam standard SGML zawiera formalną definicję nazw znaków innych stron kodowych, należy się spodziewać, że wkrótce będą one interpretowane w interfejsach graficznych WWW. Zastosowane w `web500gw` podejście do kodowania znaków diakrytycznych pozwoli w tym momencie w prosty sposób zmodyfikować kod źródłowy i pozbawić program balastu translacji z postaci SGML.

Polska wersja programu `web500gw` wykorzystuje możliwość umieszczania w bazie X.500 obiektów opisanych za pomocą atrybutów lokalnych, o których była mowa w rozdziale 4.2.3.

W przypadku odczytu hasła w ramach polskiego poddrzewa informacji sprawdzamy, czy obiekt należy do klasy `newPolishObject`, jeżeli tak, odczytywana jest wartość atrybutu `polishRDN` (jest to atrybut obowiązkowy dla tej klasy i jednowartościowy), która jednoznacznie decyduje o nazwie głównej obiektu. Pobierane są również informacje umieszczone w innych lokalnych atrybutach (m.in. `polishDescription`, `polishTitle`, `polishPostalAddress` itp.)

Z przyczyn efektywnościowych przedstawionych w rozdziale 4.5 konieczne było zaimplementowanie algorytmu *cachowania*, czyli przechowywania w podręcznej pamięci danych przemapowujących nazwę wyróżnioną obiektu w jego postać lokalną. Zasada działania programu `web500gw`, który startując uruchamia proces macierzysty oczekujący na połączenia, a każde odwołanie typu *HREF* generuje nowy proces wymusiła potrzebę stosowania pamięci współdzielonej jako *cache*'a. Konieczna jest kontrola zajętości pamięci podręcznej, jej wielkość jest programowo ograniczona poprzez ustawienie zgodne z argumentem wywołania programu lub w przypadku jego braku przyjmowana jest domyślnie pojemność niezbędna do przechowania 800 przemapowań. Przyjęto rotacyjne umieszczanie kolejnych elementów w pamięci. *Cache* ma postać par:

(nazwa wyróżniona obiektu, wartość atrybutu `polishRDN`)

przy czym `polishRDN` jest przechowywany w postaci SGML, tzn. zawiera *SGML-entities* w miejscu znaków diakrytycznych. Optymalizuje to wykorzystanie pamięci podręcznej i stwarza warunki do dynamicznego przekodowywania nazw do postaci obowiązującej strony kodowej.

Drugą istotną modyfikacją zaimplementowaną w `web500gw` było udostępnienie, w przypadku odczytu danych osobowych, formularza aktualizacji. W swojej oryginalnej postaci `web500gw` udostępnia eksperymentalnie funkcję aktualizacji danych bezpośrednio w bazie X.500. Uprawniono do tego właścicieli obiektów klasy *Person*, znających swoje hasło zabezpieczające (*password*). W ramach polskiej bazy X.500 zrezygnowaliśmy z funkcji bezpośredniej aktualizacji, w zamian oferujemy możliwość przesłania za pomocą poczty elektronicznej specjalnego formularza z nowymi danymi. Ponieważ tematyka związana z aktualizacją danych w ramach X.500 znacznie wykracza poza ramy naszego artykułu, problem ten zostanie opisany

w odrębnym raporcie. W tym miejscu warto jedynie nadmienić, że dane w formularzu mogą zawierać polskie znaki diakrytyczne, które niezależnie od stosowanej strony kodowej zostaną prawidłowo dostarczone do administratora (w standardzie T.61).

Bibliografia

[1] M. Górecka, T. Wolniewicz, *X.500 - standard i usługi katalogowe*, kwiecień 1995, materiały konferencyjne Polman.

[2] M. Górecka, T. Wolniewicz, *Stosowanie znaków diakrytycznych w systemach baz danych X.500*, wrzesień 1994, raport NASK.

[3] P. Barker, S. Kille, T. Lenggenhager (May 1994) *Naming and Structuring Guidelines for X.500 Directory Pilots*, Request for Comments RFC1618.

[4] M. Górecka, T. Wolniewicz, *"Naming in the X.500 Directory"*, 1995, propozycja zmiany nazewnictwa obiektow w projekcie Paradise przesłana do Dante i koordynatorow X.500.

WYKORZYSTANIE SIECI INTERNET W HANDLU I DYSTRYBUCJI

Piotr Wajszczyk

Katedra Marketingu Uniwersytetu Łódzkiego
ul. POW 3/5, 90-255 ŁÓDŹ
Tel. (042) 30-47-80 wew.5205, 5203
E-mail: <peterwaj@krysia.uni.lodz.pl >

1. WSTĘP

Od początku lat 90. sieć Internet rozwija się bardzo dynamicznie, a jej zastosowanie z początkowo naukowego i badawczego charakteru zaczyna stawać się coraz bardziej komercyjne. Właściwie można powiedzieć, że bez zainteresowania się siecią przez duże kompanie telekomunikacyjne, firmy hardwarowe i softwarowe, nie byłoby dzisiejszego Internetu na świecie. Jego rozwój komercyjny stał się możliwy dzięki temu, że firmy i korporacje ujrzały w sieci lepsze niż dotychczas istniejące narzędzie przydatne zarówno do reklamy towarów i usług, jak i do ich dystrybucji i przenoszenia płatności.

Szacuje się, że ok. 70 mln ludzi na świecie ma dostęp do sieci Internet, zaś w tylko w USA ok. 28.8 mln w wieku ponad 16 lat, 16.4 używa Internet, 11.5 mln używa W3, a 1.51 mln wykorzystało ją do dokonania zakupów [2]. Jak wskazują te i inne [5], [7], [8], [9] badania sieci pod kątem jej komercyjnego wykorzystania, demografia użytkowników sieci Internet silnie zależy od typu dostępu do niej, czasu dostępu do sieci i możliwości sprzętu.

Jednak nadal brak podstawowych informacji na temat rynków, które stworzył Internet, np. ilu naprawdę użytkowników jest podłączonych do ok. 9.47 mln hostów na całym świecie.

Różne badania podają różne szacunki zależnie od sposobu zdefiniowania poszczególnych kategorii "użytkownik", "podłączony do sieci". Np. [3] i [4] oceniało, że 37mln osób pow. 16 lat w USA i Kanadzie ma dostęp do Internetu, 24 mln używa go, 18 mln używa W3, zaś 2.5 mln dokonało zakupów poprzez sieć w badanym okresie.

Pracuje się także nad nowymi metodami badań rynków, gdyż nie ma dotychczas wypracowanych metod statystycznych analizy rynków sieciowych [10].

Niektóre badania systematyczne wskazują dynamiczny i ewolucyjny charakter demografii sieci: przestaje ona być domeną mężczyzn, pionierów i innowatorów, a staje się coraz bardziej masowym zjawiskiem społecznym [5]. W tym też kontekście uzasadnione jest traktowanie samej sieci Internet jako sieci dystrybucji, która w niedalekiej przyszłości docierać będzie do globalnych rynków masowych.

2. NOWE ROZWIĄZANIA W HANDLU

Problem komercjalizacji sieci jest nowy również dla polskich naukowców i badaczy rynku, ponieważ będą oni musieli brać pod uwagę zmiany strukturalne w handlu spowodowane przez nowe technologie. Choć w chwili obecnej wykorzystanie potencjalnych możliwości handlu, stworzonych przez nowe technologie przez podmioty rynkowe w Polsce jest raczej marginalne, to jednak samo zjawisko jest naszym przeznaczeniem, do którego wszyscy nieuchronnie zmierzamy. Nieznana jest tylko skala i tempo rozwoju tego zjawiska.

Służenie klientom wymaga znajomości ich potrzeb, ich oczekiwań, preferencji obecnych i przyszłych, tak aby do stworzonego w ten sposób otoczenia organizacja mogła możliwie najlepiej dopasować swoją strukturę i możliwości funkcjonowania.

Dotyczy to każdej organizacji, w tym również firm pośredniczących w dystrybucji towarów i usług. Presja, jaką wywiera szybki postęp w dziedzinie teleinformatyki, zmusza wszystkie organizacje, a szczególnie pośredników (w tym hurtowników i detalistów) w handlu i dystrybucji towarów i usług, do dostosowania się do zaistniałej sytuacji.

Naturalną tendencją wolnego handlu jest, by jak najbardziej uprościć sieć dystrybucji towarów i usług i zapewnić końcowemu odbiorcy maksimum użyteczności towaru dostarczanego po jak

najniższym koszcie dystrybucji. Jednakże podstawową cechą, wspólną dla wszystkich kanałów dostępu do rynku jest to, że wszystkie one podlegają procesowi dojrzewania, który polega na :

* wzroście siły przetargowej podmiotów zarządzających takim kanałem wobec producentów dóbr i usług, zmusza to producentów do poszukiwania alternatywnych kanałów dystrybucji;
* specjalizacji kanałów dystrybucji na ściśle określonych asortymentach wyrobów, cecha która znacznie ogranicza elastyczne penetrowanie rynków docelowych przez producentów dóbr i usług.

Zjawisko takie jest niekorzystne, gdyż nadmierna liczba pośredników-uczestników przekazywania towaru do końcowego konsumenta powoduje opóźnienie przepływu towarów od producenta do konsumenta, opóźnienie reakcji producenta danego towaru na bodźce płynące z rynku, zniekształcenie informacji o rynku, o potrzebach i preferencjach konsumentów.

Łańcuch: producent - pośrednik (hurtownik) - pośrednik (detalista) - konsument nie działa więc w sposób efektywny z punktu widzenia optymalnego zaspokajania potrzeb konsumenta. Jest to typowa sytuacja opisywana mianem strategii *push* w odróżnieniu od strategii *pull*, bardziej efektywnej, w ktorej końcowy klient "przeciąga" pożądany towar lub usługę przez poszczególne ogniwa rynku.

Dlatego też producenci nie ustają w poszukiwaniach innych kanałów dostępu do rynków, aby zwiększyć swój udział w zyskach w grze, która toczy się pomiędzy nimi, pośrednikami a końcowymi konsumentami dóbr i usług. Poszukiwania te przede wszystkim dotyczą kanałów informowania klienta o cechach, cenach i jakości oferowanych towarów, tak by przez nie klient **sam** mógł składać zamówienia bezpośrednio u producenta, a nie u pośrednika.

I taką właśnie szansę dają przedsiębiorstwom produkcyjnym sieci informatyczne i ich operatorzy sieciowi.

3. ZASTOSOWANIE SIECI W REKLAMIE

Istnieje też inny problem, na jaki natrafiają współcześni handlowcy, tym razem w sferze reklamy i informowania klientów. Są to trudności w efektywnym docieraniu z informacją o oferowanym produkcie do danego wybranego segmentu rynku. Problemy te wynikają głównie z malejącej efektywności kosztowej reklamy masowej oraz jej pasywnego charakteru (szczególnie chodzi tu o TV). Efektem takiej ewolucji mediów jest to, że kampania reklamowa :

* musi być obliczona na długi okres czasu by przynieść wymierne efekty;
* powoduje wzrost specjalizacji danego kanału reklamy masowej obsługującego dany typ widowni;
* jest w stanie jedynie pobudzić wyobraźnię klienta, oddziaływać na jego odczucia, skojarzenia, ze względu na krótki czas jej trwania, nie zaś bezpośrednio informować, przekonywać i nakłaniać do decyzji kupna produktu;
* jest skomplikowana w zarządzaniu, gdyż rośnie liczba jej elementów składowych które muszą być koordynowane przez wyspecjalizowane agencje reklamowe. I również w tej dziedzinie sieci komputerowe znalazły ostatnio duże zastosowanie, przede wszystkim dzięki rozwojowi sieci Internet.

Internet wykorzystany do celów komercyjnych ujawnił kilka cennych zalet:

- ***szybkość reakcji*** - możliwość prawie natychmiastowej odpowiedzi na zamówienie dostawy towaru, usługi, prośbę o informację;
- ***elastyczność medium*** - gdy badania wskazują brak zadowolenia odwiedzających stronę klientów, handlowiec może zmienić jej układ, treść czy zawarte funkcje w ciągu kilkunastu minut projektując nowy przekaz reklamowy strony WWW;
- ***głębię przekazu*** - która umożliwia oferowanie klientowi nie tylko produktu, ale też *jednocześnie* wzbogacanie go o wiedzę o produkcie (innych usługach firmy, czy informacji o firmie) o dowolnej porze w ciągu całej doby, inicjując z nim więź z licznymi sprzężeniami zwrotnymi (cecha nieosiągalna w przypadku reklam drukowanych czy filmowych), przy czym występuje wręcz tendencja do umożliwienia klientowi konstruowania idealnego produktu on-line;

- ***globalny zasięg całego kanału*** - dający dostęp do każdego uczestnika globalnej wioski w każdym punkcie na ziemi i w kosmosie, do którego dociera kanał sieci;
- ***multimedialny charakter przekazu*** - przekazywaną informacją może być tekst, obraz kolorowy i trójwymiarowy, film, dźwięk stereofoniczny i dowolna ich kompozycja;
- ***przyjazny charakter dla środowiska naturalnego*** - brak opakowań, drukowanych ulotek, wykorzystania farby drukarskiej, papieru itp., co gwarantowane jest przez kompletność informacji zawartej w przekazie elektronicznym;
- ***niski koszt przekazu*** - jest on o blisko rząd wielkości niższy niż w przypadku tradycyjnych kanałów komunikacji z klientem przy porównywalnych cechach (np. reklama w telewizji omercyjnej), wynika to głównie z młodego wieku tej formy przekazu i ustrukturalizowanej formie jej obsługi (zarządzanie reklamą przestaje mieć cechy twórcze i nabiera charakteru czynności rutynowej).

Obecnym zadaniem dla internetowych agencji reklamowych jest wypracowanie wiarygodnego modelu szacowania efektywności reklamy i płatności za nią.

Transfery funduszy i płatności poprzez Internet jak dotąd rozwija się głównie w USA dzięki istnieniu tzw. banków wirtualnych np. Cybercash czy First Virtual. Choć nie ma na świecie w chwili obecnej odpowiednich regulacji prawnych, które sankcjonowałyby powszechne i globalne użycie płatności sieciowych na szeroką skalę (może za wyjątkiem USA, gdzie niedawno Prezydent Clinton podpisał ustawę idącą w tym kierunku: Telecommunications Bill), rozwój tych operatorów jest niezwykle intensywny.

Pomimo pewnych trudności, w świecie nasila się trend do komercjalizacji usług sieciowych, co moim zdaniem dowodzi o wyraźnych dążeniach operatorów sieciowych do przejęcia roli pośredników w dostępie do rynków.

Należy przy tym podkreślić, że w działalności operatorskiej w przyszłości należy oddzielić kwestię rozliczeń za generowany ruch w sieci [ustalony model płatności] od pomiaru i kontroli przepływu wartości towarów i usług przez sieć.

Tę zasadniczą różnicę między nimi można porównać do mierzenia intensywności ruchu samochodowego na rogatkach granicy a pomiarem wartości przewożonych przez nie towarów ujawnianych w deklaracjach celnych. O ile mi wiadomo nie ma jeszcze takich narzędzi programowych umożliwiających pomiar w sieci i kontrolę takich wielkości jak: cena usługi, ilość nabytych towarów i usług czy ich jakość. Obecnie pomiar tych ostatnich jest możliwy jedynie pośrednio, poprzez badania ankietowe wśród użytkowników sieci.

4. KTO KORZYSTA NA ŚWIECIE Z SIECI INTERNET

Podzieliłem wszystkie ogranizacje na dwie grupy :

a) Podmioty (organizacje), dla których działalność sieciowa jest podstawowa lub jedyna (choć jest ona często sponsorowana):

- dostawcy sieciowi (popularni głównie w pierwszym etapie rozwoju sieci);
- drobni detaliści wirtualni, wydawcy, publicyści, naukowcy;
- operatorzy płatności sieciowych (First Virtual, CyberCash, Digicash);
- wirtualne agencje informacyjne, wydawnicze (dzienniki, biuletyny sieciowe);
- biblioteki sieciowe i firmy obsługujące zasoby sieciowe (Yahoo, Lycos, Altavista itp.) ;
- wirtualne agencje marketingowe - prowadzące marketing bezpośredni, badania marketingowe;
- wirtualne agencje reklamowe (reklama przy pomocy poczty elektronicznej, stron 3W, ogłoszeń w bazach danych (search engines);

b) Firmy, których podstawowa działalność gospodarcza nie jest związana z sektorem sieciowym (np. Pizza Hut , banki: Mellon Bank, Chase Manhattan, First American, Wells Fargo) i które głównie reklamują się przez sieć.]

Jest to jednak podział arbitralny i orientacyjny, gdyż najczęściej firmy łączą kilka typów działalności i ten fakt utrudnia jednoznaczne zakwalifikowanie do jednej i tylko jednej kategorii.

5. PRZYSZŁOŚĆ MARKETINGU W INTERNECIE W USA

Wiele instytucji stara się dokonać szacunków i projekcji rozwoju i kształtu sieci w przyszłości. Chociaż na pewno żadne z nich się nie sprawdzi w 100 procentach, to jednak warto przytoczyć w tym miejscu wybrane i przykładowe opinie praktyków marketingu internetowego w USA. Przewiduje się że w ciągu dekady Internet będzie rosnąć w tempie co najmniej takim jak obecnie.

Do korzystania z pośrednictwa z Internetu służyć będą wyspecjalizowane programy (będą to oczy i uszy użytkownika/firmy i od ich sprawności zależeć będzie jego sukces lub porażka). Przewiduje się stworzenie dla każdego użytkownika jego indywidualnego modelu w CAD (Computer Aided Design) wiernie oddającego jego rozmiary ciała i parametry poszczególnych jego elementów. Model ten służyć będzie do pośrednictwa w zakupach obuwia i garderoby, których części składowe będą szyte na miarę modelu przez zautomatyzowane fabryki. Rolą użytkownika będzie jedynie utrzymywanie zgodności parametrów modelu ze swoimi rzeczywistymi wymiarami. Specjalne programy służyć będą do wyszukiwania danego produktu o podanym zakresie cenowym, o określonych cechach i warunkach dostawy.

Podobnie, poprzez sieć odbywać się będą usługi bankowe i informacyjne. Najprawdopodobniej książki będzie się zamawiało bezpośrednio u wydawcy, u którego będą drukowane i oprawiane pojedyncze zamówione egzemplarze, które będzie można odebrać w ciągu godziny. Filmy video, przechowywane w sieci będzie można przegrać na własną taśmę lub obejrzeć bezpośrednio w sieci.

Ponieważ transport i magazynowanie towarów kosztuje, szacuje się że ok. 50% towarów będzie wysyłana tylko raz: od producenta do finalnego konsumenta. Następcy VRLM (Virtual Reality Modelling Lines) będą w stanie modelować większość produktów, do których reklamy nie będzie potrzeba fizycznych witryn sklepów.W perspektywie dekady nowy kanał będzie tak silnie zintegrowany z innymi częściami infrastruktury gospodarki, że nie będzie można oddzielić dóbr sprzedawanych poprzez sieć od tych sprzedawanych poza nią. Handlowcy podkreślają, że obecnie niewielkie grupy klientów, którzy korzystają z pośrednictwa sieci, to jeszcze pionierzy i innowatorzy. Handlowcy obecnie koncentrują swoje wysiłki na zbudowaniu doświadczenia w pracy z nowym kanałem. Za ok. 5 lat firmy, które dopiero teraz uczą się komercyjnego wykorzystania nowego kanału, będą już miały zupełnie inną wielkość i strukturę.

6. JAK WYGLĄDA W PRAKTYCE HANDEL ELEKTRONICZNY

Zazwyczaj firma, która nie ma znaczącego doświadczania w posługiwaniu się nowym medium, zleca operatorowi sieciowemu wykonywanie w jej imieniu określonych w umowie funkcji, np. reklamy danych produktów firmy.

Obowiązkiem operatora może wówczas być zaprojektowanie, skonstruowanie, uruchomienie, obsługa i utrzymanie poprawnego funkcjonowania przekazu reklamowego, co w praktyce sprowadza się do :

* zapewnienia jej widoczności w sieci,
* pomiaru liczby klientów, którzy ją oglądają w określonym czasie, ew. prowadzenia badań,
* zbieranie zamówień złożonych za jej pośrednictwem, a bywa że i do współpracy ze zleceniodawcą w obsłudze klientów.

Naturalnie, koszt skonstruowania takiej reklamy waha się w dość szerokich granicach i zależy od stopnia jej skomplikowania, jakości, cech funkcjonalnych miejsca jej umieszczenia i wykonawcy. Najbardziej znani amerykańscy pośrednicy świadczący odpłatne usługi reklamowe to Yahoo i Lycos.

Oprócz reklamy, istnieją też inni uczestnicy rynku, którzy przejmują funkcję pośredniczenia w przepływie i przenoszeniu produktów materialnych od producenta do pośrednika lub bezpośrednio do konsumenta (mogą to być np. Federal Express, United Parcel Service, czy innych przewoźnicy lądowi czy powietrzni).

Jeszcze inni uczestnicy zajmują rolę pośrednika w obsłudze płatności dokonywanych poprzez sieć i współpracują z bankami i firmami przetwarzającymi płatności kart kredytowych[1]. Dobór uczestników kanału dystrybucji odbywa się tak, aby wykorzystać jak najlepiej wszystkie atuty jakie oferuje sieć, przede wszystkim zaś jej szybkość działania.

W Europie rynek usług stworzony przez Internet nie jest jeszcze tak bardzo rozwinięty jak w USA. Ponadto wielojęzyczność produktów tworzy naturalne bariery dla wolnej konkurencji i sugeruje, że ten rynek będzie ewoluował wolniej niż jego amerykański odpowiednik.

Ponadto w Polsce nie ma zbyt silnej branży przedsiębiorstw produkujących tani sprzęt telekomunikacyjny i teleinformatyczny. Sieć telekomunikacyjna nie jest rozpowszechniona szczególnie na wsi, nie wspominając o sieciach teleinformatycznych.

Ideą przewodnią powstania i gwałtownego rozwoju Internetu była i jest nadal misja każdej firmy telekomunikacyjnej: "łączyć ludzi" wszelkiej narodowości, rasy, religii i zamieszkałych na wszystkich kontynentach. Właśnie ta filozofia umożliwiła zaistnienie warunków na traktowanie Internetu w kategoriach rynku. Chcę tutaj mocno podkreślić słowo "łączyć", ponieważ w naszych polskich realiach ten właśnie element jest jeszcze bardzo słaby, aby Polski Internet stał się początkiem otwartego społeczeństwa informatycznego, rządzonego prawami gospodarki rynkowej.

Brakuje nam poważnych inwestycji w sprzęt telekomunikacyjny w miastach, a przede wszystkim na wsi, by "łączenie ludzi" miało realny oddźwięk. Z tych też powodów uważam, że rozwój handlu elektronicznego oraz elektronicznych sieci dystrybucji na znaczną skalę w Polsce jest jeszcze sprawą przyszłości.

Bibliografia :

1. "Marketing in Hypermedia Computer-Mediated Environments: Conceptual Foundations" - Donna L. Hoffman, Thomas P. Novak, Working paper #1, July, 11 1995 Project 2000 Research program in Marketing in Computer mediated environments, Owen Graduate School pf Management, Vanderbilt University, http://www2000.ogsm.vanderbilt.edu.
2. "Internet use in the United States: 1995 Baseline Estimates and Preliminary Market Segments", Donna L. Hoffman, Thomas P. Novak - Project 2000 Owen Graduate School of Management, Vanderbilt University, William D. Kalsbeek, Survey Research Unit, Dept. of Biostatistics, Univ. of North Carolina at Chapel Hill; Working Paper April 12, 1996.
3. CommerceNet/Nielsen Internet Demographic Study August 1995, published: November 1995, Nielsen Media Research, http://www.nielsen.com, CommerceNet Consortium, 800 El Camino Real, Menlo Park CA 94025, E-mail: info@commerce.net, http://www.commercenet.com.
4. CommerceNet/Nielsen Internet Demographic Study August 1995, Frequently Asked Questions, December 20 1995, CommerceNet Consortium/Nielsen Media Research.
5. The Third 3W Demographic Consumer Survey, Sunil Gupta 1996; A HERMES Project in collaboration with Graphics Visualisation and Usability (GVU) Georgia Institute of Technology, hermes@cochrane.bus.umich.edu, http://www.cc.gatech.edu/gvu/user_surveys/.
6. "The Death of Distance", The Economist Group, Sept.30, 1995, Survey : Telecommunications.
7. Times Mirror 1995. Technology in the American Household: Americans Going Online. Times Mirror Center for the People and the Press. October 16, 1995.
8. "The 01/05/96 Snapshot Internet Info". Walsh Michael 1996.
9. Yalenkovich Partners 1995. The Yalenkovich Cybercitizen Report. The Yalenkovich Partners, Inc. August 1995.
10. "Internet - nowy kanał marketingowy", Piotr Wajszczyk, Marketing i Rynek, listopad 1995.

USŁUGI MARKETINGOWE „BUSINESS-TO-BUSINESS" NA PRZYKŁADZIE FIRMY INDUSTRY.NET

Maria Baranowska

Naukowa i Akademicka Sieć Komputerowa NASK, ul. Bartycka 18, 00-716 Warszawa
E - mail: maria@nask.pl

Wstęp

Vince Emery, autor książki *How to Grow Your Business on the Internet* podaje w miesięczniku *PC World* z października 1995 roku adresy WWW jedenastu najbardziej znanych *miejsc* w Internecie, gdzie można skorzystać z kompleksowej informacji dla biznesmenów. Na liście Emery'ego znajdują się serwisy informacyjne, prowadzone przez różne instytucje. Jedne z nich działają na zasadach czysto komercyjnych, inne tworzą i udostępniają informacje w ramach grantów finansujących działalność naukową. Na dynamicznie rozwijającym się rynku usług informacyjnych, dostępnych w sieci Internet, występują również serwisy sponsorowane przez konsorcja wielkich firm - producentów i hurtowych sprzedawców sprzętu służącego do dalszej produkcji. Wszystko razem można określić coraz popularniejszym terminem usług marketingowych: *business-to-business*. Poniżej przedstawiam krótką charakterystykę wybranej przez Emery'ego „jedenastki".

1. Na pierwszym miejscu swej listy Vince Emery stawia powstałą w styczniu 1994 r. **CommerceNet (http://www.commerce.net)** - konsorcjum *non-profit* złożone z ponad 140 firm i organizacji, które stawiają sobie za cel przyspieszenie i spopularyzowanie handlu i wymiany informacji komercyjnej za pośrednictwem sieci Internet. Firmy - założyciele organizacji - to przede wszystkim instytucje wiodące na polu elektroniki, produkcji komputerów i tzw. przemysłu informacyjnego w Stanach Zjednoczonych. Serwis informacyjny CommerceNet stanowi aktualny przewodnik po producentach *soft-ware'u* i dziesiątkach sposobów wykorzystania Internetu do zdobycia bieżącej informacji handlowej; znaleźć tam można między innymi wykazy firm dostarczających i pomagających w uzyskaniu dostępu do sieci Internet i wiele innych, użytecznych dla handlowców i przedsiębiorców, informacji.

2. Na drugim miejscu w zestawieniu *PC World* znajduje się wielki „elektroniczny dom handlowy" (*online mall)* **Industry.NET (http://www.industry.net)**, w którym setki producentów i hurtowników sprzedaje produkty *high-tech*, wykorzystywane m.in do projektowania maszyn i urządzeń, narzędzia do testów i pomiarów w procesie produkcji etc. W serwisie IndustryNET można znaleźć również najświeższe informacje o nowych produktach na rynku, o targach i pokazach promocyjnych odbywających się na terenie Stanów Zjednoczonych i w innych krajach świata.

3. Twórcy bazy **Premenos (http://www.premenos.com)** określają ją jako przewodnik po biznesie elektronicznym. To miejsce oferujące odniesienia do działających na rynku dostawców usług internetowych, do informacji o wydarzeniach komercyjnych w Internecie, targach etc.

4. Kolejnym źródłem informacji o najważniejszych poczynaniach firm komercyjnych w Internecie jest **Business Sites (http://www.rpi.edu/~okeefe/business.html)** - prowadzona przez Boba O'Keefe'a, profesora ze *School of Management* w *Rensselaer Polytechnic*. Jest to wybór ok. 50 najciekawszych połączeń do komercyjnych stron WWW z całego świata.

5. **Mouse Track (http://nsns.com:80/Mouse Track)** to firma, która obok standardowej działalności dostawcy dostępu do Internetu, udostępnia w sieci katalogi dotyczące głównych źródeł wiedzy na temat działalności marketingowej, reklamy i sprzedaży hurtowej, znajdujących się w Internecie i poza nim.

6. **Rutgers Accounting Web (http://www.rutgers.edu./Accounting/raw.html)** - to strona WWW tworzona i aktualizowana w Uniwersytecie Rutgers w Australii, specjalizująca się w dostarczaniu łatwego dostępu do informacji księgowej, finansowej i podatkowej z całego świata.

7. **FINWeb (http://riskweb.bus.utexas.edu/finweb.html)** - przygotowana w University of Texas aktualna książka adresowa najciekawszych *Web sites* poświęconych finansom, ekonomii i problematyce inwestowaniu kapitału.

8. **Yahoo Business Directories (http://www.yahoo.com/business)** - w tej najczęściej bodaj odwiedzanej obecnie bazie informacyjnej WWW znaleźć można wszystko: spisy organizacji przemysłowo-handlowych i odnośniki do ich stron WWW, zestawy serwisów informacyjnych o komercyjnych przedsięwzięciach w Internecie, informacje o przepisach finansowych i podatkach, różnego typu informacje o regulacjach prawnych, dotyczących m.in. ochrony własności intelektualnej etc.

9. **EINet Galaxy's Business and Commerce Directory (http://galaxy.einet/galaxy/Business-and-Commerce.html)** to baza danych informująca o sposobach korzystania z protokołów, standardów, stosowania strategii określanych jako *business-to-business* lub *business-to-consumer* oraz wielu innych źródeł wiedzy na temat metod marketingu stosowanych w elektronicznym biznesie.

10. **Information Services for Professionals (http://ioma.com/ioma)** wprowadza nas w opracowywane przez amerykański *Institute of Management and Administration* materiały informacyjne dotyczące biznesu i zarządzania.

11. **Electronic Commerce on the World Wide Web (http://amex.cox.smu./edu/mis/cases/webcase/home.html)** - Szkoła Biznesu z *Southern Methodist University* dostarcza w swym serwisie przykłady różnych rozwiązań (*case studies*) odnośnie prowadzenia interesów w sieci przez znane firmy, nie szczędząc uwag i teoretycznych refleksji o tym, jak należałoby stworzyć lepsze usługi w tej dziedzinie.

Firma IndustryNET

Powstała w 1990 r., założona w Pittsburgu przez znanego przemysłowca Dona H. Jonesa i kierowaną przez niego grupę specjalistów w dziedzinie wydawnictw informacyjnych, marketingu i łączności elektronicznej IndustryNET od początku postawiła sobie za cel ułatwienie komunikacji pomiędzy podmiotami zainteresowanymi kupnem, sprzedażą i informacją o nowych produktach i usługach dostępnych na rynku. Jakkolwiek w ciągu 6 lat istnienia firmy zmieniały się metody zbierania i udostępniania informacji klientom (od dystrybucji dyskietek z bazami adresowymi firm do rozbudowanej działalności w sieci Internet) to misja jej założycieli nie uległa zmianie. Jak pisze o tym Don Jones - *wyszliśmy z przemysłu i wiemy dobrze, jak ważną rzeczą jest umożliwić producentom i konsumentom dostęp do dynamicznej informacji w warunkach wzajemnego oddziaływania (interactive environment) obu stron.*

Rozwój IndustryNET jest bardzo intensywny. Wystarczy powiedzieć, że jej obroty i liczba klientów rośnie średnio o ponad 200 % rocznie. W tej chwili IndustryNET wraz ze swoimi 17 oddziałami na terenie Stanów Zjednoczonych i z kadrą pracowników w liczbie ok. 160 specjalistów z różnych dziedzin marketingu i *public relations* urosła do jednego z najprężniej rozwijających się przedsiębiorstw, torujących drogę profesjonalnym usługom marketingowym dla firm zainteresowanych produkcją, dystrybucją i zakupem nowoczesnych technologii. Dotyczy to szczególnie elektroniki i jej zastosowań w projektowaniu i produkcji maszyn, urządzeń, narzędzi pomiarowych i wszystkich produktów potrzebnych w rozwoju przemysłu na wysokim poziomie technologicznym. Główną siedzibą firmy jest Pittsburgh w stanie Pensylwania.

Warto poświęcić parę słów samemu miastu, bowiem nie przypadkiem tam powstała jedna z pierwszych baz komercyjnych w Internecie. Do niedawna Pittsburgh kojarzył się powszechnie z brudnym przemysłem ciężkim, zanieczyszczeniem środowiska, zatruciem rzek. Od przełomu XIX i XX wieku miasto rozwijało się intensywnie jako ośrodek przemysłu stalowego i wydobywczego. Pittsburgh był wówczas miejscem, do którego zdążały rzesze imigrantów z biednych krajów Europy zasilając szeregi niewykwalifikowanych pracowników kopalni i hut. Po II wojnie światowej powoli lecz konsekwentnie zmieniał się obraz miasta. Od początku lat 70-tych porzucało ono starzejący się przemysł ciężki i weszło w sferę nowych usług i technologii. Dzisiejszy 600-tysięczny Pittsburgh jest ważnym ośrodkiem przemysłu i usług *high-tech*, miastem, w którym działa 6 wyższych uczelni z prestiżowymi *Carnegie Mellon i Pittsburgh University* na czele. W trzech rzekach, które zbiegają się w centrum, płynie czysta woda, a miasto położone na zielonych wzgórzach jest nazywane „pensylwańskim San Francisco".

Usługi w IndustryNET

Na początku lat 90-tych IndustryNET rozpoczęła swe usługi od dystrybucji dyskietek z bazami danych zawierającymi informacje o firmach i produktach; wkrótce do usługi tej dodano dostęp do baz przez telefon (wolne od opłat numery 800), wreszcie jako jeden z pierwszych na świecie zespół firmy rozpoczął serwis *online* w sieci Internet. W chwili obecnej IndustryNET jest największym i najbardziej popularnym źródłem informacji o usługach i produktach dla przemysłu amerykańskiego. Firma nadal rozwija bazę danych stanowiącą elektroniczny przewodnik po rynku produktów i usług dla przemysłu; jest ona obecnie dostępna w sieci, ale także można zamówić wszelkie informacje w formie dyskietek i wydruków. Nadal działają telefony 800. Dostęp do wszelkich informacji jest bezpłatny.

Od 2 lat na czoło usług wysuwa się Forum Rynkowe IndustryNET (*Online Marketplace*), na którym swoje informacje w formie stron WWW umieszcza obecnie 4 000 firm i organizacji, wśród których są takie giganty jak skupiająca setki firm *Telecommunication Industry Association (TIA)*, znane firmy i koncerny międzynarodowe (wśród nich przykładowo Ericsson, ABB, Nissan, Texas Instruments, IBM - patrz lista największych klientów IndustryNET) i małe firmy działające na regionalnych rynkach Stanów Zjednoczonych. Forum dostarcza regularnie odnawiane szczegółowe opisy usług, software, katalogi wyrobów, opisy ich zastosowania, ogłoszenia o wprowadzaniu nowych produktów na rynek etc.

Forum jest medium interaktywnym, tzn. można połączyć się z każdą z „witryn" przy pomocy sieci, zadać pytania, wysłać i otrzymać e-mail. W chwili obecnej z informacji Forum korzysta ok. 180 tysięcy „kwalifikowanych nabywców" - wyselekcjonowanych przy pomocy kwestionariuszy stałych „członków" IndustryNET. Chodzi o to, by zapewnić firmom ogłaszającym się na Forum poważnych klientów. Członkostwo w sieci jest bezpłatne. Poza serwisem *online*, który jest dostępny dla każdego użytkownika Internetu, stali członkowie sieci otrzymują co trzy tygodnie publikację zatytułowaną „IndustryNET Report" - najświeższą informację o tym, co się dzieje na rynku oraz „Directory of Leading Suppliers on Disk" - aktualizowany co pół roku elektroniczny przewodnik po rynku usług i sprzętu. IndustryNET organizuje również regularne seminaria z różnych dziedzin, w których członkowie sieci mają zapewniony bezpłatny udział. Całość „darmowych" usług informacyjnych pokrywają opłaty klientów, a więc firm ogłaszających się czy w jakichś inny sposób wykorzystujących usługi IndustryNET. Cena za utrzymanie typowej strony WWW składa się z opłaty początkowej i abonamentu (ok. 5000 dolarów rocznie). Ceny za duże zamówienia wykraczające poza standard abonamentu są każdorazowo negocjowane.

Poza witrynami poszczególnych klientów na Forum Rynkowym znajdziemy wiele innych źródeł informacji. Najważniejsze z nich to kilkadziesiąt katalogów produktów (*Electronic Catalogs*) i usług (*Online Services*); każdy z nich zawierający aktualną informację i odniesienia do stron WWW głównych producentów danej dziedziny przemysłu. Dysponując gigantycznymi bazami danych o podmiotach działających na rynku IndustryNET wprowadziła ostatnio nową usługą, polegającą na „celowych usługach marketingowych" (*Target Marketing Services*). W dziale tych usług można

zamówić przeprowadzenie badań rynkowych, zorganizowanie kampanii promocyjnej nowego produktu czy też przygotowanie dla działu sprzedaży firmy danych o sytuacji na rynku danego produktu i usługi.

IndustryNET zatrudnia obecnie w swych 17 oddziałach regionalnych 160 osób, specjalistów w dziedzinie informatyki, doradztwa finansowego, ekonomii, marketingu, *public relations* i reklamy. Firma rozwija się bardzo intensywnie i właściwie cały czas przyjmuje nowych pracowników. Na głównej stronie WWW firmy (http://www.industry.net) jest stała rubryka skierowana do osób zainteresowanych pracą w firmie.

Oferując usługi marketingowe innym podmiotom gospodarczym IndustryNET nie zaniedbuje budowy własnego wizerunku. Nad kontaktami z mediami czuwa biuro prasowe firmy (*Press Room).* Każdy może się zarejestrować w bazie biura prasowego - dzięki temu stanie się odbiorcą wszystkich materiałów prasowych i informacji przygotowywanych przez IndustryNET. Są one również dostępne *online*, wystarczy na stronie WWW wybrać opcję „Press Room".

W materiałach prasowych IndustryNET czytamy o liczbie połączeń *online* z bazami danych, która oscyluje ok. 1 mln miesięcznie. Co miesiąc przybywa też ok. 1000 stałych członków sieci. Gwałtowny rozwój usług oferowanych przez IndustryNET ściąga coraz większe zainteresowanie tą forma biznesu. O wzrastającym zainteresowaniu świadczą też zmiany, jakie dokonały się ostatnio w zarządzie IndustryNET. 23 stycznia 1996 r. ogłoszono, że prezydentem i głównym dyrektorem firmy zostaje dotychczasowy szef Lotus Development Corp., Jim Manzi. Manzi, który przez ostatnie 9 lat zarządzał Lotusem i w dużej mierze zbudował potęgę tej firmy, postanowił przyjąć propozycje pokierowania rozwojem IndustryNET i jak oświadczył, zainwestował dość znaczny kapitał w akcje firmy, stając się jednym z głównych jej udziałowców. Twórca IndustryNET, Don Jones, znany i ceniony w kręgach amerykańskiego biznesu, pozostaje nadal prezesem firmy, ale realne kierownictwo spoczywa teraz w rękach Jima Manzi. Osiadły w Bostonie Manzi zamierza przekształcić tamtejsze biuro IndustryNET w równorzędną z Pittsburgiem siedzibę zarządu spółki.

Do mojej prezentacji załączam dodatkowe materiały informujące o:

- „jedenastce głównych baz danych w dziedzinie *online business*,
- informację o Business Centers na Forum Rynkowym IndustryNET,
- informację o Online Services w IndustryNET,
- zmianach personalnych w kierownictwie IndustryNET,
- największych klientach IndustryNET,
- seminariach organizowanych przez IndustryNET,
- charakterystyce firm korzystających z usług IndustryNET.

AS SEEN IN PC WORLD OCTOBER 1995

TOP WEB SITES FOR ONLINE BUSINESS

by **Vince Emery**

1. CommerceNet

http://www.commerce.net

CommerceNet provides guidance about how companies can take advantage of the Internet. (Look under the heading "Reference Information" for background on dozens of ways businesses can use the Internet.) Check out the directories of electronic business consultants and access providers, or browse the entire site from the text-only index.

2. IndustryNET

http://www.industry.net

This is huge online mall where hundreds of manufacturing and wholesaling companies sell new and used industrial products such as engineering software, process equipment and instrumentation, test and measurement equipment, and advanced manufacturing systems; you'll also find news and information. Registration at this business-to-business site is free.

3. Premenos

http:/www.premenos.com

Billing itself as "The Electronic Commerce Resource Guide," Premenos is the place to go for information about electronic commerce and Electronic Data Interchange (a method for passing purchasing, inventory, and shipping information between computers). It offers linked access to network providers, electronic commerce publications, and Internet resources, as well as an up-to-date calendar of offline business events around the world.

4. Business Sites

http://www.rpi.edu/~okeefe/business.html

This frequently updated list of Web sites offers miniprofiles of Net success stories. The site is maintained and organized by Bob O'Keefe, a professor at Rensselaer Polytechnic Institute's School of Management, and limits itself to a select 50 or fewer links.

5. Mouse Tracks

http://nsns.com:80/MouseTracks

New South Network Services, a network provider, provides this catalog of great resources for both online and offline marketing, advertising, and retailing professionals - all served up with a sense of humor.

6. Rutgers Accounting Web

http://www.rutgers.edu/Accounting/raw.html

Part of the International Accounting Network created by Southern Cross University in Australia, this Rutgers University site provides easy access to online accounting, finance, and tax information from all over the world.

7. FINWeb

http://riskweb.bus.utexas.edu/finweb.html

The University of Texas prepares this regularly updated directors of dozens of well-described Web sites dealing with finance, economics, and investments.

8. Yahoo Business Directories

http://www.yahoo.com/business

One of the most up-to-date catalogs of businesses on the Web. You'll find everything here: lists of consortiums; electronic commerce resources (sites with information on specific subjects); a catalog of business directories; and information on taxes, intellectual property rights, and other legal issues.

9. EINet Galaxy's Business and Commerce Directory

http://galaxy.einet.net/galaxy/Business-and-Commerce.html

This well-chosen list of electronic commerce-related Web sites includes topics not usually covered by other business research sites. You'll find useful information on protocols, standards, markets, and business-to-business and business-to-consumer strategies, as well as cross-references to other relevant sites on the how-to's, whys and wherefores of electronic business methods.

10. Information Services for Professionals

http://ioma.com/ioma

This is a very useful (but not comprehensive) directory of hundreds of business-related sites run by the Institute of Management and Administration, a publisher of business and management information newsletters. Topics include administration, finance, management, sales and marketing as well as resources available by specific industry.

11. Electronic Commerce on the World Wide Web

http://amex.cox.smu.edu/mis/cases/webcase/home.html

The Edwin L. Cox School of Business at Southern Methodist University provides these case studies of how business is currently conducted on the Net - and how it might be done better. Topics include key players, what industries benefit the most and why, and how Web marketing differs from traditional marketing.

Vince Emery is the author of How To Grow Your Business on the Internet *(Coriolis Books, $24.99; 800/410-0192).*

Make The Connection For Yourself.

ONLINE SERVICES ON INDUSTRY.NET

- *Industry.Net Online Marketplace*
- *APICS Online*
- *Consulting Online*
- *Control Products Online*
- *Electrical Manufacturing Online*
- *Electronic Components Online*
- *Engineering Software Online*
- *Industrial Computers Online*
- *Manufacturing Systems Online*
- *Material Handling Industry Online*
- *Mechanical Manufacturing Online*
- *Metalforming Online*
- *MROP Online*
- *Networks Online*
- *ODVA Online*
- *PC's & Workstations Online*
- *PLC's Online*
- *Pittsburgh Technology Online*
- *Power Transmission Online*
- *SMC Online*
- *Telecommunications Online*
- *Test & Measurement Online*
- *Valves & Actuators Online*

Over 180,000 of today's top industry professionals now come to Industry.Net for the information they need to make purchasing decisions. And together they spend over $165 billion per year.

These buyers and specifiers rely on Industry.Net for the latest industry news, product and service announcements, application stories, and other information vital to their companies. And it's here they expect to find you and *your* company.

That's why almost 4,000 of industry's leading manufacturers and suppliers have already established Business Centers with us -- and why over 200 more are coming online every month.

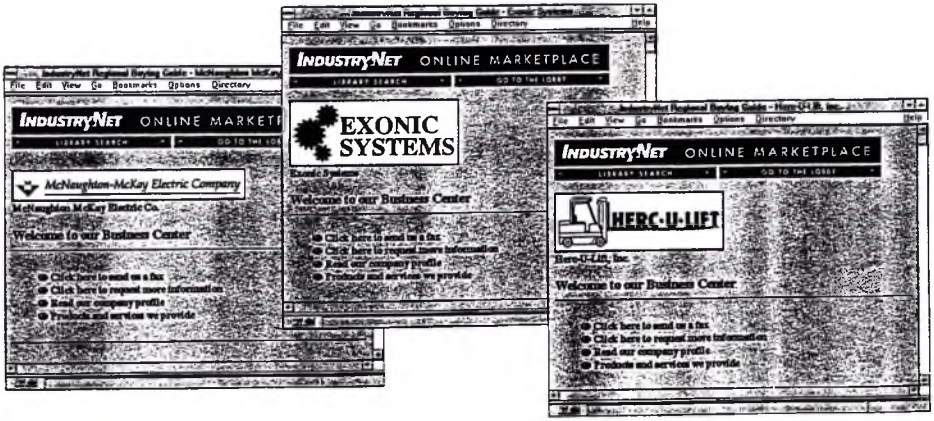
So, if you want to make the ultimate business connection, too -- make the connection to Industry.Net. For information on how you can become a member, call Jennifer Gilman today at 1-800-266-8724.

Business Centers on Industry.Net.

Electronic Business Centers are the "locations" that industry professionals visit to do business online. And because they're open 24 hours a day, 7 days a week, they make sure a supplier's information is always right at a customer's fingertips when purchasing decisions are being made.

But Industry.Net's advanced interactive system doesn't stop there. It also connects buyers and sellers via e-mail, and tracks all activity in every Business Center. So it can report interested prospects within minutes, and provide a complete profile of anyone who visits a site online.

Only an Industry.Net Electronic Business Center delivers this kind of powerful, fully-functional online performance -- the kind of performance you need to compete in regional, national, and even global markets. That's what makes it the ultimate business connection for today's fast-moving world.



Major Companies Who Use Industry.Net To Find Manufacturers & Suppliers.

Thousands of buyers and specifiers from these major companies use Industry.Net every day to find companies like yours.

Partial listing of major companies using Industry.Net (over 1,000 employees per location).

3M Company
A. C. Delco Systems Div. of G. M.
A. K. Steel
A. M. Multigraphics
A. O. Smith Co.
AB SANDVIK Coromant
ABB Combustion Engineering
ABB Industrial Systems
ABB Process Automation
Abbott Laboratories
Abex/NWL Aerospace
AC Delco Systems
AC Rochester
ACCRA-PAC INC
Acme Frame Products
ADEQ
ADF Inc./NASA Lewis Research Cntr
Advance Transformer Co.
Advanced Micro Devices
Advanced Systems Development Inc.
AEG Transportations Systems Inc.
Aerojet Electronic Systems
AEROQUIP INOAC
Aerospace Design and Fabrication
AEROTEK
Aetna Ind.,Inc.
AFG Industries
Air Products and Chemicals, Inc.
Aircraft Braking Systems Corp.
AK Steel Corporation
Akron Beacon Journal
Aladan Corp.
Alberta Energy Company Ltd.
Alberta-Culver Company
Alcan Smelters & Chemicals Ltd
Alcatel Data Networks
Alcoa
Alfa Laval Separation
Algoma Steel Inc.
Allegheny Ludlum
Allegheny Power Service Corporation
Allen-Bradley Company
Alliance Capital Management Corp.
Alliant Techsystems Inc.
Allied Signal Inc.
AlliedSignal Aerospace Co.
AlliedSignal Automotive
AlliedSignal Engines
AlliedSignal Fibers
AlliedSignal Technical Services Corp.
Allison Engine Co.
Allison Gas Turbine
Allstate
Alpena General Hospital
Alsco
ALUMAX
Alza Corporation
AM GRAPHICS
AM MULTIGRAPHICS
AMANA REFRIGERATION
American Axle & Manufacturing
American Bumper & Mfg. Co.
American Business Information
American Cyanamid
American Electric Power Serv. Corp.
American Fiber & Finishing
American Greetings Corporation
American Home Foods
American National Can Company
American Saw & Mfg. Co.
American Sterilizer Company
American Uniform Co.
Americhem, Inc.
Americold Compressor
Ames Lab
Amgen
AMI Semiconductors
Amoco Fabrics & Fibers Company
Amoco Oil Company
AMP Inc
Amtrak
AmTran Corporation
Amway Corp.
Analog Devices, Inc.
Anchor Hocking Specialty Glass
Andersen Consulting
Anheuser Busch Company
ANR PIPELINE
ANSELL EDMONT
AP Technoglass co.
Apple Computer, Inc
Appleton Papers, Inc.
Applied Materials, Inc.
Applied Research Labs
APV
APV CREPACO
ARCO Alaska Inc.
ARCO Chemical Co.
ARDEC
Argonne Laboratory
Aristech Chemical
Aristocrat Leisure Industries Pty. Ltd.
Aritech/Moose
Arizona Public Service
Armco AMC
Armco Steel Company, L.P.
Armour Pharmaceutical Company
Army Research Laboartory
Arthur D. Little, Inc.
Arvin NAA
Asea Brown Boveri
Ashland Chemical, Inc
Ashland Petroleum
Aspect
AST Computer
astec ind.
Astra USA
AT&T Bell Labs
AT&T EasyLink Services
AT&T Global Information Solutions
AT&T Microelectronics
AT&T Network Systems
AT&T NWSBU
Atlantic City Medical Center
Atlantic Steel
Atomic Energy of Canada Limited
Auburn Foundry, Inc
Austin Quality Foods
Autodie International Inc.
Automatic Switch Co.
Automation Tooling Systems
Aviation Supply Office
Avon Products, Inc.
B F Goodrich Aerospace
Babcock & Wilcox
Bailey Controls Co.
Baltimore Gas & Electric
Barclays Bank PLC
BASF Corporation
Batesville Casket Company
Battelle Memorial Institute
Batts Inc.
Baxter Healthcare
Beaulieu Nylon
Bechtel Petroleum
Becton Dickinson
Belden Wire & Cable
Bell & Howell Co.
Bell Atlantic
Beltone Electronics
Bemis Co. Inc
Bently Nevada Corp
Berkley
Bernhardt Furniture Co.
Besser Company
Best Lock Corp.
Best Power Technology, Inc.
Bethlehem Steel Corporation
BHP Slab and Plate Products
Bil-Mar Foods
Bimm Inc.
Biomet Inc.
Black & Decker
Black & Veatch
Black Box Corporation
Bodine Electric Company
Boeing Computer Services
Boeing Defense & Space Group
Boeing Helicopters
Boeing Information Services
Boise Cascade Canada
Boise Cascade Corp.
BorgWarner
Boston Gas Company
Bourns, Inc.
Brach & Brock Confections
Bridgestone/Firestone Inc.
Briggs & Stratton
Bristol Myers Squibb. Co.
Brock
Brookhaven National Laboratory
Brooklyn Union Gas
Brooks Instrument
Brown & Root, Inc.
Brown & Williamson
Brown Printing Company
Brunswick Corp
Brush Wellman Inc
Brutus
Buckeye Steel
Bucyrus Erie
Budd Company
Bull HN Information Systems
Burgess-Norton Plt. #6
Burlington Northern
Burns & McDonnell Engr
Burns Chemical
Burr-Brown Corp
Bush Industries, Inc.
BWX Technologies
Cabot Corp.
Cabot Performance Materials
CACI, Inc.
cad designs
Cadence Design Systems
Cadillac Luxury Car Division, GMC
Cady Bag Company Inc.
CAE-Link
Calspan Corp.
Carbaloy Inc.
Cardiac Pacemakers Inc
Cargill Fertilizer, Inc.
Carlisle SynTec Systems
Carlisle Tire & Rubber
Carolina Power & Light Company
Carpenter Technology Corp
CarTech
Case Corp.
Caterpillar,inc
CBI Tech Services
CBS TV
CEBAF
Centerior Energy
Centerior Service Co.
Century Products Company
Cerro Matoso S.A.
Cessna Aircraft
Champion International
CHAMPION SPARK PLUG
Char-Broil (div. of W.C. Bradley Co.)
Charles Stark Draper Laboratory
Charlotte Pipe & Found., Plastics Div.
Cherry Electrical Products - Auto.
Chevron USA
Chore-Time Brock
Chromalox
Chromium Corporation
Chrysler Corporation
Church & Dwight
CIBC
Cincinnati Incorporated
Cincinnati Milacron
Citgo Petroleum Corp.
Citicorp
Citicorp Securities, Inc.
Claremont Technology Group
CLCD-Parma, Div. of General Motors
Cleveland Cliffs Iron Co.
Cleveland Public Library
CNA Insurance
CNG Transmission
Co-Steel Raritan
Coatesville VAMC
Cold Spring Harbor Laboratory
Collins & Aikman Corp.
Colonial Rubber Works
Columbia Gas Transmission
Columbus Coated Fabrics
Columbus Foundries
Columbus Regional Hospital
Comdata Corporation
Comdisco, Inc.
ComEd
Commercial Intertech Corp.
Commonwealth Aluminum Corp.
Commonwealth Edison
Computer Sciences Corporation
Computervision Corp
Compuware
Comsat Corp
Concurrent Technologies Corp.
Connaught Laboratories Inc
Conoco, Inc.
Conrail
Consol Inc.
Consolidated Diesel Company
Consolidated Papers, Inc.
Consumers Power Company
Contraves USA
Control Data Systems, Inc.
Control Solutions
Convex Computer Corp.
Cooper Industries
Cooper Power Systems
Cooper Tire
Coors Brewing Co
Copeland Corporation
Corning Incorporated
Corning Vitro
CPC International
Cray Research
Crosfield Electronics LTD
Crown Equipment Corporation
CRYDOM
Cryovac, Div of W.R.Grace & Co.
CSC Index

CSIRO Division of Mfg Tech
CTA INCORPORATED
CTC
Cubic Defense Systems
Culligan International Company
CUMIS Insurance Society, Inc
Cummins Engine Co.
Cummins Industrial Center
CURRIES CO.
Curwood,Inc
Cutler-Hammer, Westinghouse Prod.
Daewoo Telecom
Dale Electronics
Dana Corporation
Daresbury & Rutherford Appleton Lab.
Data General Corporation
Datastream
David Sarnoff Research Center
Davy International
Day and Zimmermann Inc.
Dayton Products Div./ Emerson Elec.
DEC
Deere & Company
Defence Science & Technology
Defense Industrial Supply Center
Defense Information Systems Agency
Degussa Corp.
Delco Chassis, Div. of GM
Delco Electronics
Delco Remy America
Delredo SA DE CV
Delrina Technology, Inc
Delta Air Lines
Delta Faucet
Department of Commerce/ITA/IA
Department of Defense
Dept of Economic Sec., Aging & Adul
Department of Industrial & Eng. Tech.
Department of Treasury
Dept. of the Navy
Dept. of Water & Power
DePuy
Detroit Diesel Co.
DeZURIK, A Unit of General Signal
Diesel Technology Co.
DIGI MATEX, INC.
Digital Equipment Corp.
Digital Semiconductor
Diversey Corp.
Donnelley Printing
Dow Chemical Canada Inc.
Dow Chemical Co
Dow Corning Corp
Dresser-Rand
Drexel Heritage
Dreyer Tool & Die
Duke Engineering & Services, Inc.
Duke Power Company
Dun & Bradstreet - Info. Serv. NA
Duo-Fast Corporation
Duplex, Inc.
DuPont Company
Duquesne Light Company
Dynamics Research Corporation
E-Systems, Melpar Division
E.F. Johnson
E.J. Brach Corp.
East Driefontein Gold Mine
East Penn Mfg Co Inc
Eastman Chemical Company
Eastman Kodak Co.
EATON Corporation
Eaton Technologies
Ecusta Division, P.H.Glatfelter Co.
Edmonton Telephones Corp.
EDS
EDS/AC Delco Systems
EDS/Delco Electronics
EG&G Mound Applied Technologies
Elana Corporation, Inc
Electra-Motive General Motors Corp
ELECTROMAGNETIC SCIENCES INC
Electronic Data Systems
Eli Lilly & Co.
Elkay
Elkem Metals Company
Elliott Company
Elliott Turbomachinery Co.
Elsag Bailey Process Automation
Empire Brushes
Engelhard Corp.
Environmental Protection Agency
Equitable Resources Inc.
Ericsson, Inc.
Ernst & Young Mgmt Consultants
Essex Group Inc
Ethicon Endosurgery
European Space Agency
FaberCastell Corp.
Fabri-Center Of America, Inc
Fairbanks Morse Eng. Div. Coltec Ind.
Fairmont Tamper
Falconbridge Ltd
Fannie Mae
FANUC USA Co.
Fasco Controls
Federal Aviation Administration
Federal Cartridge Company
Federal Express Corp.
Federal Mogul Corporation
Federal Paper Board
Federal Signal
Federal-Mogul Corporation
Ferco Ford Elec Refridg Connersville
Fermi National Accelerator Lab.
Fermilab
Ferno-Washington, Inc.
Fieldcrest Cannon, Inc.
Financial Alliance
Fingerhut Companies
Firestone Tire & Rubber Co.
Fischer & Porter Company
Fisher & Paykel. PSC Section
Fisher Controls
Fisher Rosemount Systems, Inc
Fisher Scientific
Fisher-Price
Fleetwood Folding Trailers
Florida Power & Light Company
Ford Motor Company
Ford Motor Company of Canada Ltd
Fort Howard Corp
Foseco, Inc.
Foss Manufacturing Co. Inc.
Foxboro Co
Frigidaire Company
Furman Selz, Inc.
Furnas Electric Co
G.T.E
Gardner Denver Machinery Corp.
Gast Mfg. Corp.
GE Aircraft Engines
GE Appliances
GE CANADA
GE Fanuc Automation
GE Lighting Systems
GE MOTORS
GE Plastics
GE Superabrasives
GEC-Marconi Electronic Sys. Corp.
GenCorp Automotive
General Binding Corporation
General Dynamics
General Electric
General Extrusions
General Foods Bakery Cos.
General Motors - Flint Metal Fab.
General Motors - Powertrain Division
General Motors Corp. CLCD
General Motors Corp. NAO Mfg. Cntr
General Motors Corporation
General Motors Powertrain
General Motors R&D Center
General Motors Technical Center
General Motors Truck Platform
General Services Administration
General Tire
gentex corporation
Georgia Power Co.
Georgia-Pacific
Giddings & Lewis Co.
Gilbarco Inc.
Gill Mfg
GLAXO
Globe Net Inc.
GM Hughes Information Tech. Co.
GM Powertrain
GM Powertrain - Machine Tool Div.
GM Powertrain Bay City
GM, Allison Transmission
GoldStar Industrial Systems
Goodyear
GPS TECHNOLOGIES
GPU Service Corporation
Graco
Gradall Co.
Granite City Steel
Great American Knitting Mills
Great Dane Trailers Inc.
Great Lakes Steel
Grimes Aerospace
Group Dekko
Grove Cranes
Grumman Aerospace
GRUMMAN LONG LIFE VEH.
Grupo IMSA
GSA
GTE
GTSI
Guardian Industries Corp
Gulf States Paper Corp
Gulf States Steel, Inc.
Gulfstream
Guy Tessier Consulting
H J HEINZ
H.A. Simons
Hale and Dorr
Hamilton Beach Proctor Silex
Hamilton Standard
Hankook Tire Co.
HANOVER FOODS CORP.
Hardinge Brothers, Inc.
Harris Corporation
Harris Semiconductor
HARRISON DIVISION GMC
Harrison Steel Castings Co.
Harte-Hanks Comprint
Hatfield Quality Meats Inc.
Haworth, Inc.
Hayes Albion Corporation
Haynes International, Inc.
heartland food co.
Heery International
Heinz USA
Helene Curtis USA
Henkels & McCoy,Inc
Hercules Incorporated
Hershey Chocolate USA
Hewlett Packard
Hi-Stat Mfg.
Hill-Rom Co.
hillshire farm & kahn's
Hoechst Celanese
Hoffman Engineering Company
HOGSHEAD INC
Hoke Inc
Holiday Rambler LLC
Honda Of America
Honeywell
Honeywell Comm. Flight Sys. Gr.
Honeywell Europe
Honeywell HBC
Honeywell Inc., Micro Switch Div.
Honeywell Military Avionics
Huffy Bicycles
Hughes
Hughes Danbury Optical Sys., Inc.
hughes network systems inc.
Hughes STX
Humboldt-Universitaet
Hunt Foods
Hyatt Regency Chicago
Hydro-Quebec
IBM
IBM Microelectronics
IBM Research
IBP INC.
ICF Kaiser Hanford
ICI Americas
IDS Financial Services, Inc.
IES Industries
Illinois Power Co.
Imed Corporation
IMI Cornelius Inc.
IMP Group Ltd., Aerospace Div.
IMS America
In-Sink-Erator Div.
INA BEARING COMPANY, INC.
Inco Alloys International, Inc.
Industry Canada
Ingersoll Milling Machine Co.
Ingersoll Cutting Tool Company
Ingersoll Dresser Pump
Ingersoll-Rand
Inland Fisher Guide
Inland Steel Company
INRIA
Intel Corporation
Intergraph Corporation
International Paper Company
Invacare
INX International Ink Company
Irving Forest Services Ltd.
ISI Robotics
ISIS Distributed Systems
ITT A-C Pump
ITT BARTON
ITT Hartford
ITW Inc.
J&L Specialty Steel
James River Corp.
Jervis B. Webb Co.
Jet Propulsion Laboratory
JLG Industries, Inc.
JOHN CRANE, INC.
John Deere Ottumwa
Johnson Controls Inc.
Johnson Yokogawa Corporation
johnsonville foods, inc.
JOY Technologies
K. A. STEEL CHEMICALS
Kaiser Engineers/Hanford Co
KAMAN INDUSTRIAL TECHNOLOGEIS
Keebler Company
Keithley Instruments
Kellogg USA, Inc.
Kemet Electronics
Kemira Pigments, Inc
Kennametal
Kerr-McGee Corporation
Key Services Corp.
keystone carbon co.
Keystone Steel & wire
Kidd Creek Mines
Kidder, Peabody
Kimball Electronics
Kimball Electronics Group
Kimberly-Clark Corp.
Kimble Glass Inc
Kingsbury Corporation
Knape & Vogt Manufacturing
Koch Industries, Inc.
Koch Refining Company
Kodak Canada Inc
Kohler Company
Koppel steel corp
kovatch corporation
Kraft General Foods Canada
Kraft USA
KraftMaid Cabinetry, Inc.
Krohne America
KUMHO & CO.,INC
la-z-boy chair company
Lake Region Manufacturing Co., Inc.
Lam Research Corp
Lamb Technicon
Land O'Frost, Inc.
Landis & Gyr Powers, Inc.
Lawrence Livermore National Lab.
LEAR SEATING CORPORATION
Lectron Products
Lederle Labs
Leeds and Northrup
LEGO Systems Inc
Lever Brothers Co.
Lexmark International, Inc.
Liberty Mutual
Liebert Corp.
Life Fitness
LifeScan inc.
Liggett Group
Lincoln Electric Co.
LINVATEC
LITCO
LITTELFUSE
Litton Poly-Scientific
LITWIN
Lockheed Advanced Development Co.
Lockheed Aeronautical Systems Co.
Lockheed Idaho Technologies Co.
Lockheed Sanders
Lockwood Greene Engineers
LOCTITE CORPORATION
Loral Defense Systems-Akron
Loral Federal Systems
Loral Space Information Systems
Lord Corp
Lorillard Research Center
Los Alamos National Lab
Los Angeles Dept of Water & Power
Louis Perry & Assoc.
LoveStory Co.
LSI Logic Corporation
LTV Steel Company, Inc.
Lubrizol Corp.
Lukens Steel
Lund Institute of Technology
Mac Tools
MacMillan Bloedel Limited
MacNeal Schwendler Corporation
Madison Kipp Corp.
Magcorp
Magee Carpet Company
Magnavox Electronic Systems Co.
Magnetics
Mallory Controls
Malt-O-Meal Company
Manpower Temporary Service
Marathon Oil Company
Maricopa County
Marion Merrell Dow
Marquip Inc.
Martin Marietta Control Systems
Martin Marietta Corporation
Martin Marietta Defense Systems
Martin Marietta Govt Electronic Sys
Martin Marietta Technologies Inc.
Martin Marrietta Control Systems
MasterCraft Boat Company
Mastercraft Fabrics
Matrix Essentials, Inc.
Matrox Electronic Systems
Matsushita Elec. Components
Maytag Company
Maytag Hermn Laundry Products
Mayville Engineering Co.
Mazak Corporation
Mc Donnell Douglas
McGraw-Hill
MCI
MCI Data Services
McKee Foods Corporation
McKinsey & Company, Inc.
MDT Corp.
Mead Coated Board
Mead Paper
Medeco Security Locks, Inc.
Medtronic, Inc
Melroe Company
Memtec America Corp.
Menard, Inc.
Mentor Graphics Corp.
Merck & Company, Inc.
Merck Research Laboratories
Mercy Information Systems
MESC Electronic Systems Inc
Metric Systems Corp.
Metro Information Services
Mettler - Toledo, Inc.
MGM Grand
Michelin Tire Corporation
Micro Craft Technology
Micro-Rel
MicroAge
Microchip Technology Inc.
MICROCOMPUTO
Micron Semiconducter
Microsoft
Mid-South Electric
Midland Brake
Midwest Industries
Midwest Power
Miles, Inc.
Miller Brewing Co.
MILLER Electric Mfg. Co.
Minco Products
Mine Safety Appliances Company
Mineracao Morro Velho
Minster Machine Company
Mitsubishi Semiconductor America, Inc

MKS Instruments Inc
ML-KS Bearings Inc.
Mobil Oil
Mobil R & D Corp
Modicon Inc.
Mohican Mills, Inc.
Monarch Marking Systems
Monsanto
Moog Inc.
Moore Products Company
Morgan Corporation
Morgan Foods
Morrison Knudsen Corp
MOTOR COACH INDUSTRIES
Motorola Inc
MSA Instrument Division
MTC
Munhwa Broadcasting Corp.
murata electronics
N.A.S.A. Lewis Research Center
Nabisco
Nalco Chemical Company
NASA - Langley Research Center
NASA / Goddard Space Flight Center
NASA Ames Research Center
NASA Langley Research Center
Nasa Lewis Research Center
nasa-marshall space flight center
National Center For Mfg. Sciences
National Forge Company
National Institute of Standards & Tech
National Instruments
National Machinery Co.
National Renewable Energy Lab.
National Research Council
National Steel Midwest Division
National Steel - Granite City Division
National Steel - Great Lakes Division
NAVISTAR
Navy Public Works Center
NAWC
Neville Chemical Co
New Hampton, Inc.
Newark Electronics
Newport Steel Corp
Nippondenso Tennessee
Nissan Motor Mfg Corp., USA
Norand Data Systems
Nordson Corporation
NORFOLK SOUTHERN CORP.
NORGREN
NORHTROP GRUMMAN CORP.
North American Comm., Inc.
North American Mfg. Co.
North Atlantic Energy Service Co.
Northeast Utilities Service Company
Northern Telecom
Northrop ESD
Northrop Grumman
Norton Co
Norwalk Furniture Corporation
Novacor Chemicals Limited
Novell, Inc.
NTN-Bower
NuTone Inc.
OHM Corporation
Ohmeda
OLIN CORPORATION
Olin Winchester
Ontario Corporation
Oregon Steel Mills
Oscar Mayer Foods
OSi SPECIALTIES, INC.
Osmonics, Inc
Osram Sylvania
Otis Elevator
Outdoor Technologies Group
Owens Corning
Owens Corning Science & Technology
Owens Illinois
Owens-Brockway Glass Containers
PA Pressed Metals
pacific bell
Pacific Gas & Elect Co
Pacific Telesis
PacifiCare
Packaging Corp
Packard Bell
Packard Electric
Panametrics, Inc.
Panduit Corp.
Panhandle Eastern Pipe
Pantaloons Productions
Parke-Davis Div. Warner-Lambert Co.
Parker Hannifin Corp.
PCC Air Foils
Peabody Myers Corp.
PECO Energy Company
Pencom Software Company
PENN LINE SERVICE
Penn Power
Pennsylvania Power & Light Co.
Peoples Gas
Pepperl & Fuchs
Perkin Elmer corp
pfalzgraff
Pfizer Pharmaceuticals
Phar-Mor
Phifer Wire Products Inc
Philadelphia Electric Company
Philadelphia Naval Shipyard
Philadelphia Newspapers, Inc.
Philip Morris
Philips Consumer Electronics
Philips Display Components Co
Philips Process & Mach. Automation
Philips Semiconductors Inc.
phillips petroleum co
Phillips Pipe Line Co.
Picker International
Pierce Mfg. Inc.
Pillsbury
Pioneer Hi-Bred Intl Inc.
Pioneer-Standard Electronics
Pitney Bowes
Plasti-Line, Inc.
Playtex Products Inc.
Pmi Food Equipment Group
PNI
POPE & TALBOT, INC.
POSS
Potlatch Corp.
Potomac Electric Power Co
Powertrain Warren Div Of GM
PP&L Co.
PPG
Pratt & Whitney
PRC
Precision Interconnect
PreMark International
Premix Inc.
Presbyterian University Hospital
PRESIDENT BAKING COMPANY
Primerica Finacial Services
PrimeWood, Inc.
Prince Corp
Procter & Gamble
Progressive Insurance Co.
Promus Companies
Providence Metallizing Co., Inc.
PSE&G
PSTI
Puget Sound Naval Shipyard
PURethane, Incorporated
QMS, Inc.
Quad Graphics
Quaker Oats Company
Quantum Chemical Company
R R DONNELLEY & SONS
R. D. Werner Co. Inc.
R. J. Reynolds Tobacco Co.
Rapistan Demag
Ravenswood Alum. Corp.
Raychem Corporation
Raytheon
Raytheon Engineers & Constructors
Reliance Electric
Rensselaer Polytechnic Institute
Resipironics, Inc
Rexnord Corporation
Reynolds and Reynolds
Reynolds Metals Co.
Ridge Tool Company
RMI Titanium Co.
RMS Technologies Inc.
Robert Bosch
Robertshaw Controls
ROBROY
Rockwell Automation / Allen-Bradley
Rockwell Automotive
Rockwell International
Rockwell Software
Rockwell Space Operations Co.
Rockwell Tactical Systems
ROHR, INC
ROQUETTE AMERICA
Rosemount Inc
Rouge Steel
Roush Technologies
RPD, Abbott Labs
Rubbermaid Commercial Products
Russell Corp.
Rycotonics
Saginaw Division, GM Corp.
Saint Gobain/Certainteed Corporation
Samsung Aerospace Industries, Ltd.
Samsung Electronics
San Antonio Air Logistics Center
San Diego Gas & Elec
Sandia Labs
Sandvik Coromant
SANDVIK STEEL
Sara Lee Bakery
Sara Lee Knit Products
Sargent & Lundy
Saturn Corp.
Schlumberger
SCHNEIDER
Science Applications Intl Corp.
Scientific Atlanta
SCM Chemicals
Scot Industries, Inc.
SDRC
SDSU
Seaboard Corporation
Seaboard Farms of Athens
SEI Corporation
SELLERS ENGINEERING CO
SEMATECH
Senco Products Inc.
Sensus Technologies
Sequent Computers
SERNAGEOMIN
ServiceMaster
SGL Carbon
Shaw Industries, Inc.
Sherwood Medical Co.
Shop-Vac Corp
Siebe Environmental Controls
Siemens Automotive
Siemens Corporation
Siemens Energy & Automation
Siemens Industrial Automation, Inc.
Siemens Nixdorf Information Sys. AG
Siemens Power Corp
Siemens Stromberg Carlson
Sikorsky Aircraft
Silicon Graphics
Singapore Computer System Limited
SmithKline Beecham
So. Charleston Stamping & Mfg.
Solar Turbines Incorporated
Soleil Industries
Sonoco Products Co.
Southam
SOUTHERN COMPANY SERVICES
Southwestern Bell Telephone
Space & Naval Warfare Sys. Command
Spectra-Physics
SPEED QUEEN COMPANY
Spencer's Inc.
Springs Industries, Inc.
SPROCKETS, INC.
Square D Company
SRI International
SSI TECHNOLOGIES, INC.
Sta-Rite Ind .
Standard Microsystems, Corp.
Stanford Linear Accelerator Center
STATE INDUSTRIES
Steel Heddle
Steelcase Inc.
Stelwire Ltd., A sub. of Stelco Inc.
Stihl,Inc.
Stolle Products
Stone & Webster Engineering Corp.
Storage Technology Corp.
StorageTek
Sun Electric Corp.
Sun Microsystems
Sun Pipe Line Co.
Sutherland-Schultz Inc.
Sverdrup Technology
Sveriges Television
sweetheart cup company inc
Symbiosis
Syncrude Canada Limited
System Sensor
System Software Associates
Systems Research Labs.
Tandem Computers Incorporated
Tandy Corp
Taylor Co.
Taylor Packing Co. Inc.
Techneglas
Technicolor
Telecom Australia Research Lab.
Telecommunications Inc
TELEDYNE ALLVAC
Teledyne Brown Engineering
teledyne water pik
Tellabs Operations, Inc.
Telxon Corp
Tembec Inc
Tennant Co
Tennessee Eastman Division
Teradyne, Inc.
Texaco Inc.
Texas Gas Transmission Corp.
Texas Instruments, Inc.
TEXTRON AEROSTRUCTURES
TH-Darmstadt
The Aerospace Corp
The Boeing Company
The Buschman Company
The Campbell Group
The Canadian Red Cross Society
THE CHINET COMPANY
THE COOPER TIRE COMPANY
The Flexible Corporation
The Ford Meter Box Co., Inc.
The Foxboro Company
THE FRIGIDAIRE COMPANY
The GAP
The L. S. Starrett Company
The Ladish Co., Inc.
The Longaberger Company
The Pillsbury Company
The Ridge Tool Co.
The Timken Company
The Toro Company
The Torrington Company
The Trane Company
The Valspar Corporation
Therma-Tru Corp
thermodisc
Thilmany International Paper
Thomson CE
thomson consumer electronics
Thorn Apple Valley
Time Life Inc.
TIMES FIBER COMMUNICATIONS
tootsie roll ind.
Torrington Co.
Toshiba International Corp.
Toyota Motor M. C.
TPI Corporation
Traco
Tracor Applied Sciences, Inc.
Trane Co.
Trans-Apparel Group
TransCanada Pipelines
Tropicana Products Inc.
Truth Hardware
TRW Automotive Steering & Suspen.
TRW Ballistic Missiles Division
TRW Inc
TRW Steering & Suspension Division
TRW Vehicle Safety Systems, Inc.
U S Precision Lens Inc.
U. S. Steel Corporation
U. S. Steel Irvin Wks.
U. T. Automotive
U.S. Borax
U.S. Steel Gary Works
U.S.X.
Uarco Inc.
Underwriters Laboratories
UNICOR
UniMac, A Division of Raytheon
Union Camp Corp.
Union Carbide
Union Oil of California
Union Special Corp
Union Switch & Signal
Uniroyal Goodrich Tire Co.
unisys corp.
United Defense - FMC
United Parcel Service
United States Postal Service
United Technologies
United Technologies Automotive
United Technologies Carrier
United Technologies Research Center
Unitel Communications Inc.
Upstate Milk Cooperatives, Inc.
US Electrical Motors
US General Services Administration
US Precision Lens Inc.
US West Marketing Resources Group
USS/Kobe Steel Co.
USX/US STEEL
UT Space Institute
Utica Engineering
UTILIMASTER CORP.
Valmet Automation Inc
Valtek, Inc
Vastar Resources, Inc.
Veda Inc
Velcro USA INc.
Videojet Systems
Virginia Power
Vistakon, Inc
Volvo GM Heavy Truck Corporation
W.R. Grace & Co.
W.W. Grainger, Inc.
Wabash National Corp.
Wagner Lighting
Wang
Warner Electric
Warner Lambert Co.
Washington Steel Corp
Water Authority of Western Australia
WCI Steel
Webcraft Technologies, Inc.
Weirton Steel Corp.
Weldun International
Werner Co.
Wesley-Jessen
West Bend Company
West Penn Power Company
western sugar co.
Westighouse Electric Corp.
Westinghouse Electronic Systems
Westinghouse Hanford Co.
Westinghouse PCD
Westinghouse Plant Apparatus
Westinghouse Power Systems
Westinghouse Savannah
Westinghouse Science & Tech Cntr
Westinghouse/DCBU
Weyerhaeuser Co.
Wheaton Industries
Whessoe Varec
Whirlpool Corp.
Wilcox Electric
Williams Electronics
Williams International
Williams Trading Services
Winnebago Industries
Wisconsin Electrci Power Company
Wix/Dana Corporation
WL Gore & Associates, Inc
World Vision Enterprise
Wynn's Precision, Inc.
Xerox
Yokogawa Electric Co.
YORK INTERNATIONAL CORP.
Zilog Corporation
Zimmer Inc., Div. Bristol-Myers Squibb
Zinc Corp. of America
Zoom Telephonics Tech Support
Zum Energy Division
ZYTEC CORPORATION

Jim Manzi Takes Helm at Industry.Net, The Internet Online Commerce Leader

Former Lotus Executive Appointed President/CEO; Makes Equity Investment

Pittsburgh, PA - Jan. 23, 1996 -- Industry.Net today named Jim Manzi its president and chief executive officer. Industry.Net, (www.industry.net) is the developer of a leading Internet-based business-to-business online marketplace. Donald H. Jones, the nationally recognized entrepreneur who founded Industry.Net in 1990, will remain chairman of the company.

Jim Manzi, President & CEO. Right: Don Jones, Founder & Chairman.

Manzi, who built Lotus Development Corp. into a billion-dollar company over his nine-year tenure as president, CEO and chairman and is credited with turning groupware and workgroup computing from technology buzzwords into critical business applications, also announced that he has made a substantial equity investment in Industry.Net and is now a significant shareholder in the privately held company.

"Many companies are trying to climb aboard the Internet phenomenon, but in Industry.Net, Don Jones had created the definitive example of how to actually build a market and make money from Internet commerce," said Manzi. "Industry.Net is a leader in business-to-business commerce on the Internet because it has made it fast and easy for buyers and sellers to conduct their day-to-day business electronically. It enables companies to promote their offerings to a huge audience of prospective customers and allows those customers to find the products and services they need instantly.

"My experience is that this whole industry is driven by people and by brainpower. It is intense in that respect. I have been extremely impressed by all the people at Industry.Net and I hope to be able to attract that kind of talent to help Industry.Net reach its full potential."

"Jim's vision of the enormous potential of network computing actually set the stage for much of what is happening on the Internet and the World Wide Web today," said Industry.Net Chairman Jones. "And now that we have built the critical mass of vendors, content, and users necessary to make online electronic commerce an everyday reality, Jim is just the experienced chief executive we need to help us take Industry.Net to the next level and realize the business potential we have created."

To accommodate the tremendous growth of its network, which now includes buyers and specifiers from over 36,000 companies, Industry.Net said it will expand its current Boston office to share headquarters duties with Pittsburgh, and that substantial expansion is slated for both offices. "Industry.Net members already have the power to purchase more than $165 billion worth of products and services every year, and we plan to make it possible for them to do more and more of their business online in the future," Manzi said.

Industry.Net has grown an average of 200% a year since 1991, and is now a leading Internet-based business-to-business online marketplace serving business and industry in North America. The company's products and services include: Online Services, Industry.Net Directory of Leading Suppliers, Industry Publications, Market Research, and Target Marketing Programs for business professionals.

Industry.Net Corporation

Industry.Net was founded in 1990 with the goal of streamlining industry's buying and selling process. The company has created a unique suite of interactive electronic and print media which offers industry professionals a faster, easier, and more productive way of conducting business. Industry.Net is a privately held company headquartered in Pittsburgh, Pennsylvania with more than 150 employees and 17 regional offices.

Industry.Net Special Events

Industry's most respected seminar series

Industry.Net Special Events brings you hands-on seminars featuring the industry's latest developments and technology. SEMINARS ARE FREE TO INDUSTRY.NET MEMBERS.

SPACE IS LIMITED - Call 1-800-266-8724
or use the INFO-Express card for more information.

Presented by CSI, Inc.

CSI, Inc.
Computer Systems Integration

Learn about the Latest in Manufacturing Execution Systems @ This FREE Seminar

This could be the most useful two hours you spend this year! We know it's hard to get away form the mountain of work at your desk, but this event brings you current information that you can't afford to be without. Learn how you can **improve** on time performance, **reduce** inventory, **gain** greater operational control and **meet** ISO 9000 standards. Experts will demonstrate the latest in: • **Windows '95 and UNIX manufacturing/ accounting systems** • **Integrated bar coding/data collection systems** • **Integrating EDI and shipping manifest systems.**

DATE: March 21, 1996

TIME: 8:30 am to 11:30 am

LOCATION: CSI, Inc., 2300 North Barrington Road, 4th Floor, Hoffman Estates, IL

Continental Breakfast Included

TO PREREGISTER:
Call 1-800-266-8724 or circle **#201**

Presented by BEA electro-optics, inc.

Electro-Optic and Laser Advancements

Four seminars on Electro-optics and Laser technology all in one day: • **Radiometry and Photometry** *(8:30-10:00 or 1:30-3:00)* -- The science of light measurement • **Silicon Photodetector Technology** *(10:30-12:00 or 3:30-5:00)* -- Various types of photodetectors as well as design constraints and applications • **Nd: YAG Lasers for Machining** *(8:30-10:00 or 1:30-3:00)* -- Advancements making high power CW Nd: YAG lasers an alternative to CO_2 lasers • **Laser Power/ Energy Measurements** *(10:30-12:00 or 3:30-5:00)* -- Applications of the various types of detectors used in power/energy measurement.

DATE: March 12, 1996

TIME: See ad for session times

LOCATION: Illinois Institute of Technology, Herman Hall, 3341 South Federal, Chicago, IL

Tuition -- $60 per student

TO PREREGISTER:
Call 1-800-266-8724 or circle **#202**

Presented by CAD/CAM Source, SDRC and Hewlett-Packard

CAD/CAM SOURCE
SDRC
Structural Dynamics Research Corporation
HEWLETT PACKARD

SDRC I-DEAS Master Series -- Helping You Bring Designs to Life

I-DEAS Master Series offers superior design, simulation, manufacturing and testing applications. That's why companies, like **FORD**, have chosen SDRC as their strategic partner to develop better products, more rapidly and more cost effectively. Don't miss this opportunity to experience one of the easiest-to-use, highest functionality, team-oriented software solutions for mechanical design automation. Come and bring your designs to life.

DATE: March 28 or April 11

TIME: 8:30-11:30 or 9:00-12:00

LOCATION: Rolling Meadows, IL (3/28); Milwaukee, WI (4/11)

March 28 -- 8:30-11:30
April 11 -- 9:00-12:00
Continental Breakfast Included

TO PREREGISTER:
Call 1-800-266-8724 or circle **#203**

Presented by Moore Products Co.

MOORE®

IEC 1131 -- International Programming Standard for Programmable Controllers

The IEC 1131 standard defines five languages for programming process control systems. Experts will cover IEC 1131 Ladder Logic, Function Blocks, Sequential Function Charts, Structured Text, and Instruction List Languages and their interaction. The language capabilities will be demonstrated, along with examples to show the advantages of using one versus another. Get the answers to questions such as: • **What are the benefits of standard structured languages?** • **When should you use each of the five languages?** • **Is it compatible with other industry standards?**

DATE: March 27, 1996

TIME: 9:00 am to 12:00 noon

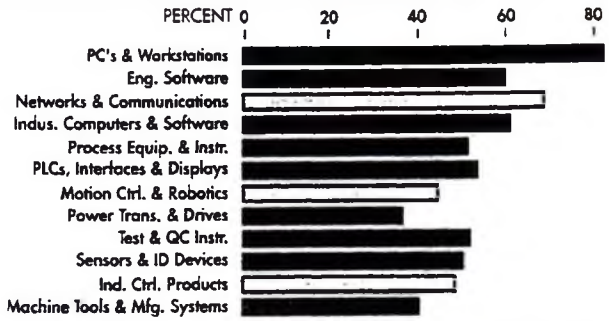
LOCATION: Roosevelt Glen Corporate Center, 799 Roosevelt Road, Building 4, Meeting Room A, Glen Ellyn, IL

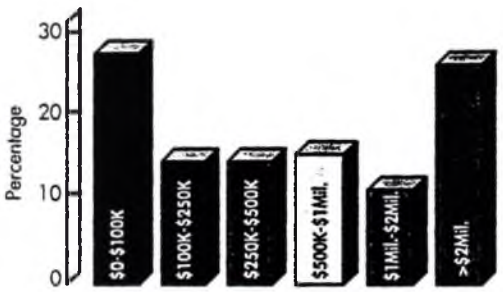
TO PREREGISTER:
Call 1-800-266-8724 or circle **#204**

SEE MORE SEMINARS ON THE NEXT PAGE →

Industry.Net User Analysis

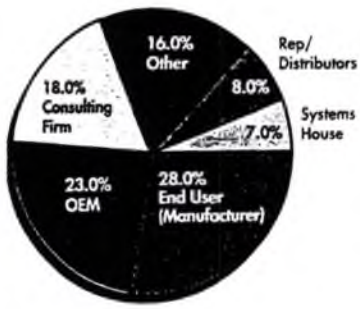
Users by Product Buying Interest

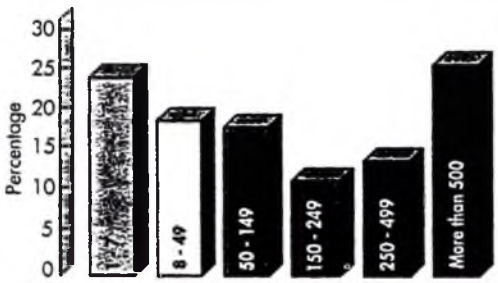




Annual Buying & Specifying Power of Users

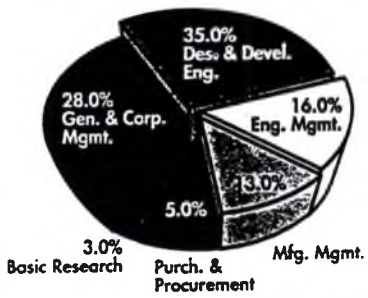
Users by Type of Company





Company Size of Users

Users by Principal Job Description



MODEL ZARZĄDZANIA BEZPIECZEŃSTWEM OŚRODKA SIECIOWEGO MOŻLIWOŚĆ PODWYŻSZENIA STOPNIA BEZPIECZEŃSTWA KOMPUTEROWEGO PRZEZ STOSOWANIE PROGRAMU INTERNET SECURITY SCANNER.

mgr Karol Frańczak

Akademickie Centrum Komputerowe
CYFRONET-KRAKÓW
ul. Nawojki 11
30-950 Kraków

1. Wyniki badań stopnia bezpieczeństwa w Internecie w 1995 r

Instytut Bezpieczeństwa Komputerowego (CSI) zbadał bezpieczeństwo sieci Internet i ujawnił niektóre wyniki. Wyniki badań oparte są na 320 odpowiedziach od osób zawodowo zajmujących się bezpieczeństwem informacji w 500 największych przedsiębiorstwach (wg FORTUNE), agencjach rządowych i wyższych uczelniach: 66% tych firm zatrudnia 1000 lub więcej osób, 32% z nich ma ponad 1 mld $ obrotu rocznie. [1] Oto ankieta i jej wyniki.

CZY TWOJA ORGANIZACJA KORZYSTA Z INTERNETU?
Tak: 78%
Nie: 22%

JEŻELI NIE, CZY PLANUJE KORZYSTAĆ Z INTERNETU?
Tak: 84%
Nie: 16%

CZY TWOJA FIRMA UŻYWA FIREWALLI?
Tak: 48%
Nie: 34%
Brak odpowiedzi: 18%

CZY TWOJA KOMPANIA MA DOŚWIADCZENIE Z NARUSZENIEM BEZPIECZEŃSTWA PRZEZ INTERNET?
Tak: 20%
Nie: 75%
Brak odpowiedzi: 5%

JEŻELI TAK, CZY MIAŁO ONO WCZEŚNIEJ MIEJSCE NIŻ ZAINSTALOWANY FIREWALL?
Tak: 52%
Nie: 30%
Brak odpowiedzi: 18%

JAKI RODZAJ FIREWALLA JEST ZAINSTALOWANY?
Screnning router: 52%
Dual-homed or application gateway: 43%

Inne: 5%
Jaki produkt jest używany?
ANS: 14%
TIS Toolkit: 13%
TIS Gauntlet: 9%
DEC: 8%
IBM 7%
Chechpoint Firewall 1: 7%
Raptor Eagle: 3%
Blackhole: 3%
NetGate: 2%
Sidewinder: 1%
Harris Cyberguard: 1%
Inne: 16%
Brak odpowiedzi: 14%:

DO JAKICH USŁUG JEST WYKORZYSTYWANY INTERNET

Jak Internet jest wykorzystywany ?
Badania: 84%
Poczta z partnerami zawodowymi: 70%
Wsparcie oprogramowania: 60%
Badania rynkowe: 48%
Poczta z kupującymi: 39%
Transakcje pieniężne: 8%
Inne: 8%

Jakie opcje są dostępne dla wszystkich zatrudnionych?

E-mail: 83%
FTP: 50%
WWW: 53%
Gopher: 41%
Newsgroup: 39%
WAIS:20%

Na podkreślenie zasługuje fakt, że mimo, że 78% przedsiębiorstw które odpowiedziały na ankietę jest podłączonych do sieci, i ponad 50% udostępnia programy obarczone wysokim ryzykiem, takie jak FTP i WWW, wszystkim zatrudnionym, to 39% spośród nich, nie ma zainstalowanego porogramowania zwanego ścianami przeciwogniowymi lub grodziami przeciwogniowymi (firewall) .

Wyniki podają także, że co piąte przedsiębiorstwo doświadczyło naruszenia bezpieczeństwa przez Internet. Jakkolwiek wydaje się, że 20% to rozsądna wielkość, większość ekspertów uważa, że rzeczywistość jest o wiele gorsza i większość respondentów, którzy odpowiedzieli "nie" albo nie przyznało się do naruszenia bezpieczeństwa we własnym ośrodku, albo po prostu o tym nie wiedziało.

Powstaje rynek firewalli i tylko kilka kompanii wykazuje umacnianie się na nim. W rzeczywistości największy procent udzielono odpowiedzi "Inni" i dodano komentarze podobnych do "krajowych ścian ogniowych " lub "rozwijanych domowym sposobem". Powinno to podgrzać współzawodnictwo na tym rynku, 70% tych którzy nie mają ścian

ogniowych zamierza je wprowadzić. Tymczasem, 25% firm z planujących chce to zrobić przy pomocy publicznie dostępnych. Badania także pokazują, że same firewalle nie dają wystarczającego zabezpieczenia. 30% naruszeń bezpieczeństwa w Internecie miało miejsce gdy firewalle były stosowane.

2. Model rozwiązania organizacyjnego

Podział zadań pomiędzy specjalistami w ośrodku obliczeniowym odpowiedzialnymi za utrzymanie systemów jest wynikiem poprzednich doświadczeń tego ośrodka i nowych wyzwań. W podręcznikach systemowych sprawy bezpieczeństwa komputerowego i sieciowego znalazły swoje miejsce dopiero od kilku lat. Poprzednio stanowiły one jedynie mały fragment grubych podręczników.

Problemy bezpieczeństwa komputerowego nie znalazły satysfakcjonującej autora odpowiedzi w podręcznikach CONVEXa, SUN-a. Model rozwiązania prezentowany poniżej za Hewlett-Packardem wydaje się być zadawalający.

Wprowadzony podział i nazewnictwo stanowisk pracy nie jest zgodny z obecnie obowiązującym taryfikatorem.

Kluczowy personel zabezpieczający

Jedną z technik prowadzących do zwiększenia odpowiedzialności przy administracji systemu jest podział odpowiedzialności związanej z utrzymaniem bezpieczeństwa na różnych pracowników. W opisanym poniżej modelu, zalecanym przez NCSA, oficer zabezpieczenia systemu jest odpowiedzialny za całokształt bezpieczeństwa systemu, podczas gdy administrator systemu odpowiada za pracę systemu i współpracuje z oficerem zabezpieczenia systemu w celu zaplanowania wszystkich potrzeb zarówno sprzętowych jak i oprogramowania [2]. Wraz z operatorami i programistami systemowymi tworzą oni kluczowy personel zabezpieczający.

Zadania oficera systemu zabezpieczeń

Inicjowanie i nadzorowanie zakresu kontroli.

Wyznaczanie jacy użytkownicy i wydarzenia będą kontrolowane.

Utrzymywanie systemu bezpiecznych haseł.

Inicjalizowanie uprawnień DAC (dla zbiorów publicznych.

Zatwierdzanie accountów nowych użytkowników.

Sprawdzanie systemów plików z uwagi na występowanie suid/sgid (set user ID/set group ID)

Zadania administratora systemu

Wprowadzanie procedur kontroli zabezpieczenia systemu.

Przeglądanie i analiza logów po kontroli.

Administrowanie accountami grup i użytkowników.

Naprawianie zepsutych zbiorów użytkowników i dysków.

Aktualizacja oprogramowania systemowego

Ustalanie parametrów konfiguracyjnych systemu

Prowadzenie różnych statystyk systemowych

Unieważnianie i usuwanie kont.

Wykonywanie okresowych sprawdzeń systemu - z intencją wykrycia czy nie została dodana wersja trojańska programu systemowego.

Śledzenie powtarzających się prób loginowania.

Okresowe sprawdzanie pozwoleń dla zbiorów.

Zajmowanie się nieprawidłowymi usiłowaniami zaloginowania jako SU (podstawiając użytkownika, lub superużytkownika) i nieprawidłowymi żądaniami sieciowymi.

Zadania operatora

Instalacja oprogramowania związanego z bezpieczeństwem.

Wykonywanie rutynowych prac podtrzymujących, jak zrzuty plików dyskowych.

Wykonywanie testów on-line terminali i urządzeń.

Odpowiadanie na rutynowe żądania użytkownika do systemu .

Zadania programistów systemowych

Instalacja upgrade'ów systemu.

Wykonywanie analizy dumpów.

Pisanie programów utrzymujących wymagania bezpieczeństwa.

3. Informacje o stanie bezpieczeństwa na uniwersytetach amerykańskich i w USA

Fragment z serwera http://underground.org/mlist/

"Wiele udokumentowanych wypadków włamań pochodziło albo przechodziło przez instytucje akademickie. Podejście do spraw bezpieczeństwa w większości uniwersytetów jest dość dowolne lub nawet w niektórych wypadkach zupełnie ignorowane. Większość instytucji nie używa ścian ogniowych ponieważ nie dba o swoje bezpieczeństwo. Uważają ściany ogniowe za nieodpowiednie lub niepraktyczne, lub nie znają rodzaju i zakresu możliwego ataku jaki może nastąpić przy użyciu INTERNETu."

Według danych na serwerze http://www.iss.net

- FBI oszacowało roczne straty wskutek ataków elektronicznych na 7,5 mld $ rocznie.
- Raport Departamentu Obrony USA stwierdza, że 88% ich komputerów było penetrowane. W 96% przypadków włamań, ich sprawcy pozostali niewykryci.
- W 1993 roku CERT stwierdził wzrost o 73% ilości naruszeń bezpieczeństwa.
- "Bezpieczeństwo systemów informatycznych i sieci jest głównym wyzwaniem tej dekady i możliwe, że następnego stulecia", Scott Charney, Przewodniczący, Zespół Przestępstw Komputerowych, Ministerstwo Sprawiedliwości USA.
- "Rosyjscy hackerzy komputerowi z powodzeniem złamali dużą ilość rachunków w korporacji Citicorp, wykradli ukradkiem 400,000$ i nielegalnie przetranfserowali dodatkowo 11,6 mln $", Wall Street Journal, August 21, 1995.
- Zgodnie z raportem Dataquest, bezpieczeństwo pozostaje problemem numer jeden organizacji podłączonych do Internetu.

4. Opinia o stanie bezpieczeństwa na uniwersytetach w Polsce

Według słów Pana Krzysztofa Młynarskiego, zastępcy Dyrektora ds. merytorycznych Instytutu Bezpieczeństwa Sieciowego, na konferencji "Bezpieczne podłączanie sieci lokalnych do Internetu" w dniu 27 marca 1996 roku w Łodzi, podczas Targów INTERTELECOM, "Pewna ilość administratorów systemów systematycznie nie wprowadza patchy systemowych. W szczególności dotyczy to patchy bezpieczeństwa".

Autorowi nie jest znana ocena stanu bezpieczeństwa w polskich wyższych uczelniach.

5. Dotychczasowe prace

W Akademickim Centrum Komputerowym jednocześnie z urządzeniami sieciowymi oddawanymi do eksploatacji korzystano z dostępnych informacji jakie generują światowe centra doradcze w zakresie bezpieczeństwa sieci Internet (np. CERT). w celu zapewnienia stanu bezpieczeństwa sieciowego zgodnego z najnowszymi osiągnięciami wiedzy .

Dotychczas korzystano z niżej wymienionych programów i korzystanie z nich było nieodpłatne:

Crack - szybki program do łamania haseł, przeznaczony do wspomagania administratorów ośrodków w celu upewnienia się, że użytkownicy wykorzystują efektywne hasła.

COPS i Tiger - te pakiety identyfikują wspólne problemy bezpieczeństwa i konfiguracji. Pozwalają na sprawdzanie występujących przejawów ataku. Zalety TIGERa to łatwość.

npasswd, passwd+ - te programy sprawdzają hasła. Wykonują serię sprawdzeń na hasłach w czasie wprowadzania ich przez użytkowników i odrzucą je gdy hasło nie przejdzie serii testów.

tcp_wrapper - to oprogramowanie podaje czas pracy i kontrolę dostępu dla większości usług sieciowych.

Tripwire - ten pakiet utrzymuje bazę danych sum kontrolnych dla ważnych plików systemu. Może służyć jako system wczesnego wykrywania intruza.

cpm - sprawdza czy twój interfejs sieciowy pracuje w promiscuous mode. W zwykłych warunkach może to oznaczać, że program intruz-przechwytywacz pracuje w twoim systemie.

md5 - algorytm obliczania sum kontrolnych.

SATAN - Security Administrator Tool for Analysing Network

lsof - program drukuje nazwy wszystkich otwartych plików.

6. Stan obecny - istniejące zagrożenia

Administratorzy komputera sieciowego stwierdzili posługiwanie się przez niektórych użytkowników programem do łamania haseł. Łamaniu haseł poddano np. plik z hasłami z

serwera Instytutu Matematyki Uniwersytetu Jagiellońskiego. Może to świadczyć o próbach przygotowywania się do włamania.

Istnienie w jednym środowisku komputerów o różnych poziomach technologicznych stwarza możliwość nowych zagrożeń. Jeżeli administrator systemu Unixowego ma do dyspozycji terminal np. typu VT100, a użytkownicy w sieci korzystają z X-terminali, to istnieje zagrożenie wzajemnego podglądania okien przez użytkowników X-terminali .

Inny przykład zagrożenia, to oddanie do eksploatacji komputerów bez dokonania niezbędnych zmian mających na celu zapewnienie bezpieczeństwa.

W związku z lawinowym wzrostem ilości instalacji komputerowych z systemami wielodostępnymi należy liczyć się z tym, że stopień zabezpieczenia w nowo oddawanych instalacjach, administrowanych przez nowych - niekiedy niedoświadczonych - administratorów, może różnić się od tych administrowanych dłużej. I na odwrót. Biorąc pod uwagę fakt, że o stopniu zabezpieczenia sieci komputerowych stanowi jej nasłabsze ogniwo oraz, że istnieje stopień zagrożenia nie typu "jeden na jednego" ale "wszyscy na jednego" można uznać za stosowną sugestię zakupu oprogramowania wspierającego, mogącego jednolicie ocenić system zabezpieczania poszczególnych ogniw.

7. Czy Internet Security Scanner może pomóc w podwyższeniu stopnia bezpieczeństwa komputerowego ?

Od kilku lat obserwowałem prace prowadzone przez pana Christofera Klausa, których wyniki były prezentowne w liście dyskusyjnej alt.comp.security, pierwsze wersje scannera internetowego oraz opracowywane przez niego odpowiedzi na najczęściej zadawne pytania.

W ACK korzystano także z pierwszych - użytkowanych bezpłatnie - wersji scannera.

Obecnie pojawiła się komercyjna wersja programu, która pokrótce zostanie omówiona.

Na uwagę zasługuje fakt podziału istniejących zagrożeń na trzy kategorie w zależności od stopnia ryzyka dla bezpieczeństwa systemu.

Wykaz usterek wychwytywanych przez program Internet Security scanner

HIGH Risk - Usterki prowadzące do bezpośredniego przejęcia systemów, uzyskania hasła roota lub przejścia przez gródź przeciwogniową

Firewalls

Source porting
Source routing
SOCKs
RPC scan directly
TCP sequence prediction (IP Spoofing) (SunOS only)

Sendmail

Debug and Wizard
Aliases
Pipe
Identd
8lgm

Inne

WWW - NCSA Httpd < V1.4.1
Rsh with hosts.equiv +
Rlogin -froot
Rexd
X Windows

Brute Force Attempts: Default Accounts

Attempts through Telnetd, FTPd, and Rexecd
Tries with gathered information from Finger and Rusers

Anonymous FTP

Main directory writeable or owned by root
WuFTP 2.2- with Site Exec
Invalid password gives root access

NFS

Mountable by everyone
Mountable by Portmapper
Filehandle guessing
UID
Mknod
CD ..

MEDIUM Risk - Usterki prowadzące do wysokiej możliwości przejęcia lub wyłączenia zaatakowanych usług

NFS (exporting sensitive files, i.e., .rhosts, .cshrc)
NIS (Network Information Service) Anonymous FTP with writeable directories
TFTP
Selection_svc
Walld
UUCP
UDP Bomb

LOW Risk -Usterki mogące prowadzić do potencjalnego przejęcia systemów

Finger
Rusers

Telnet banner
SMTP banner
Anonymous FTP
Rstat
X.25
Bootparamd
Gopher
Internet Relay Chat (IRC) servers
Netstat
Systat

8. Wnioski

Biorąc pod uwagę stały rozwój systemów operacyjnych, ciągłe zmiany w istniejącym oprogramowaniu, przeciążenie administratorów systemów w celu utrzymaniu ciągłości produkcji, możliwość niezrozumienia lub błędnego rozumienia opcji programów i parametrów, możliwość niewprowadzenia przez niedopatrzenie jakiegoś patcha i innych usterek w pracy w celu dokonania oceny stopnia zabezpieczenia systemu operacyjnego w wybranym komputerze lub sieci komputerów widzę potrzebę wykorzystywania oprogramowania typu Internet Security Scanner w celu stwierdzenia występowania usterek i następnie możliwości ich usunięcia.

Po przeprowadzeniu badania testowego z pozytywnymi wynikami, wersji demonstracyjnej programu Internet Security Scanner rozważany jest zakup licencji na używanie tego oprogramowania.

Wydaje się, że przebieg sprawdzający wykonany tym programem i dokonanie zmian systemowych mogłoby zapobiec powstaniu niezamierzonych "dziur" w bezpieczeństwie systemów.

Analiza opublikowanego "Regulaminu i Cennika Usług Świadczonych przez Naukową i Akademicką Sieć Komputerową (8 marzec 1995) " jakkolwiek zawiera część poświęconą Ochronie sieci NASK, §15-§21 to nie wymienia w §24 żadnego stanowiska związanego z bezpieczeństwem sieci. [4]

Wydaje się że istnieje potrzeba istnienia stanowisk: analityk penetracji sieci i specjalistów do spraw bezpieczeństwa komputerowegi i sieciowego.

Przyjęcie modelu organizacyjnego przedstawionego wcześniej mogłoby przyczynić się do podwyższenia istniejącego poziomu bezpieczeństwa.

Literatura

[1] Computer Security Institute, 6000 Harrison St., S.F. CA

http://www.csi.net

[2] HP-UX SystemSecurity, HP Part No. B2355-90045
[3] Internet Security Systems,Inc. 2000 Miller Court West, Norcross, Georgia
http:/www.iss.net
[4] Tomasz Hofmokl, Andrzej Zienkiewicz "Naukowa i Akademicka Sień komputerowa", Materiały seminarium MIEDZESZYN '95

Sieć Internet w NASK

Sieć Internet w NASK znajduje się w tej chwili w stadium normalnej eksploatacji. Na dzień dzisiejszy posiadamy węzły dostępowe do Internetu w 32 miastach. W ciągu najbliższych 3 miesięcy planujemy instalację węzłów regionalnych w kolejnych pięciu miastach. W 15 miastach posiadamy węzły dostępowe do sieci Frame Relay, a w 10 serwery umożliwiające dostęp do sieci Internet po łączach komutowanych (dial-up).

Obecnie NASK posiada 4 połączenia międzynarodowe:

- 2 Mb/s satelitarne do GIX-a w Sztokholmie
- 256 kb/s do Ebone w Wiedniu
- 64 kb/s do FreeNET-u w Moskwie
- 64 kb/s satelitarne do ICMP w Lwowie

W Sztokholmie posiadamy bezpośrednią łączność z NorduNET-em i Sunet-em. Rozpatrujemy możliwość wymiany danych na terenie GIX-a również z innymi operatorami.

Do końca maja zostanie uruchomione bezpośrednie łącze satelitarne do USA o przepustowości 3 Mb/s. Operatorem satelitarnym tego łącza jest Telekomunikacja Satelitarna SA we współpracy z Orion Atlantic, a naszym partnerem Internetowym po stronie amerykańskiej - **Digex**.

Liczba abonentów sieci Internet w NASK w szybkim tempie rośnie. W ciągu pierwszych czterech miesiecy tego roku zanotowaliśmy wzrost o 50%. Tranzyt ruchu w sieci szkieletowej NASK również szybko rośnie i wynosi w tej chwili przeciętnie około 50 GB (miliardów znaków) na dobę, z czego ponad 50% stanowi ruch zagraniczny.

NASK obsługuje domenę krajową PL, pięć z sześciu istniejących domen funkcjonalnych drugiego poziomu oraz dużą część domen regionalnych. Liczba nowych domen rejestrowanych przez NASK wynosi przeciętnie 25 do 30 miesięcznie. NASK oferuje również swoim abonentom możliwość obsługi secondary Name Server'ów dla ich domen. Aktualnie taką usługę prowadzimy dla ponad 400 domen i to zarówno krajowych, jak i zagranicznych.

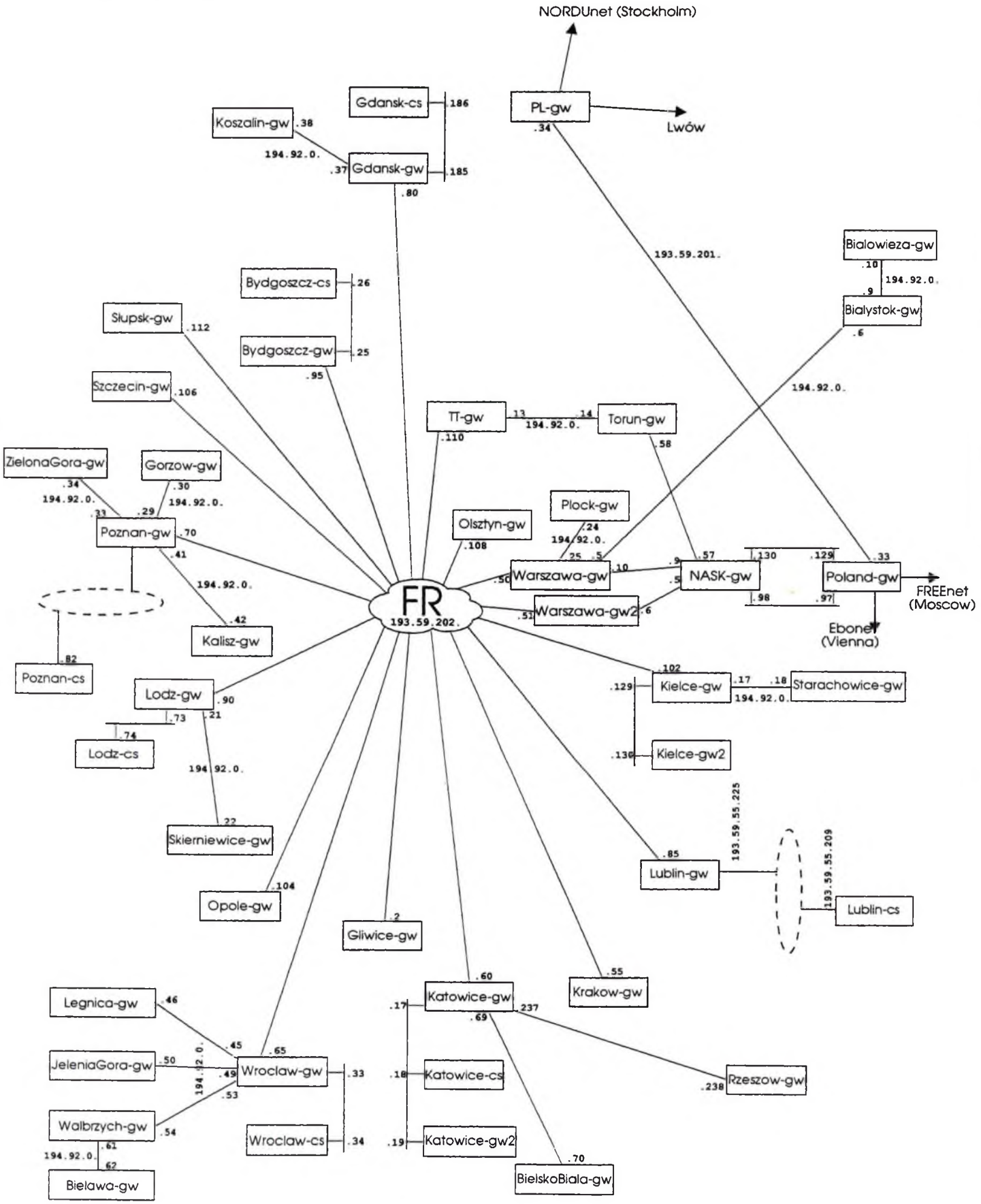
Jak każdy operator sieciowy (service provider) posiadamy własną pulę adresów IP przeznaczoną dla naszych abonentów. Na podstawie odpowiedniego formularza rejestracyjnego jesteśmy w stanie - praktycznie od ręki - przydzielić nowo dołączającym się abonentom NASK od pojedynczych adresów IP na potrzeby serwerów informacyjnych lub pocztowych, aż do bloku 32 klas C (ponad 8 tysięcy adresów) dla bardzo dużych sieci korporacyjnych.

NASK jest w tej chwili w trakcie tworzenia tzw. puntu wymiany Internetowej dla operatorów, czyli GIX-a (Global Internet eXchange). Na początku będzie cię on znajdował w Centralnym Węźle NASK w budyku Centrum Informatycznego UW. W dalszej kolejności rozszerzymy ten punkt dostępowy do Centrum Radiokomunikacji i Telekomunikacji na ul. Barbary. Taki punkt wymiany w ogólności jest miejscem wymiany danych między operatorami posiadającymi własne numery AS (systemów autonomicznych). W naszym przypadku funkcja ta zostanie rozszerzona o możliwość szybkiego dostępu do sieci szkieletowej IP NASK oraz łączności międzynarodowej dla operatorów nie posiadających własnego numeru AS. Każdy operator dołączający się do takiego punktu może postawić własny router i wymieniać dane z innymi operatorami posiadającymi własne routery w tym miejscu. Można również dołączyć się bezpośrednio do routera NASK i uzyskać łączność ze wszystkimi operatorami, z którymi NASK jest połączony.

NASK IP Backbone

1996-05-07

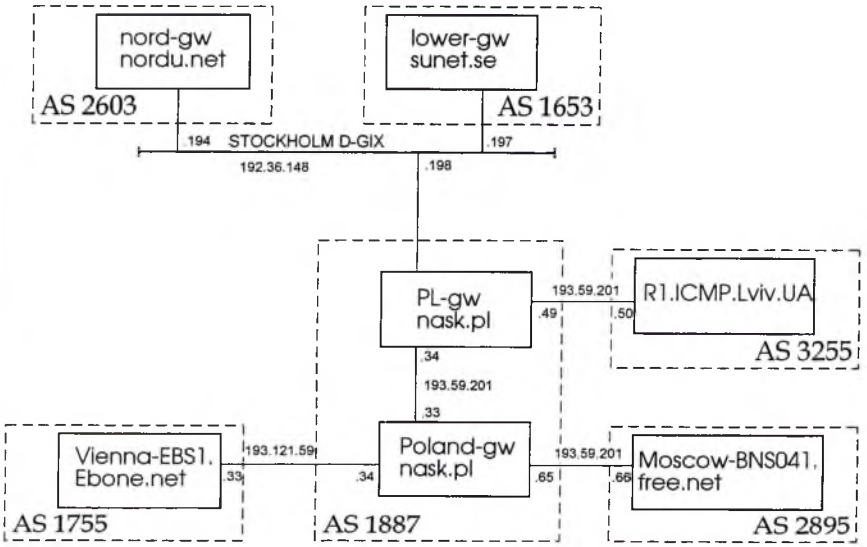
193.59.200.xxx



rys.: Jerzy Helewski
<jurek@nask.pl>

NASK peerings

Połączenia międzynarodowe i międzyoperatorskie NASK



rys.: Jerzy Helewski
<jurek@nask.pl>

Sieć Frame Relay NASK

Sieć szkieletowa oparta o technologię Frame Relay powstała w NASK w połowie 1995 roku. Pełna eksploatacja rozpoczęła się w październiku zeszłego roku. W chwili obecnej w szesnastu głównych miastach Polski pracują switch'e Frame Relay NASK. Stanowią one podstawę działania największej pod względem ilości użytkowników sieci szkieletowej w kraju. Ponad 95% ruchu Internetowego jest transportowana poprzez połączenia logiczne Frame Relay. Struktura połączeń wirtualnych tworzy topologię "full-mesh" czyli połączeń "każdy z każdym". Taka konstrukcja sieci zapewnia bezpośrednią wymianę informacji miedzy wszystkimi routerami IP dołączonymi do switch'y Frame Relay. Jako przykład niech posłuży połączenie między Szczecinem a Kielcami. Fizyczne łącza przebiegają poprzez trzy węzły tranzytowe: Bydgoszcz, Warszawę i Lublin. Pomimo to, z logicznego punktu widzenia router IP w Kielcach otrzymuje informacje od routera w Szczecinie, tak jakby był z nim bezpośrednio połączony. Fakt tranzytowania ruchu przez wiele węzłów jest ukryty dla protokołów wyższych warstw.

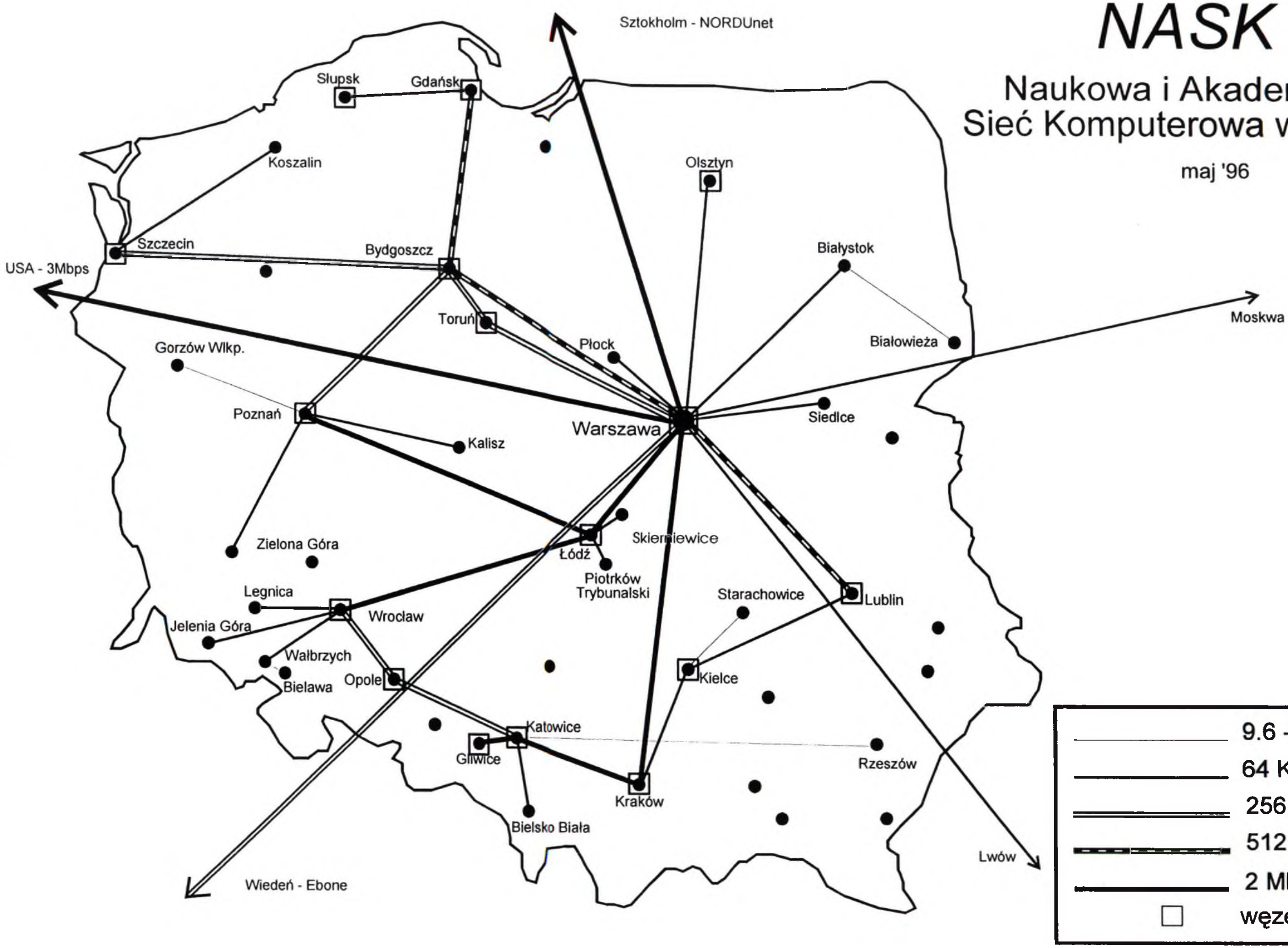
Warto podkreślić bardzo wysoką niezawodność sieci Frame Relay NASK. Zrealizowana w zeszłym roku struktura połączeń fizycznych zapewnia co najmniej jedną drogę obejściową dla wszystkich węzłów Frame Relay. W przypadku awarii traktu podstawowego zostaje natychmiast aktywowane łącze zapasowe. Czasy przełączania nieprzekraczające 2 sekund są niezauważalne z punktu widzenia transmisji TCP/IP. Z codziennych doświadczeń wynika, że normalne sesje połączeniowe są kontynuowane bez żadnych przeszkód.

Dotychczasowa eksploatacja wykazała przydatność technologii Frame Relay w sieci NASK. W związku ze wzrostem zapotrzebowania na pasmo są prowadzone intensywne prace mające na celu przystosowanie istniejącej struktury do przenoszenia ruchu o większym natężeniu. W chwili obecnej w fazie testowej eksploatacji znajdują się karty z nowym typem szybkiego styku - HSSI. Umożliwia on transmisję z prędkościami do 52 Mbps.

NASK

Naukowa i Akademicka Sieć Komputerowa w Polsce

maj '96



- 9.6 - 28.8 Kbps
- 64 Kbps
- 256 Kbps
- 512 Kbps
- 2 Mbps
- węzeł Frame Relay

rys.: Jerzy Helewski <jurek@nask.pl> dn.: 10.05.96