PRACE INSTYTUTU ŁĄCZNOŚCI

1997
108

PRACE INSTYTUTU ŁĄCZNOŚCI

INSTYTUT ŁĄCZNOŚCI NR 108

WARSZAWA 1997

ISSN 0020-451X

Redaktor: mgr Krystyna Juszkiewicz

Skład komputerowy: techn. Danuta Pol, techn. Grażyna Woźnica

Instytut Łączności, Ośrodek Informacji Naukowej i Normalizacji
ul. Szachowa 1, 04-894 Warszawa

SPIS TREŚCI

KOMUNIKAT

СОДЕРЖАНИЕ

СООБЩЕНИЕ

CONTENS

STATEMENT

SOMMAIRE

COMMUNIQUE

INHALTSVERZEICHNIS

MITTEILUNG

Andrzej P. Wierzbicki

62:621.391.008.2

ROLA TECHNIKI W CYWILIZACJI INFORMACYJNEJ

Artykuł stanowi refleksję na temat roli techniki w cywilizacji informacyjnej. Oparty jest na analizie wybranych problemów przełomu ery cywilizacji przemysłowej i cywilizacji informacyjnej, będących źródłem konfliktów społecznych oraz gospodarczych. Do najważniejszych autor zalicza zmiany zapotrzebowania na pracę, które są przyczyną głębokiego, strukturalnego bezrobocia, a także niejednakowy dostęp do edukacji dostosowanej do wymagań ery informacyjnej, którego skutkiem są nowe rozwarstwienia społeczne. Na tym tle istotna jest odpowiedź na pytanie, jaką rolę będzie odgrywać technika, a zwłaszcza technika informacyjna. Zdaniem autora technika, w nowym globalnym rozumieniu i nowym wymiarze, będzie decydującym narzędziem ery cywilizacji przemysłowej - mimo stopniowego zmniejszania się udziału produkcji przemysłowej w produkcie narodowym.

1. POCZĄTEK ERY CYWILIZACJI INFORMACYJNEJ

Już dziś cywilizacja informacyjna dociera do nas wieloma drogami: przez komputeryzację prac biurowych, zarządzania, księgowości; przez sieci komputerowe i Internet; przez reklamy wielkich firm międzynarodowych; przez inicjatywę *Globalnej Infrastruktury Informacyjnej* wiceprezydenta A. Gore'a; czy działania Unii Europejskiej, oparte na *Raporcie Bangemana*. Jednak zrozumienie cywilizacji informacyjnej jest niewielkie; wielu ludzi koncentruje uwagę jedynie na obawach przed jej skutkami. Brak pełnego zrozumienia pogłębia obawy przed cywilizacją informacyjną. Tym niemniej, nikt już dzisiaj nie kwestionuje faktu, że cywilizacja taka nadeszła lub nadchodzi.

Według dość powszechnej opinii ekspertów światowych, za cezury początku i końca ery cywilizacji przemysłowej należy przyjąć rok 1760, związany z wynalazkiem maszyny parowej, oraz lata tuż przed rokiem 1980, czyli rokiem, w którym opracowano protokół TCP-IP. Jest wprawdzie wiele innych protokołów teleinformatycznych, ale to właśnie od protokołu TCP-IP zaczął się burzliwy rozwój Internetu i sieci komputerowych - które nie różnią się od sieci teleinformatycznych techniką, tylko rozłożeniem akcentów, naciskiem na zastosowania i usługi (czyli koncentracją na najwyższych z siedmiu warstw protokołu TCP-IP, podczas gdy bardziej tradycyjne podejścia do telekomunikacji cyfrowej koncentrują się na najniższych warstwach - od warstwy fizycznej zaczynając). Era cywilizacji informacyjnej trwa już zatem kilkanaście lat. Oczywiście, wielu ludzi na świecie jeszcze tego nie zauważa lub nie chce zauważyć; ale ilu ludzi na świecie zdawało sobie sprawę z perspektyw ery cywilizacji przemysłowej w 1776 roku?

Istotą cywilizacji informacyjnej nie jest, jak to się sądzi w uproszczeniu, powszechne wykorzystanie środków i metod telekomunikacyjnych oraz informatycznych. Znacznie bardziej istotny jest fakt, że **informacja zaczyna odgrywać rolę podstawowego, a stopniowo nawet decydującego, czynnika produkcji - obok kapitału, pracy i surowców**. Decydujący dla sukcesu ekonomicznego przedsiębiorstwa staje się więc dostęp do światowych zasobów informacji i umiejętność ich wykorzystania. Coraz powszechniej, podstawowym narzędziem tego dostępu staje się sieć komputerowa. Nie jest to jednak cywilizacja **informatyczna** (choć tak chcieliby ją nazwać niektórzy informatycy), tylko **informacyjna**. Tak też nazwał ją A. Toffler w *Trzeciej fali* i nazwa ta przyjęła się już powszechnie na świecie (wypierając dawne nazwy, takie jak "*społeczeństwo poprzemysłowe*" czy "*usługowe*" czy też lansowane niekiedy "*post-fordowskie*", czy proponowane wcześniej przez autora tego tekstu "*społeczeństwo poinformowanego rozumu*").

Nie możemy przy tym zamykać oczu na fakt początku nowej ery. Czy nam się to podoba, czy nie, czy to rozumiemy, czy tylko się tego boimy, według opinii ekspertów światowych zaczęła się już era cywilizacji informacyjnej i rozwój w tym kierunku jest nieuchronny. Tyle tylko, że na tym tle różnie mogą zostać ukształtowane szanse Polski na uczestnictwo w Unii Europejskiej, na utrzymanie znaczącej pozycji cywilizacyjnej w środku Europy oraz na ogólny rozwój w całym XXI wieku. Jeśli nie zrozumiemy dostatecznie głęboko przesłanek, wyzwań i szans epoki cywilizacji informacyjnej, jeśli ograniczymy dyskusję tylko do naszych obaw, to szanse te wykorzystają inni - ze stratą dla interesów Polski.

2. WIEK XXI ERĄ CYWILIZACJI INFORMACYJNEJ

Trudno tu przedstawić szczegółowo wszystkie poglądy na cywilizację informacyjną - napisano już na ten temat wiele książek, zaczynając od *Trzeciej fali* A. Tofflera, opublikowanej po raz pierwszy w 1980 roku, a także wiele artykułów naukowych i publicystycznych*). Trzeba jednak przedstawić przesłanki przekonania o tym, że istotnie żyjemy dziś na przełomie er cywilizacyjnych oraz pewne wynikające stąd wnioski.

Toffler sądził, że jest to tylko trzecia fala (po cywilizacji rolniczej i przemysłowej). Znając teorie rozwoju cyklicznego, autor niniejszego tekstu zwrócił uwagę, że cykli takich mogło być wiele. W historii

*) Zob. m.in. A.P. Wierzbicki: Changing Cultural Paradigms, *Options* IIASA, No. 4, 1983, p.10; Education for a new cultural era of informed reason, in J.G. Richardson, *ed: Windows of Creativity and Inventions*, Lomond, Mt Airy, Ma. 1988; *Perspektywy cywilizacji światowej w XXI wieku a przemiany w Polsce*, referat plenarny na konferencji jubileuszowej Komitetu Prognoz "Polska w XXI wieku" PAN, w *Świat przyszłości a Polska*, Elipsa, Warszawa 1995.

Europy wyraźne są następujące okresy cywilizacyjne: późnego średniowiecza (od około 1000. do około 1440. roku); potem łączny okres renesansu, reformacji i kontrreformacji (od około 1440. do około 1760. roku); następnie okres cywilizacji przemysłowej. Mechanizm powstawania takiego cyklu można wytłumaczyć, zakładając stopniową akumulację czynników materialnych oraz kulturowych rozwoju, a także wzajemne sprzężenie zwrotne między nimi (żaden z czynników nie może się rozwinąć nadmiernie bez drugiego*). Sprzężenie to jednak charakteryzuje się pewnym **cywilizacyjnym czasem opóźnienia**: od powstania nowej teorii, nowego pojęcia podstawowego do rozumienia świata (które to pojęcia, jak wskażemy dalej, są niesłychanie ważne w rozwoju cywilizacyjnym), czy wreszcie nowego wynalazku o przełomowym znaczeniu, upływa zwykle wiele czasu, zanim teorie te, pojęcia podstawowe i przełomowe wynalazki zostaną powszechnie zrozumiane i wykorzystane.

Procesy z akumulacją i czasem opóźnienia w sprzężeniu zwrotnym mogą łatwo wywołać powstawanie cykli rozwojowych długości - co można wykazać różnymi metodami, włącznie z matematyczną analizą stabilności - około 4 czasów opóźnienia. Procesy takie i cykle są dość powszechne.

Jako przykład, można przywołać tu prosty i opisywany w literaturze** cykl zapotrzebowania na absolwentów wybranej specjalności uniwersyteckiej w warunkach rynkowych. Przypuśćmy, że w danym

---

*) Zatem nie *byt określa świadomość* i nie *świadomość określa byt*, tylko *oddziałują one na siebie we wzajemnym sprzężeniu zwrotnym*; ale po to, aby ten fakt zrozumieć, trzeba było najpierw spopularyzować pojęcie sprzężenia zwrotnego, które zostało wprowadzone przez telekomunikację około 60 lat temu i dotąd nie zawsze jest dostatecznie głęboko zrozumiane.

**) R.B. Freeman, *The Over-Educated American*. Academic Press, New York 1976.

momencie powstała przewaga popytu nad podażą na absolwentów tej specjalności. Młodzież licealna dowiaduje się o tym szybko, wobec czego znaczna jej część wybiera ten kierunek studiów. Jednakże, aby wykształcić absolwenta, potrzeba około 5 lat (to właśnie czas opóźnienia); więc przez pięć lat niedobór takich specjalistów będzie się pogłębiał. Po pięciu latach zacznie się zmniejszać - ale zakładając symetrię przebiegów, potrzeba będzie następnych pięciu lat, aby niedobór zmalał do zera. Po dziesięciu latach pojawia się przewaga podaży nad popytem, zatem licealiści przestają wybierać tę specjalność. Ale studiuje jeszcze pięć dużych roczników studentów, więc nadmiar specjalistów w danej dziedzinie się powiększa; zacznie on maleć po piętnastu latach od chwili początkowej i trzeba będzie następnych pięciu lat, aby znów zmalał do zera. *Quod erat demonstrandum*: okres cyklu to czterokrotnie liczony czas opóźnienia.

Jeśli jednak czasy opóźnienia dotyczą zjawisk cywilizacyjnych i wynoszą kilka pokoleń ludzkich, to okresy cyklu są kilkusetletnie. Przed wynalazkiem druku, ten cywilizacyjny czas opóźnienia wynosił, być może, około 110 lat, co zgadza się z cezurami cyklu 1000 - 1440 rok (pierwsza - to idea *Treuga Dei*, druga to właśnie wynalazek druku). Po wynalazku druku, w miarę jego upowszechnienia, czas ten skrócił się do około 80 lat, co zgadza się z cezurami cyklu 1440 - 1760 rok (druga data, to wynalazek maszyny parowej). W epoce cywilizacji przemysłowej, wynalazki tej ery spowodowały dalsze skrócenie czasu opóźnienia cywilizacyjnego - do około 55 lat, bo końcową cezurę cywilizacji przemysłowej wypada przyjąć na lata tuż przed 1980 rokiem (początki sieci Internet, protokół TCP-IP o parę lat przed 1980), przyjmijmy w przybliżeniu - rok 1980. Można przy tym zapytać - po co komu takie cezury, czy to nie jest próżna historiozofia? A może wręcz nawrót myślenia o sztywnych prawach historii?

Bynajmniej - chodzi tu tylko o **model przybliżony, pomocny w zrozumieniu** mechanizmów nowej ery cywilizacyjnej. W szczegól-

ności, cezury takie potrzebne są do przybliżonej choćby odpowiedzi na pytanie: **a ile to lat potrwa era cywilizacji informacyjnej?** Nie jest to pytanie nieważkie. Jeśli era ta będzie tylko kilkunastoletnią efemerydą, to nie ma o co kruszyć kopii. Jeśli jednak chodzi o erę o czasie trwania przekraczającym sto lat, to **żyjemy obecnie w czasie przełomu cywilizacyjnego i pozornie drobne decyzje dziś mogą wpłynąć w sposób zasadniczy na rozwój przyszłości.**

Jeśli więc mamy prawo wyciągać wnioski z modelu długich cykli cywilizacyjnych, to trzeba stwierdzić, że ich długość skraca się nieco wraz z przyspieszeniem obiegu informacji. Z definicji, era cywilizacji informacyjnej wniesie dalsze przyspieszenie. Decydujące jest tu jednak opóźnienie nie materialne, lecz kulturowe. Po to, by nowe pojęcie stało się powszechnie zrozumiałe i stosowane, trzeba najpierw wykształcić nauczycieli, którzy potem muszą wykształcić uczniów. To nie może trwać bardzo krótko. (Przykładem niech będzie nowe rozumienie pojęcia *chaosu*. Pojęcie to pojawiło się już ponad 30 lat temu, w trzydzieści lat po pojawieniu się pojęcia sprzężenia zwrotnego. Do dziś niewiele ludzi dobrze rozumie oba te pojęcia). Dlatego można sądzić, że era cywilizacji informacyjnej będzie wprawdzie nieco krótsza od poprzednich - może od 120 do 180 lat - ale na tyle długa, że zajmie zapewne cały wiek XXI. **Zdajmy więc sobie sprawę z przełomowego znaczenia czasów, w których żyjemy: to nie przełom tysiącleci jest ważny, tylko przełom er cywilizacyjnych.**

Głębia przemian sposobu życia i pracy, wywołanych tym przełomem, będzie równie wielka - jeśli nie większa - jak tych, które zapoczątkowała era cywilizacji przemysłowej. To, co dziś oferuje nam sieć telekomunikacyjna, to dopiero prymitywny początek. Wyobraźmy sobie, jak zmienią się sposoby komunikacji międzyludzkiej z chwilą upowszechnienia wideofonu, czyli pełnej integracji multimedialnej transmisji głosu i obrazu. A jak wpłynie na tę komunikację

automatyczne rozpoznawanie głosu i obrazu przez komputer; jak zmienią się techniki zarządzania i przedsiębiorczości? Dzisiejszy rozmiar automatyzacji i robotyzacji produkcji - to też tylko początek, ograniczony uzasadnionymi obawami wielu społeczeństw przed wzrostem bezrobocia. Jak to się zmieni w ciągu stu lat? Jak te wszystkie możliwości wpłyną na edukację, naukę i kulturę; jak na obronność kraju? Można podać wiele innych takich przykładów. Wszystkie one świadczą o głębi wyzwań cywilizacyjnych, wynikających z przełomu epok.

Musimy przy tym zrozumieć i odpowiedzieć na główne wyzwania czasów przełomu cywilizacji przemysłowej i informacyjnej, których jest wiele. Wymienimy tu tylko niektóre z nich, zaczynając od bardziej oczywistych i o technicznym charakterze, stopniowo przechodząc do wyzwań bardziej ogólnych:

- rozwój i upowszechnienie zastosowań technik informacyjnych, sieci komputerowych itp.;
- intensyfikacja inwestycji w infrastrukturę sieciowo-informacyjną, warunkującą zwiększenie innowacyjności gospodarek narodowych;
- wykorzystanie technik informacyjnych dla sprostania globalnym wyzwaniom demograficznym i środowiskowym;
- wyzwania globalizacji gospodarki i cywilizacji - jej zalet i wad, wraz z koniecznością większej odpowiedzialności za różnorodność kulturową świata;
- upowszechnienie szkolnictwa wyższego wraz z jego przystosowaniem do wymagań ery cywilizacji informacyjnej;
- przewidywane, nowe konflikty społeczne ery cywilizacji informacyjnej.

Wyzwań tych nie będziemy omawiać tu szczegółowo; część z nich była dostatecznie obszernie przedyskutowana w pracach Komitetu Prognoz *Polska w XXI wieku*. Omówimy tu przykładowo tylko jedno z tych wyzwań, o dużym znaczeniu dla kultury polskiej.

● **Odpowiedzialność za różnorodność kulturową świata**

Globalizacja ma różnorodne aspekty. Na przykład, *Globalna Infrastruktura Informacyjna* jest bardzo ważną inicjatywą rządu St. Zjedn. AP i wiceprezydenta A. Gore'a, umożliwiającą dostęp do różnych źródeł informacji na całym świecie, przez światową sieć komputerową. Inny aspekt, to globalizująca się sieć telewizyjna; pozwala ona na szybkie zapoznanie się z bieżącymi wiadomościami politycznymi i kulturalnymi, ale szerzy też jednolitość kulturową świata. Globalizacja dając więc ogromne możliwości, stwarza jednocześnie wiele niebezpieczeństw.

Za jedno z **poważniejszych niebezpieczeństw trzeba uznać uniformizację kulturową świata**. Język angielski stał się dziś językiem światowym i jest to rozwój w kierunku pozytywnym, nie należy - i nie ma sensu - temu przeciwdziałać. Ale nie może to oznaczać, że kulturę świata zdominuje jednolita formuła kultury massmediów - do czego nieświadomie przyczynia się wiele sieci telewizyjnych.

Istota tego niebezpieczeństwa polega na tym, że nie potrafimy do końca przewidywać przebiegu zdarzeń na świecie. Żeby się zabezpieczyć przed nieprzewidzianymi katastrofami, system musi mieć wbudowany zapas różnorodności. Nie wiadomo, która z kultur narodowych na świecie da impuls do pokonania kolejnego kryzysu. Nie chodzi tu o popieranie nacjonalizmu - ale o to, by **każdy naród, w epoce globalizacji dbał o różnorodność kulturową świata przez podtrzymywanie specyfiki swojej kultury narodowej**. Ma to być może jeszcze większe znaczenie niż obowiązek ochrony różnorodności genetycznej gatunków zwierząt i roślin na świecie. W Polsce powinno to polegać na intensywnych pracach nad wykorzystaniem światowej infrastruktury informacyjnej do posadowienia w niej i udostępnienia światu - np. Polonii rozproszonej po świecie - zasobów cywilizacyjnych polskiej strefy językowej (polskich muzeów, bibliotek, filmów itp.).

Przed przejściem do zasadniczego tematu artykułu - roli techniki w erze cywilizacji informacyjnej - podamy jeszcze komentarze dotyczące dwóch aspektów wyliczonych wyżej wyzwań, a mianowicie roli informacji jako zasobu produkcyjnego i zmian strukturalnych ery cywilizacji informacyjnej.

3. INFORMACJA JAKO ZASÓB PRODUKCYJNY

Informacja była zawsze swoistym zasobem produkcyjnym - wiedza o nowych wynalazkach czy technikach umożliwiała lepszą organizację lub podwyższenie jakości produkcji. Dziś jednak mamy do czynienia z różnicą jakościową, dotyczącą charakteru tego zasobu. Różnica ta wynika z następujących czynników.

Po pierwsze, nastąpił **gwałtowny rozwój ilości dostępnej informacji** - współczesna nauka zgromadziła tak wiele faktów istotnych dla naszej wiedzy o świecie, a współczesna technika (np. zdjęcia satelitarne) umożliwiła zgromadzenie tak dużych ilości informacji, że przeciętny człowiek, posługujący się tradycyjnymi metodami, czuje się bezradny wobec tego zalewu informacji.

Po drugie, nastąpiła **globalizacja dostępu do informacji** - nie trzeba dzisiaj, jak za czasów Marco Polo, wysyłać wyprawy na wielbłądach na kilka lat, aby dowiedzieć się, co się dzieje w innych krajach. Stąd też dostosowanie produktów czy usług do potrzeb innych krajów jest tylko kwestią umiejętności wyszukania i wykorzystania informacji.

Po trzecie, zostały opracowane zupełnie **nowe metody wyszukiwania informacji**. Nie każdy zdaje sobie sprawę, że głównym powodem popularności Internetu, a zwłaszcza usługi WWW (*World Wide Web* - ogólnoświatowa pajęczyna), jest ułatwienie wyszukiwania informacji posadowionej w sieci komputerowej w dowolnym punkcie globu ziemskiego. Kto umie z takich możliwości skorzystać - i wybrać informacje rzeczywiście istotne, nie tracąc czasu na zapoznawa-

nie się z informacjami ciekawymi, ale akurat nie najbardziej istotnymi - ten zapewnia sobie zasadniczą przewagę.

Po czwarte, nowe sposoby przesyłania, wyszukiwania i przetwarzania informacji spowodowały **możliwość rewolucyjnych przemian organizacji pracy i zarządzana**. Przykładem tego są tzw. **elastyczne systemy produkcyjne**, w których można wytwarzać produkty zindywidualizowane, przystosowane do potrzeb poszczególnych klientów, na żądany termin, a jednocześnie ograniczając do minimum niezbędne zapasy materiałów produkcyjnych - wszystko to wyłącznie przez zastosowanie odpowiednich metod komunikacji i przetwarzania informacji. Ale to tylko przykład; komunikacja multimedialna stworzy jeszcze inne możliwości zmian organizacji pracy i jej zarządzania. Wskazują na to np. prace nad tzw. **groupware**, czyli oprogramowaniem dla sieciowej pracy zespołowej.

Wszystko to powoduje, że odpowiednie wykorzystanie technologii czy technik informacyjnych może dziś wielokrotnie zmniejszyć koszty produkcji czy usług lub zwiększyć ich rentowność. Stąd też koszty technik informacyjnych stają się dziś w krajach rozwiniętych znacznym elementem kosztów, często dorównującym lub przekraczającym koszty robocizny. Informacja staje się więc podstawowym zasobem produkcyjnym w pełnym znaczeniu tego słowa.

Kilkanaście lat minęło zaledwie od początków epoki informacyjnej, a już przedsiębiorstwa technik informacyjnych dominują na rynkach krajów rozwiniętych. Klasycznym przykładem jest tu konkurencja *Microsoft* (firma znana większości użytkowników komputerów, dosadnie scharakteryzowana przez ekonomistę B. Arthura "*Great marketing of mediocre technology*") i *Netscape* (firma znana w Internecie, która pierwsza wprowadziła przeglądarki WWW o ogólnosieciowym zasięgu), firm uważanych dzisiaj za przodujące na rynku St. Zjedn. AP. Jednakże specjaliści na świecie są dziś zgodni, że są to zaledwie początki; możliwości ekspansji gospodarczej opartej na technice informacyjnej są dziś ogromne.

Od połowy XX wieku potrafimy dość dobrze określać **ilość informacji**; mniej natomiast rozwinięte są atrybuty **jakości informacji**. Do atrybutów takich można zaliczyć:

- **przydatność informacji**, czyli jej dostosowanie do potrzeb użytkowania;
- **aktualność informacji**, czyli jej dostosowanie do czasu użytkowania;
- **odpowiedzialność informacji**, czyli gwarancje jej poprawności;
- **typ własności informacji**, czyli określenie praw dostępu do niej;
- **typ ochrony informacji**, czyli sposoby utrudniające*) dostęp oraz modyfikację informacji przez osoby niepowołane.

Wraz z dalszym rozwojem epoki cywilizacji informacyjnej należy spodziewać się, że atrybuty jakościowe informacji będą dalej rozwijane i standaryzowane. Należy też jednak spodziewać się dalszej intensyfikacji już dziś obserwowanego **konfliktu o prawa dostępu do informacji**. W konflikcie tym wyróżnić można następujące perspektywy:

- przedsiębiorca uważa informację za zasób produkcyjny, a więc za dobro o określonej cenie, którego prawa własności powinny być ściśle określone;
- nauczyciel uważa informację za środek edukacji, a więc będzie za możliwie swobodnym dostępem do niej;
- przedstawiciel administracji rządowej uważa informację za narzędzie władzy, a więc będzie obstawał przy kontroli i wpływie na przepływ informacji;

*) Nie ma sposobów gwarantujących pełną ochronę informacji, ale istnieją już rozwinięte techniki kryptograficzne, zwłaszcza tzw. asymetryczne techniki kodowania, które gwarantują, że ich złamanie za pomocą najpotężniejszych komputerów świata trwałoby lata.

- "surfer Internetu" uważa informację za czynnik o tak nadrzędnym znaczeniu, że nikt nie powinien wtrącać się do jego umiejętności wyszukiwania i posługiwania się informacją!

Konflikt ten ma jednak też poważne, nie tylko żartobliwe znaczenie - związany jest on bowiem ze zmianami strukturalnymi ery cywilizacji informacyjnej oraz podstawowym konfliktem społecznym tej ery, czyli kwestią dostępu do edukacji i pracy.

4. ZMIANY STRUKTURALNE ERY CYWILIZACJI INFORMACYJNEJ

Zmiany możliwości technicznych i metod przetwarzania, przesyłania i magazynowania informacji wywołują już dziś i wywoływać będą przez następne kilkadziesiąt lat dalsze głębokie zmiany strukturalne. Wspominaliśmy wcześniej elastyczne systemy produkcyjne. W epoce cywilizacji informacyjnej należy spodziewać się dalszej intensywnej robotyzacji i automatyzacji produkcji przemysłowej, powodującej zmniejszenie kosztów tej produkcji oraz naczne zmniejszenie zatrudnienia w przemyśle. Nie oznacza to, że przemysł straci swe znaczenie, podobnie jak nie straciło znaczenia po dziś dzień rolnictwo. Oznacza to jednak, że **za lat sto, zarówno w przemyśle jak i w rolnictwie, będzie zatrudnionych po kilka procent ludności.**

Rozwiną się natomiast usługi najbardziej różnorodnego rodzaju, zwłaszcza - usługi komunikacyjno-rozrywkowe. W tej dziedzinie, obejmującej tradycyjne dziś środki przekazu (telewizję, radio i prasę), mogą nastąpić i już następują też ogromne zmiany. Zmiany te wynikają z nowych tendencji technicznych, do których należą:

- **przekaz multimedialny**, czyli integracja w jednym światłowodzie przekazu telewizyjnego, wideofonicznego, danych komputerowych itp.;
- **zbieżność technologiczna**, czyli tendencja do zastąpienia różnorodnych urządzeń elektroniki domowej (telefonu, radia, telewizora,

magnetowidu, komputera itp.) jedną lokalną, domową siecią komputerową ze standaryzowanymi elementami wykonanymi w jednej technice i pracujących w jednolitych standardach cyfrowych.

W związku z tymi tendencjami należy też spodziewać się integracji dotychczasowych rodzajów usług komunikacyjno-rozrywkowych, ale też zupełnie nowych modeli takich usług. Wystarczy wyobrazić sobie ogólnoświatową sieć cyfrowej telewizji interaktywnej, w której klient może sam wybierać sobie dowolną informację czy rozrywkę - włącznie z możliwością wyświetlenia na ekranie i w razie potrzeby wydruku dowolnie wybranych stron gazet, nie publikowanych już w formie tradycyjnej, ale wyłącznie w formie elektronicznej.

Silnie rozwijającą się formą usług będzie szkolnictwo, które ulegnie poważnym zmianom i dywersyfikacji (zróżnicowaniu), uwarunkowanym nie tylko przez możliwości techniczne (np. możliwość zdalnego nauczania z wykorzystaniem wideofonów), lecz także przez wymagania gospodarcze - gdyż informacja jako nowy zasób produkcyjny ma specyficzne wymagania edukacyjne - a także wymagania społeczne, które jeszcze omówimy nieco bardziej szczegółowo.

Należy też spodziewać się dalszych a zasadniczych zmian w rozwoju usług finansowych, zwłaszcza bankowości. Przewidywany jest dziś szybki rozwój sieciowych (zdalnych) usług bankowych i obsługi zakupów; niezbędna technika, polegająca przede wszystkim na odpowiedniej ochronie kryptograficznej danych, jest już w zasadzie rozwinięta i wymaga tylko dopracowania standardów i szczegółów.

Przy wszystkich tych perspektywach rozwoju gospodarczego należy jednak stwierdzić, że związane z nim zmiany strukturalne będą w zasadniczy sposób wpływać na tradycyjne pojęcia zawodów. **Utrata pracy wskutek dezaktualizacji wiedzy czy zawodu - to główne zagrożenie wieku XXI.**

Z teorii i historii długich cykli cywilizacyjnych wynika, że każdy taki cykl miał typowy dla siebie, główny spór społeczny. W epoce renesansu i reformacji spór ten znalazł wyraz w konflikcie katoli-

cyzm - protestantyzm, a dotyczył - jak wiadomo - praw do czytelnictwa i interpretacji Biblii, wraz ze wszystkimi wynikającymi stąd skutkami. W epoce cywilizacji przemysłowej spór ten wyraził się w konflikcie kapitalizm - komunizm, a dotyczył praw własności środków produkcji. Nadejście ery informacyjnej przyspieszyło upadek komunizmu, z wielu przyczyn - patrz np. Toffler, który dowodzi, że **cywilizacja informacyjna może rozwijać się tylko w warunkach gospodarki rynkowej i demokracji** (stąd tylko przypadkiem historycznym jest fakt, że Polska zapoczątkowała ten upadek). W każdym bądź razie, **spór kapitalizm - komunizm charakteryzował ubiegłą już erę** - z czego można wyciągnąć wiele wniosków. Tu przytoczymy tylko najważniejszy: w Polsce nie powinniśmy się koncentrować na odbudowie klasycznego kapitalizmu, ale na **budowie nowego społeczeństwa ery informacyjnej, opartego na zasadach demokracji i wykorzystującego mechanizmy rynkowe.**

W erze cywilizacji informacyjnej można oczekiwać nowego sporu społecznego. W związku z omówionymi wyżej mechanizmami zmian strukturalnych, będzie on dotyczył niewątpliwie praw dostępu do pracy i edukacji. Prawa te są związane, z jednej strony, ze wspomnianymi już możliwościami i prawami dostępu do informacji i jej wykorzystania w celach produkcyjnych oraz swobodą dostępu do informacji w celach badawczych i edukacyjnych.

Z drugiej strony, może on też dotyczyć nowego rozwarstwienia społecznego - którego nasilające się oznaki w St. Zjedn. AP opisuje w swych ostatnich książkach J.K. Galbraith. Możliwości automatyzacji i robotyzacji produkcji oraz komputeryzacji zarządzania znacznie zmniejszają zapotrzebowanie na siłę roboczą. Rozwiązaniem byłby skrócony czas pracy, ale wzmożona konkurencja na rynku pracy przeciwdziała temu rozwiązaniu, utrwala strukturalne bezrobocie - bo zmiany strukturalne gospodarki następują już tak szybko, że nigdy się nie kończą. Jedynym ubezpieczeniem przed bezrobociem staje się dobre wykształcenie. Wobec wysokich kosztów dobrego wykształce-

nia, brak dostępu do niego może stać się dziedziczny (przykłady takie podaje właśnie J.K. Galbraith). Może to stać się głównym mechanizmem nowego rozwarstwienia społecznego ery cywilizacji informacyjnej.

Jednak zmiany strukturalne wywołane postępem cywilizacji informacyjnej wymagają elastyczności i innowacyjności, a więc także silnego wpływu konkurencji rynkowej. Zbyt silne działanie opiekuńcze państwa bywa zatem często krytykowane, jako niesprzyjające innowacyjności. Należy więc spodziewać się dalszego nasilenia obserwowanego już konfliktu między opiekuńczą odmianą państwa kapitalistycznego - stosowaną dość powszechnie w Europie, zwłaszcza w Skandynawii, Niemczech, Austrii - a koniecznością zmian strukturalnych i innowacyjności. Fakt zmniejszającej się liczby miejsc pracy, wynikający z automatyzacji i robotyzacji, będzie zapewne tak silny, że rozwiązaniem okaże się jakaś forma społeczeństwa opiekuńczego - choć być może odmienna od obecnej. Odmienność ta wynika z faktu, że to właśnie problem podziału zmniejszającej się liczby miejsc pracy i przeciwdziałania nadmiernemu rozwarstwieniu społecznemu - na tle nie tylko kwestii praw, ale też faktycznych możliwości dostępu do edukacji informacji - stanie się podstawowym problemem społecznym ery cywilizacji informacyjnej.

Zauważmy, że jeśli informacja będzie traktowana coraz w większym stopniu jako własność, to dostęp do dobrej edukacji stanie się coraz bardziej kosztowny. Powszechność dostępu do edukacji stanie się tylko iluzją - osoby ubogie nie będzie stać, aby wykształcić swe dzieci na odpowiednim poziomie. Według J.K. Galbraitha, taki jest właśnie mechanizm nowej stratyfikacji (rozwarstwienia) społecznej, obserwowanej już wyraźnie w St. Zjedn. AP; mit pucybuta, który może stać się milionerem, przestał już funkcjonować, ubóstwo staje się dziedziczne.

Podobnego zdania, choć wychodząc z przeciwstawnych pozycji ideologicznych, jest ekonomista angielski I. Angell. Według jego

opinii, **nowa stratyfikacja społeczna jest faktem dokonanym** i pozytywnym - wykształcony w technice komputerowej nadczłowiek będzie panem świata, a ciemnym masom należy się miejsce podrzędne. Niezależnie od przesłanek ideologicznych, stanowisko takie budzi jednak zasadniczy sprzeciw pragmatyczny: **silna stratyfikacja społeczna wywoła** bowiem, jak to wynika z historii i z teorii cykli cywilizacyjnych, **konflikty społeczne, nowe rewolucje i wojny**. Stabilny rozwój może być zagwarantowany tylko wtedy, gdy nieuchronnie występujące nierówności*) nie staną się nadmierne i - co najważniejsze - nie będą dziedziczne. Zdolni ludzie muszą mieć szanse wybicia się niezależnie od odziedziczonych zasobów - jeśli bowiem takich szans nie będą mieli, to oni staną się przywódcami nowych rewolucji.

Dlatego też nowej stratyfikacji należy przeciwdziałać. W Stanach Zjedn. AP przewiduje się, że narzędziem takiego przeciwdziałania będzie upowszechnienie dostępu do *Globalnej Infrastruktury Informacyjnej* oraz reforma systemu edukacyjnego. Nie ulega przy tym wątpliwości, że opracowanie nowego systemu edukacyjnego na potrzeby epoki cywilizacji informacyjnej będzie tu odgrywać rolę zasadniczą. Nie jest to jednak zadanie łatwe. Nowy system edukacyjny powinien bowiem m.in.:

- być **dostępny dla wszystkich** i pomagać wszystkim w uzyskaniu zatrudnienia w epoce cywilizacji informacyjnej;
- być **zdywersyfikowany** co do poziomu i jakości, ale zapewniać najzdolniejszym dostęp do edukacji najwyższej jakości, niezależnie od posiadanych przez nich zasobów finansowych;
- być **kosztowny** (bo inaczej nie przygotuje dobrze do pracy w społeczeństwie informacyjnym), ale opłacany częściowo z budżetu państwa, a częściowo - ze środków indywidualnych;

*) Niezbędne jako metoda motywacji do pracy, jak to wynika z niedawnej historii.

- zapewniać **synergię** (wzmocnienie oddziaływania) nowej techniki z tradycją, to jest łączyć zalety wykorzystania multimedialnych sieci komunikacyjnych z wpływem bezpośredniego kontaktu z dobrym nauczycielem.

Opracowanie takiego systemu zajmie prawdopodobnie dziesięciolecia - w ciągu których nowa stratyfikacja i związane z nią napięcia będą narastać. Jak wspomnieliśmy bowiem na wstepie, przy wyjaśnieniu mechanizmu długich cykli cywilizacyjnych: decydujące są tu nie ograniczenia materialne, ale przyzwyczajenia ludzi, czas niezbędny na to, aby większość społeczeństwa przyswoiła sobie nowe pojęcie lub uświadomiła konieczność zmiany.

Na zagadnienie przemian strukturalnych i związanych z nimi konfliktów społecznych można też spojrzeć z innej perspektywy. Problemy te występują w najbogatszych krajach świata; a jak odbijają się one na krajach uboższych? Otóż odbicie tych problemów w krajach uboższych, które nie są jeszcze w pełni przygotowane do cywilizacji informacyjnej i nie podejmują aktywnie tego problemu - np. w krajach Ameryki Łacińskiej - jest jeszcze bardziej wyraziste. W tym przypadku mówi się wyraźnie o **porażce klasy średniej**, gdyż rozwarstwienie w tych krajach pozostawia w strefie bogactwa tylko bardzo wąskie elity. Ocenia się też, że klasyczna gospodarka wolnorynkowa w tych krajach zawodzi. Jak się wydaje, jest to skutek **mechanistycznego sposobu widzenia świata**, znamiennego dla ery cywilizacji przemysłowej. Charakteryzuje się on wiarą w nadrzędne mechanizmy - czy to prawa historii w marksizmie, czy prawa rynku w neoliberalizmie. I taki właśnie, mechanistyczny sposób pojmowania świata jest największym niebezpieczeństwem, utrudniającym przygotowanie czy to krajów Ameryki Łacińskiej, czy też Polski do wyzwań ery cywilizacji informacyjnej.

Argumentuje się bowiem, z jednej strony, że nie ma skrótów rozwojowych, że Polska musi najpierw powtórzyć wszystkie etapy rozwoju, które przeszły kraje rozwinięte. Z drugiej strony twierdzi się,

że o wszystkim zadecyduje rozwój rynku. Jeżeli lansuje się tezę, że nauka powinna sama na siebie zarobić konsultacjami i wobec tego wystarczą w budżecie państwa wydatki na naukę o względnym poziomie charakterystycznym dla krajów trzeciego świata, to takie właśnie mechanistyczne widzenie świata wywołuje samosprawdzającą się przepowiednię: nic w Polsce nie zdziałamy w zakresie cywilizacji informacyjnej, bo decydują za nas inne kraje (a skoro postanowimy, że nic nie zdziałamy, to itotnie tak się stanie).

Jeśli jednak spojrzeć na te problemy z innej perspektywy postrzegania świata, postmodernistycznej (w której rozwój postrzegany jest nie mechanistycznie, lecz jako proces chaotyczny*), znamiennej dla epoki cywilizacji informacyjnej, to można mieć poglądy zupełnie odmienne. Małe zmiany w punkcie zwrotnym mogą mieć ogromne znaczenie; a znajdujemy się bez wątpienia w okresie przełomu epok. W tym też sensie powinniśmy przemyśleć szczegółowo naszą strategię, zwłaszcza w odniesieniu do roli techniki w erze cywilizacji informacyjnej.

5. TECHNIKA W CYWILIZACJI INFORMACYJNEJ

Technika w kształtowaniu się cywilizacji informacyjnej ma trzy zasadnicze aspekty. Są to:

- **automatyzacja i robotyzacja produkcji,**
- **nowe technologie przetwarzania surowców i energii,**
- **techniki informacyjne - przesyłania, przetwarzania i magazynowania informacji.**

*) W sensie deterministycznej teorii chaosu, jako nieodłącznej cechy nieliniowych systemów dynamicznych ze sprzężeniem zwrotnym, charakteryzujących się bardzo złożonym, nieprzewidywalnym w szczegółach zachowaniem, ale też wielką wrażliwością na warunki początkowe.

Nadrzędny dla kształtowania się ery cywilizacji informacyjnej jest oczywiście aspekt trzeci; ale wymieniamy tu najpierw dwa inne ważne aspekty, aby przedyskutować ich rolę w porównaniu z tym trzecim, który omówimy dalej nieco obszerniej.

W odniesieniu do pierwszego z tych aspektów trzeba stwierdzić, że technika w ogóle i techniki informacyjne w szczególności zmieniają tradycyjny kształt oraz rolę przemysłu - zaczynając od jego roli nadrzędnej w erze cywilizacji przemysłowej, czynności absorbującej większość ludności, a dochodząc w perspektywie stulecia do jego roli wprawdzie ważkiej, ale dającej w niektórych krajach zatrudnienie tylko niewielkiej części ludności. Jest to rola techniki, wyrażająca się automatyzacją i robotyzacją produkcji, wraz z zastosowaniem technik komputerowych sieci przemysłowych do elastycznego zarządzania i sterowania produkcją. Trzeba tu też dodać, że automatyzacja i robotyzacja nie ograniczą się do przemysłu; umożliwią one również znaczne usprawnienie rolnictwa, a także bardziej tradycyjnych usług.

Wiadomo, że kraje najbardziej rozwinięte ograniczają zatrudnienie w przemyśle, rolnictwie, a także w mniej atrakcyjnych usługach drogą nie tylko automatyzacji i robotyzacji, lecz także przez przesunięcie mniej atrakcyjnych czynności produkcyjnych do krajów rozwijających się. Dla krajów rozwijających się oznacza to krótkoterminowe korzyści, długoterminowo zaś - pogłębienie problemów i trudności. Tym niemniej, stopniowo, także w tych krajach będzie malał udział ludności zatrudnionej w rolnictwie i przemyśle; ponadto, kraje rozwinięte zachowają i będą chronić, ze względów strategicznych, pewne działy rolnictwa i przemysłu. Przesunięcia mniej atrakcyjnych form zatrudnienia ograniczą się wtedy do dziedziny usług - bardziej tradycyjnych czy mniej atrakcyjnych. Oczywiście, w skali lokalnej, takie przesunięcia mogą być powodem bezrobocia w krajach bardziej rozwiniętych; ale w skali globalnej głównym powodem bezrobocia są zmiany strukturalne, wywołane automatyzacją i robotyzacją produkcji.

Automatyzacja i robotyzacja są więc jednym z zasadniczych powodów strukturalnego bezrobocia. Dlatego też często ten właśnie aspekt roli techniki wywołuje resentymenty społeczne. Trzeba jednak pamiętać, że automatyzacja i robotyzacja zastępuje w pierwszym rzędzie pracę niebezpieczną dla zdrowia, nużącą i jednostajną, wymagającą wielkiej precyzji czy koncentracji uwagi. I choć z tym właśnie aspektem mogą się wiązać szczególne protesty społeczne na początku ery cywilizacji informacyjnej - podobne do ruchów ludystycznych w Anglii na początku XIX wieku - to jednak jest to aspekt bardzo ważny, kształtujący zasadnicze zmiany strukturalne tej ery.

Aspekt ten będzie wymagał bardzo przemyślanej polityki państwa, gdyż związany jest z nader trudnymi dylematami. Z jednej strony, zbyt szybkie wprowadzanie automatyzacji i robotyzacji zwiększa stopę bezrobocia. Z drugiej strony, ograniczenia tego procesu - np. przez subwencjonowanie bardziej tradycyjnych a pracochłonnych dziedzin produkcji - spychają kraj do pozycji kraju mniej rozwiniętego, otwierają go na przesunięcia mniej atrakcyjnych rodzajów działalności produkcyjnej z krajów wyżej rozwiniętych. I odwrotnie; jeśli pozostawić wolnemu rynkowi rozwiązanie tych zagadnień, to też pozostawia się w tej dziedzinie inicjatywę strategiczną wielkim korporacjom międzynarodowym, które będą lokować w danym kraju taką działalność produkcyjną, jaka jest akurat im dogodna. Jednakże, wolny rynek jest motorem napędowym cywilizacji informacyjnej, i nadmierne jego ograniczenia zmniejszą szanse kraju w wyścigu cywilizacyjnym. Jak wszystkie pozornie nierozwiązywalne dylematy, problemy te rozwiązywać trzeba przez jakościowo odmienne podejścia.

By nie ograniczać roli rynku, a jednak na nią wpływać, trzeba stosować podejście **nie tyle restrykcyjne, co promocyjne**. Ale trzeba wtedy dobrze wiedzieć, co i jak chce się promować - a więc, w przypadku automatyzacji i robotyzacji (które są tu tylko ważnym przykładem, rozumowanie bowiem odnosi się również do innych dziedzin techniki), **trzeba najpierw promować badania naukowe i wykształ-**

cenie rodzimych specjalistów w tej dziedzinie. Dotyczy to zresztą wszystkich trzech decydujących dziedzin techniki, wymienionych wyżej: **bez inwestycji w potencjał intelektualny tych dziedzin skazujemy się na niewiedzę, na stanie się łatwym obiektem manipulacji przez innych.**

Znaczenie automatyzacji i robotyzacji, elastycznych systemów produkcyjnych i innych związanych z tym dziedzin jest tak duże, że niekiedy utożsamia się te dziedziny z technikami informacyjnymi. Istotnie, dziedziny te opierają się na wykorzystaniu technik informacyjnych do sterowania i zarządzania produkcją. Co więcej, podstawy teoretyczne tych dziedzin są nierozłącznie związane z podstawami teoretycznymi przetwarzania informacji. Jednakże skuteczna automatyzacja i robotyzacja wymaga głębokiej znajomości nie tylko podstaw teoretycznych oraz technik informacyjnych, lecz także - różnych dziedzin techniki (a także rolnictwa czy usług), do których stosuje się automatyzację i robotyzację. Dziedziny te więc należy raczej klasyfikować jako interdyscyplinarne, choć świśle związane z technikami informacyjnymi.

Bardzo ważny jest drugi aspekt wyżej wymieniony - nowe technologie przetwarzania surowców i energii. I w tym zakresie musimy inwestować w potencjał intelektualny - niewiedza w ważnych kwestiach zawsze kosztuje więcej, niż wykształcenie własnej ekspertyzy. Dotyczy to wielu zagadnień, które trudno szerzej rozwijać w tym artykule - biotechnologii i technik genetycznych; nowych materiałów, w tym np. ceramicznych; alternatywnych źródeł energii, w tym np. energii geotermicznej. Na przykładzie tych zagadnień omówimy tylko inny ważny aspekt współczesnej techniki: **globalizację techniki, opartą na sieciowym, globalnym dostępie do informacji.**

We wszystkich dziedzinach wysokiej techniki obserwujemy dzisiaj wykorzystanie sieci komputerowych - a zwłaszcza usługi WWW - do globalnego udostępniania i przesyłania informacji. Proces ten dotyczy

kilku warstw informacyjnych: tzw. stron domowych (*home pages*) czy stron WWW uczelni, w tym technicznych, które wykorzystują tę usługę do przedstawienia zakresu swej działalności badawczej, ale też coraz częściej prezentują także materiały dydaktyczne, np. treści wykładów; stron WWW dużych przedsiębiorstw wysokiej techniki, które wykorzystują tę usługę głównie jako narzędzie reklamy, ale popartej dość głęboką informacją; wreszcie informacji bibliotecznych, dostępnych (też coraz częściej jako strony WWW) w formie katalogów, abstraktów, czy nawet pełnych tekstów zasobów bibliotecznych w formie elektronicznej. Zaletą usługi WWW jest stosunkowo łatwe wyszukiwanie potrzebnej informacji - choć oczywiście, wybuchowy rozwój ilości dostępnej informacji zawsze grozi trudnościami w jej przeszukiwaniu.

Globalizacja informacji technicznych - zwłaszcza w odniesieniu do nowych technologii przetwarzania surowców i energii - spowoduje w przyszłości nieuchronnie większą specjalizację badań, szczególnie o charakterze podstawowym. Wyniki badań będą dość powszechnie udostępniane w sieci komputerowej; informacja o wynikach badań podstawowych jest bowiem często traktowana jako dobro publiczne. Natomiast informacja o wynikach badań bardziej stosowanych w dziedzinie techniki będzie oczywiście traktowana jako własność indywidualna i dostępna raczej w sensie reklamy oraz promocji konkretnych rozwiązań; techniczne badania stosowane, choć do pewnego stopnia ułatwione przez globalizację informacji technicznych, będą jednak tak jak dotąd określane przez uwarunkowania rynkowe i potrzeby lokalne.

6. ISTOTNE TREDNY BADAWCZE W TECHNICE INFORMACYJNEJ

Nieco szerzej omówimy tu trzeci, być może najważniejszy, aspekt roli techniki w cywilizacji informacyjnej. Chodzi tu o techniki infor-

macyjne - przesyłania, przetwarzania i magazynowania informacji - które stanowią główne narzędzia ery cywilizacji informacyjnej. Zaliczyć do nich należy przede wszystkim **telekomunikację** i **informatykę**, choć nieodłączną częścią technik informacyjnych jest też, jak wspomniano wyżej, **automatyka i robotyka**, a także **elektronika**, której rozwój umożliwił ekspansję innych dziedzin technik informacyjnych. Nie oznacza to jednak, że techniki informacyjne należy ograniczyć tylko do wymienionych tu dziedzin. Równie istotne są związane z nimi pewne interdyscyplinarne dziedziny techniki, których przykłady podamy dalej. Z rozwojem cywilizacji informacyjnej związane też są inne ważne a nietechniczne badania interdyscyplinarne, np. obejmujące:

- ogólne trendy, wyzwania i zagrożenia, szanse i mechanizmy epoki cywilizacji informacyjnej;
- aspekty ekonomiczne i prawne epoki cywilizacji informacyjnej, w tym w szczególności - problemy ekonomiki telekomunikacji;
- aspekty kulturowe i edukacyjne epoki cywilizacji informacyjnej.

Zaczniemy jednak od dziedziny, która rozwija się dziś niezwykle szybko i stworzyła warunki dla cywilizacji informacyjnej, m.in. umożliwiając globalizację informacji - czyli **telekomunikacji**. W tej dziedzinie, za szczególnie istotne uważa się dziś m.in. badania w niżej podanych obszarach.

- **Usługi multimedialne**. Podkreślić tu trzeba, że choć rozwiązania techniczne wideofonu są już dziś znane, to jednak na masowe jego upowszechnienie trzeba będzie jeszcze zaczekać - jedno lub kilka dziesięcioleci - gdyż goranicza je koszt takiego aparatu oraz pasmo przenoszenia istniejących sieci. Do czasu pełnego upowszechnienia wideofonu, odpowiednie rozwiązania - oraz możliwości łączenia różnych usług, jak np. w telewizji interaktywnej - będą testowane w różnorodnych usługach multimedialnych.

- **Ochrona oraz bezpieczeństwo danych i usług w sieciach**. Jest to problem może nawet bardziej aktualny, niż usługi multimedialne. Wykorzystanie sieci do usług bankowych i komercyjnych wymaga znacznie większego poziomu zabezpieczeń sieci, usług i danych przed niepowołanym użyciem lub modyfikacją, niż to zapewniają typowe rozwiązania sieciowe. Podstawy teoretyczne takich zabezpieczeń, oparte na asymetrycznych kodach kryptograficznych, są znane; ale znów minie czas pewien, niezbędny na odpowiednie opracowania techniczne, zanim rozwiązania takie staną się powszechne.
- **Zarządzanie oraz nadzór sieci i usług**. Współczesne sieci telekomunikacyjne i komputerowe stają się tak złożone, że nie wystarczają dziś tradycyjne metody zarządzania oraz nadzoru sieci i usług. Jest to dziedzina rozwijająca się szczególnie szybko, choć odbija się na niej też dualizm podejścia do sieci telekomunikacyjnych (od najniższych warstw w górę) lub do sieci komputerowych (od najwyższych warstw w dół). Zgodnie z tym dualizmem, podejścia do zarządzania siecią mogą albo koncentrować się na problematyce warstw najniższych, albo na problematyce warstw najwyższych.
- **Metodyka planowania i projektowania sieci**. Złożoność współczesnych sieci powoduje konieczność opracowania nowych podejść do planowania ich rozbudowy czy też projektowania ich nowych części. Istotny jest tu rozwój rozmaitych narzędzi komputerowo wspomaganego projektowania, a nawet zastosowanie metod komputerowego wspomagania decyzji (które mogą być też stosowane do nadzoru złożonych sieci).
- **Metody przetwarzania sygnałów**. Nowe podejścia do metod przetwarzania sygnałów są niezbędne, np. w przypadku transmisji multimedialnej (gdzie wymagana jest *kompresja* cyfrowych sygnałów wizyjnych dla zmniejszenia niezbędnego pasma), ale także

w przypadku analizy obrazów uzyskiwanych drogą satelitarną, odszumiania sygnałów, eliminacji odbić itp.

- **Propagacja fal elektromagnetycznych**. Istotne są tu nowe zastosowania tej dziedziny o dużych tradycjach - w systemach telefonii komórkowej, systemach satelitarnych, ale także w systemach światłowodowych o bardzo dużym pasmie, w związku z problemami kompatybilności elektromagnetycznej itp.

Kolejna dziedzina, o równie podstawowym znaczeniu, to **informatyka**, która stworzyła techniki przetwarzania i magazynowania informacji równie istotne dla cywilizacji informacyjnej jak techniki przesyłania informacji stworzone przez telekomunikację*). Za szczególnie istotne dla informatyki można dziś uznać następujące obszary badań.

- **Teoretyczne podstawy informatyki**. Wymienić tu można m.in. teorię współbieżności, matematyczne podstawy programowania, podstawy architektury komputerów, itp.
- **Komputerowe wspomaganie decyzji**. Należą tu m.in. systemy eksperckie i problematyka inżynierii wiedzy, statystyczne i wielokryterialne metody optymalizacji decyzji, zastosowania logiki wielowartościowej, itp.
- **Problemy komunikacji człowiek - maszyna** - a więc grafiki komputerowej, rozpoznawania obrazów i mowy, itp.
- **Inżynieria oprogramowania**, wraz z formalizmami specyfikacji, dokumentacji i weryfikacji oprogramowania, metodami programowania, ze szczególnym uwzględnieniem oprogramowania sieciowego - specyficznych języków oprogramowania do zastosowań sieciowych, multimedialnych baz danych itp.

---

*) Zresztą różnice między poszczególnymi dziedzinami składającymi się na techniki informacyjne będą ulegać stopniowemu zmniejszeniu.

- **Problemy systemów rozproszonych i równoległych**, wraz z mechanizmami komunikacji, problematyka przetwarzania informacji, baz danych i metod obliczeniowych.

Zagadnienia **automatyki** były omawiane już wcześniej, wymienimy tu tylko kilka zakresów problematyki badawczej:

- komputerowe systemy oraz sieci pomiarowe i nadzoru,
- komputerowe systemy oraz sieci przemysłowe do zarządzania i sterowania produkcją,
- sterowanie i konstrukcja robotów,
- elastyczne systemy produkcyjne.

Wspomnieliśmy już, że szczególnie istotne dla rozwoju technik informacyjnych mogą być badania interdyscyplinarne, w tym np. między naukami ścisłymi a technicznymi. Tak więc, na przecięciu elektroniki i fizyki niezwykle istotny będzie rozwój **optoelektroniki i fotoniki**, w tym głównie metod optycznego wzmacniania sygnałów, warunkujących dalsze zwiększenie szybkości transmisji w sieciach telekomunikacyjnych. Innym przykładem dziedziny interdyscyplinarnej, ważnej dla rozwoju technik informacyjnych, jest modelowanie matematyczne - rozwijane początkowo na przecięciu automatyki i informatyki, później wraz z biologią, fizyką, chemią i matematyką (zwłaszcza w biologii molekularnej, biochemii, bioinżynierii), dziś sięgające nawet poza te dziedziny i nabierające podstawowego znaczenia, np. dla nauk rolniczych i środowiskowych.

Powyższe przykłady nie wyczerpują wszystkich dziedzin badań, które będą istotne dla rozwoju technik czy technologii informacyjnych, wskazują jednak na znaczenie zarówno badań dyscyplinarnych, jak i - a nawet zwłaszcza - badań interdyscyplinarnych dla rozwoju cywilizacji informacyjnej. Kraj, który skoncentruje swe wysiłki badawcze na takich dziedzinach, ma szanse odegrać znaczną rolę w przyszłym światowym społeczeństwie informacyjnym. Kraje, które tego dziś nie uczynią, skazują się na rolę podrzędną.

7. WNIOSKI

Patrząc z takiej perspektywy, dochodzimy do następujących wniosków.

- Krytyczne znaczenie - dla przyszłego miejsca Polski w Europie i na świecie - ma odpowiednia głęboka oraz przemyślana reforma systemu edukacji, skierowana na potrzeby cywilizacji informacyjnej; reforma ta będzie wymagać od społeczeństwa zainwestowania znacznie większych środków, niż dotychczas, w edukację na wszystkich poziomach.
- Nie może być dostatecznie dobrej edukacji na poziomie uniwersyteckim bez odpowiednich inwestycji w badania naukowe, a więc społeczeństwo polskie musi też znacznie zwiększyć (np. podwoić, aby dojść do przyzwoitego poziomu europejskiego) inwestycje w badania naukowe.
- Priorytety tematyczne w Polsce dotyczące zagadnień edukacji i badań naukowych powinny być podobne jeśli nawet nie do priorytetów St. Zjedn. AP, to co najmniej do priorytetów Unii Europejskiej. Stąd też podstawowy priorytet powinien dotyczyć zagadnień szeroko pojętych technik informacyjnych (telekomunikacji, informatyki, automatyki, elektroniki i dziedzin pokrewnych), a zwłaszcza sieci komputerowych wraz z ich różnorodnymi zastosowaniami - w zarządzaniu, finansowości, ochronie środowiska, ochronie zdrowia, rolnictwie itp.
- W cywilizacji informacyjnej należy spodziewać się, w XXI stuleciu, stopniowego zmniejszenia udziału osób czynnych zawodowo w przemyśle. **Nie oznacza to jednak zmniejszenia roli techniki, która będzie podstawowym narzędziem** nie tylko dla usług informacyjnych, znamiennych dla **nowej ery**, lecz także - dla podstawowych zmian strukturalnych tej ery, polegających na automatyzacji i robotyzacji produkcji.

- Zrozumienie przesłanek epoki cywilizacji informacyjnej, jej szans i związnaych z nią zagrożeń jest podstawowym warunkiem przygotowania Polski do wyzwań przyszłości.

Анджей П. Вежбицки

РОЛЬ ТЕХНИКИ В ЦИВИЛИЗАЦИИ ИНФОРМАЦИИ

Резюме

Даются разсуждения относительно роли техники в цивилизации информации. Приводится анализ избранных проблемм эры цивилизации промышленности и цивилизации информации, которые являются источником общественных и экономических конфликтов. К найболее существенным проблеммам автор зачисляет изменение спроса на труд что в свою очередь вызовет глубокую структуральную безработницу,а также неодинаковый доступ к образовании, которое потребуется в эре информации. Всё это вызовет новое разслоение общества. На этом фане весьма существенны будет найти ответ на вопрос роли техники, особенно информатической техники, в этой новой эре. По мнению автора, техника - в новом глобальном мышлении и в новом масштабе будет решающим орудием эры цивилизации промышленности несмотря на постепенное относительное снижение объема промышленного производства в вырабатываемым валовом продукте.

Andrzej P. Wierzbicki

ROLE OF THE TECHNOLOGY IN INFORMATION CIVILIZATION

Summary

The paper presents a commentary on the role of technology in information civilization. It is based on analysis of chosen problems of the change

from industrial era towards information civilisation epoch, causing social and economic conflicts. Among the most important problems, the following are discussed: the changes of demand for work which will be the reason of a deep structural unemployment, and disparities in the access to good education necessary for information era. These problems will result in a new social stratification. Against this background an essential question is, what will be the future role of technology and, particularly, of information technology. In author's opinion, technology - in its new global meaning and dimension - will play the role of a decisive instrument of this period of change of industrial era towards information epoch - the gradual decreasing share of industrial production in Gross National Product (GNP) notwithstanding.

Andrzej P. Wierzbicki

ROLE DE LA TECHNIQUE DANS LA CIVILISATION D'INFORMATION

Résumé

L'article constitue une réflexion sur le rôle de la technique dans une civilisation d'information. Il est fondé sur l'analyse des problèmes choisis dudétour de l'ère de la civilisation industrielle et celle d'information d'où les sources des conflits sociaux ainsi qu'économiques. L'auteur en classe au nombre des plus importantes: des changements de la demande entravail qui constituent la cause du profond chômage structurel et l'autre qu'est inégal accès à l'éducation conforme aux éxigences de l'ère d'information en conséquence de ça nouvelle différenciation des couches sociales. A la base de ça ce qui est important c'est la réponse à la question: quel sera le rôle à jouer de la technique surtout celle d'information. A l'opinion de l'auteur c'est la technique en compréhension globale et en dimension nouvelle qui sera l'instrument décisif pour déclin de l'ère de la civilisation industrielle malgré la diminution progressive de participation de la production industrielle au produit national.

Andrzej P. Wierzbicki

DIE ROLLE DER TECHNOLOGIE IN INFORMATIONSZIVILISATION

Z u s a m m e n f a s s u n g

Im Beitrag wird die Rolle der Technologie in Informationszivilisation betrachtet. Eine Analyse von gewählten, sozialen und wirtschaftlichen Konflikte bewirkenden Probleme der Wende im Industrie- und Informationszivilisation stellt die Basis des Beitrags dar. Für die wichtigsten Probleme hält der Autor die den strukturellen Arbeitslosenstand nach sich ziehenden, tiefen Veränderungen in Arbeitsnachfrage, wie auch ungleichmäßigen Zugang zu der den Erfordernissen der Informationsära angepaßten Ausbildung, was neue Sozialschichtungen zu Folge hat. Daher wird wichtig ein Antwort auf die Frage, was wird Rolle Technologie, und besonders Informationstechnologie in Zukunft. Autor meint, daß in einem neuem globalem Sinne und neuer Maße wird doch die Technologie ein entscheidendes Instrument der neuen Zivilisationsära werden, obwohl der Anteil der industriellen Produktion in Nationalprodukt stetig sinken wird.

Elżbieta Andrukiewicz 681.324:699.8

ZARZĄDZANIE ZABEZPIECZENIEM SYSTEMU INFORMATYCZNEGO

W artykule przedstawiono model zarządzania zabezpieczeniami systemu informatycznego. Przedyskutowano podstawowe zasady tworzenia polityki zabezpieczenia systemów informatycznych w przedsiębiorstwach. Zarządzanie zabezpieczeniami podzielono na procesy: planowania i eksploatacji zabezpieczeń. Szczegółowo omówiono najważniejszy element fazy planowania, zarządzanie ryzykiem. Opisano procesy eksploatacji zabezpieczeń, do których należą: zarządzanie konfiguracją, monitorowanie systemu zabezpieczenia, procedury postępowania w przypadku naruszenia zabezpieczenia systemu informatycznego oraz w stanach awaryjnych i katastrofalnych.

1. POTRZEBA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO PRZEDSIĘBIORSTWA

1.1. Wstęp

W miarę, jak przedsiębiorstwo zwiększa swe uzależnienie od technik informatycznych, w sposób naturalny zmniejszają się możliwości kontroli informacji, która jest przechowywana i przetwarzana w systemie. Jednocześnie wzrasta wymierna wartość zasobów systemu informatycznego. Osoby odpowiedzialne za zarządzanie przedsiębiorstwami rzadko uświadamiają sobie ryzyko związane z utratą informacji i nie potrafią dostrzec znaczenia zabezpieczania swoich systemów informatycznych. Przedsiębiorstwa i urzędy wydają rocznie ogromne sumy na zakup sprzętu i oprogramowania komputerowego,

natomiast bardzo niewiele - na zabezpieczenie zasobów informatycznych.

Prowadzenie przemyślanej polityki związanej z zabezpieczeniem systemu informatycznego, planowanie i eksploatacja zabezpieczenia może uchronić przedsiębiorstwa od poważnych problemów organizacyjnych oraz finansowych, wynikających z niewłaściwego funkcjonowania systemu informatycznego.

Kwestia zabezpieczenia systemu informatycznego przedsiębiorstwa nie doczekała się jeszcze całościowego opracowania. Nie istnieją żadne międzynarodowe standardy w tym zakresie. Po kilku latach pracy nad dokumentami roboczymi Międzynarodowa Organizacja Normalizacyjna (ISO) wydała jedynie raport techniczny, nie mający statusu normy [4]. Jedynym państwem, które ma normę krajową jest Wielka Brytania [1]. W USA trwają prace nad standardem amerykańskim [5]. Oczywiście, wiele krajów i organizacji stosuje własne, wewnętrzne zalecenia. W większości przypadków są to opracowania niepublikowane.

Istnieje obszerna literatura poświęcona technicznym aspektom zarządzania zabezpieczeniem systemów informatycznych, w szczególności analizie ryzyka. Na świecie są stosowane zautomatyzowane narzędzia analizy ryzyka. Najbardziej znanym systemem eksperckim jest CRAMM**). Podstawową wadą zautomatyzowanych systemów eksperckich jest przyjęcie założenia, że zabezpieczenie ma jedynie aspekt techniczny. Tymczasem jest to problem z dziedziny zarządzania przedsiębiorstwem, a nie tylko techniki informatycznej. Zabezpieczenie systemu informatycznego, zbudowane jedynie na podstawie zautomatyzowanych narzędzi, jest zatem rozwiązaniem niekomplet-

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

nym. **System zabezpieczenia musi być tworzony z uwzględnieniem procesów zarządzania zabezpieczeniem.**

Tematem pracy statutowej Instytutu Łączności nr 073017 pt. "Planowanie i zarządzanie zabezpieczeniami systemu informatycznego", rozpoczętej w 1997 r., jest próba stworzenia koncepcji zabezpieczenia systemów informatycznych. Na podstawie tej koncepcji można zbudować, wdrożyć i eksploatować plan zabezpieczenia systemu informatycznego **każdego** przedsiębiorstwa. Jednym z efektów tej pracy będzie plan zabezpieczenia sieci lokalnej IŁ. Zakończenie pracy jest przewidywane na 1998 rok.

W niniejszym artykule zaprezentowano koncepcję zarządzania zabezpieczeniem systemu informatycznego, która powstaje jako wynik wyżej wymienionej pracy statutowej IŁ.

1.2. Bezpieczeństwo systemu informatycznego

System informatyczny uznaje się za bezpieczny, jeśli gwarantuje:

- **poufność,** co oznacza ochronę przed ujawnieniem informacji nieuprawnionemu odbiorcy;
- **integralność,** co oznacza ochronę przed modyfikacją lub zniekształceniem informacji przez nieuprawnionego użytkownika systemu;
- **dostępność,** co oznacza uprawniony dostęp do informacji przy zachowaniu określonych rygorów czasowych;
- **możliwość ewidencjonowania (rozliczalność),** co oznacza określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu informatycznego;
- **uwierzytelnienie,** co oznacza sprawdzenie tożsamości podmiotów lub zasobów systemu informatycznego.

W literaturze zestaw wyżej wymienionych pojęć występuje często pod postacią skrótu CIA+[*].

Zabezpieczanie systemów informatycznych obejmuje wszelkie działania związane ze zdefiniowaniem, osiągnięciem i utrzymaniem celów zabezpieczenia, jakimi są CIA+.

Ostatnio, do definicji bezpieczeństwa dodano jeszcze jedno, szóste kryterium bezpieczeństwa - **niezawodność** (*reliability*). Przez to pojęcie rozumie się gwarancję odpowiedniego zachowania się systemu informatycznego i otrzymanych wyników [4].

1.3. Elementy zabezpieczenia systemu informatycznego

Zabezpieczanie systemów informatycznych wymaga zdefiniowania grupy podstawowych pojęć [7], umożliwiających przeprowadzenie analizy systemu informatycznego, zaproponowanie mechanizmów zabezpieczeń i utrzymanie stanu bezpieczeństwa w warunkach działania przedsiębiorstwa w dynamicznie zmieniającym się środowisku. Poniżej wymieniono te pojęcia.

Aktywa (systemu informatycznego) - wszelkie oprogramowanie, dane, sprzęt, zasoby administracyjne, fizyczne, komunikacyjne lub ludzkie w systemie informatycznym albo działalności informatycznej.

Zagrożenia - przyczyny niepożądanych zdarzeń, których efektami są szkody w systemie informatycznym.

Słabość - podatność systemu lub majątku na zagrożenia jest wyrażona łatwością, z jaką dane zagrożenie może wyrządzić szkodę. Przykładowo, nieautoryzowany dostęp do sieci może się zdarzyć, gdy osoba z zewnątrz odgadnie hasło (słabość systemu - procedury generacji haseł). Słabe punkty zarządzania całym majątkiem, takie jak:

---

[*] CIA+ - to skrót angielskich określeń: *confidentiality, integrity, availability, accountability i authenticity.*

fizyczne rozmieszczenie, organizacja, stosowane procedury, personel, zarząd, administracja, sprzęt, oprogramowanie i informacja, mogą być wykorzystane do stworzenia zagrożenia. Konsekwencją tego są niepożądane zdarzenia, które mogą spowodować straty w systemie informatycznym lub zakłócić realizację celów przedsiębiorstwa. Samo określenie słabości nie powoduje szkody; słabość jest zbiorem warunków, które mogą umożliwić urzeczywistnienie się zagrożenia. Analizę słabości systemu należy przeprowadzić przed wprowadzeniem mechanizmów zabezpieczeń oraz po ich implementacji.

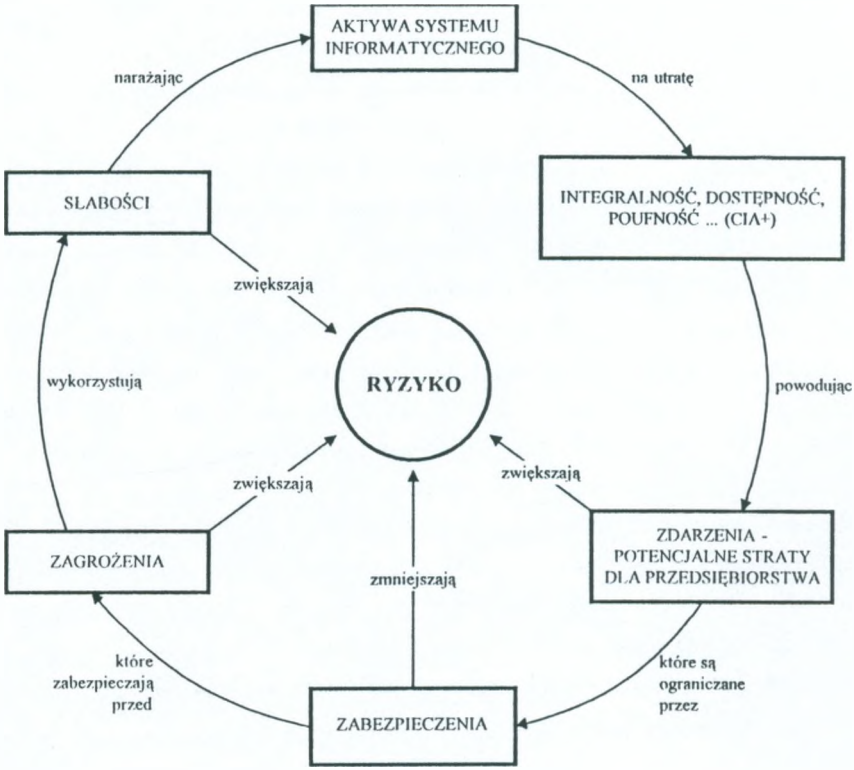
Zdarzenie - możliwa, aczkolwiek niepożądana konsekwencja posiadania majątku, spowodowana przez zagrożenie. Konsekwencją taką może być zniszczenie majątku, uszkodzenie systemu zabezpieczenia, utrata poufności, integralności lub dostępności albo inne pośrednie szkody, np. straty finansowe, utrata klientów lub dobrego imienia firmy. Analiza zdarzeń umożliwia wyznaczenie punktu równowagi między stratami wynikającymi ze zdarzeń a kosztem przyjętych procedur zabezpieczeń, zmniejszających ryzyko zdarzenia.

Ryzyko - określa prawdopodobieństwo sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie elementu majątku, a zatem, pośrednią lub bezpośrednią szkodę dla przedsiębiorstwa. Ryzyko charakteryzują dwa czynniki: prawdopodobieństwo jego wystąpienia oraz miara zdarzenia. Wszelkie zmiany w układzie wzajemnych zależności między zagrożeniami, majątkiem, słabościami i wprowadzanymi mechanizmami zabezpieczeń mogą mieć duże znaczenie dla ryzyka. Określenie poziomu ryzyka dla każdej kategorii i grupy majątku przedsiębiorstwa, dostrzeżonych zagrożeń, słabości oraz wpływów jest **analizą ryzyka**.

Mechanizmy zabezpieczeń - do zadań mechanizmów zabezpieczeń należy: ochrona przed zagrożeniami, eliminowanie słabości, ograniczanie wpływu niepożądanych zdarzeń, wykrywanie niepożądanych zdarzeń i realizowanie wyjścia z kryzysowych sytuacji.

Ryzyko szczątkowe - mechanizmy zabezpieczeń mogą jedynie zmniejszać ryzyko. Całkowita eliminacja jest zwykle niemożliwa lub zbyt kosztowna. Powoduje to konieczność oszacowania ryzyka szczątkowego i określenia poziomu jego akceptacji.

Dynamiczny układ zależności między różnymi elementami systemu zabezpieczenia przedstawiono na rys. 1. Interpretację układu zależności można rozpocząć w punkcie ZAGROŻENIA (ZAGROŻENIA [zwiększają ryzyko] wykorzystując SŁABOŚCI narażając AKTYWA...], itd).



Rys. 1. Dynamiczne zależności między elementami zabezpieczenia informatycznego

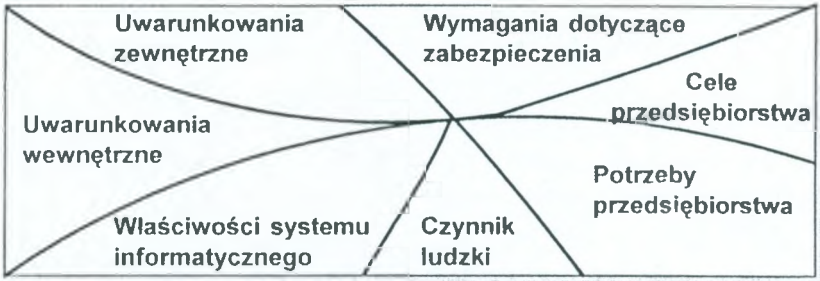
2. POLITYKA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO W PRZEDSIĘBIORSTWIE

Zabezpieczenie systemów informatycznych wymaga zdefiniowania **polityki** przedsiębiorstwa. Polityka zabezpieczenia systemu informatycznego jest dokumentem, w którym kierownictwo przedsiębiorstwa jasno określa cele (co ma być osiągnięte), strategie (jak osiągnąć cele) i działania (co należy zrobić), prowadzące do spełnienia kryteriów zdefiniowanych w pkt. 1.2.

Jeśli polityka zabezpieczenia będzie zdefiniowana poprawnie, a następnie realizowana, to spełni trzy poniżej wymienione zasadnicze zadania.

1. Zdefiniowanie **wymagań** w zakresie zabezpieczenia; bez polityki zabezpieczenia istnieje prawdopodobieństwo niejednoznaczności (sporu) stwierdzenia faktu naruszenia zabezpieczenia; brak definicji poufności dokumentów i danych może prowadzić do ujawnienia tajemnic przedsiębiorstwa, itp.
2. Określenie zakresu **odpowiedzialności**; polityka zabezpieczenia przypisuje odpowiednim osobom (działom, stanowiskom) ustalony poziom uprawnień w systemie informatycznym. Definiowanie zakresu odpowiedzialności umożliwia określenie własności danych oraz zasad ich użytkowania.
3. Określenie **zasad dostępu** do zasobów systemu informatycznego; polityka zabezpieczenia ma także wpływ na organizację działania przedsiębiorstwa - zasady prowadzenia rekrutacji pracowników, bezpieczeństwo i higienę pracy, kontrolę czasu pracy, zasady wprowadzania osób trzecich do przedsiębiorstwa, itp.

Tworzenie polityki zabezpieczenia jest procesem wieloetapowym. Wymaga wielostronnych uzgodnień i zależy od wielu czynników (rys. 2). Szczegółowe omówienie wszystkich czynników wykracza poza zakres niniejszego artykułu. Ich różnorakie działanie powoduje, że politykę zabezpieczenia należy definiować indywidualnie praktycznie dla każdego przedsiębiorstwa.



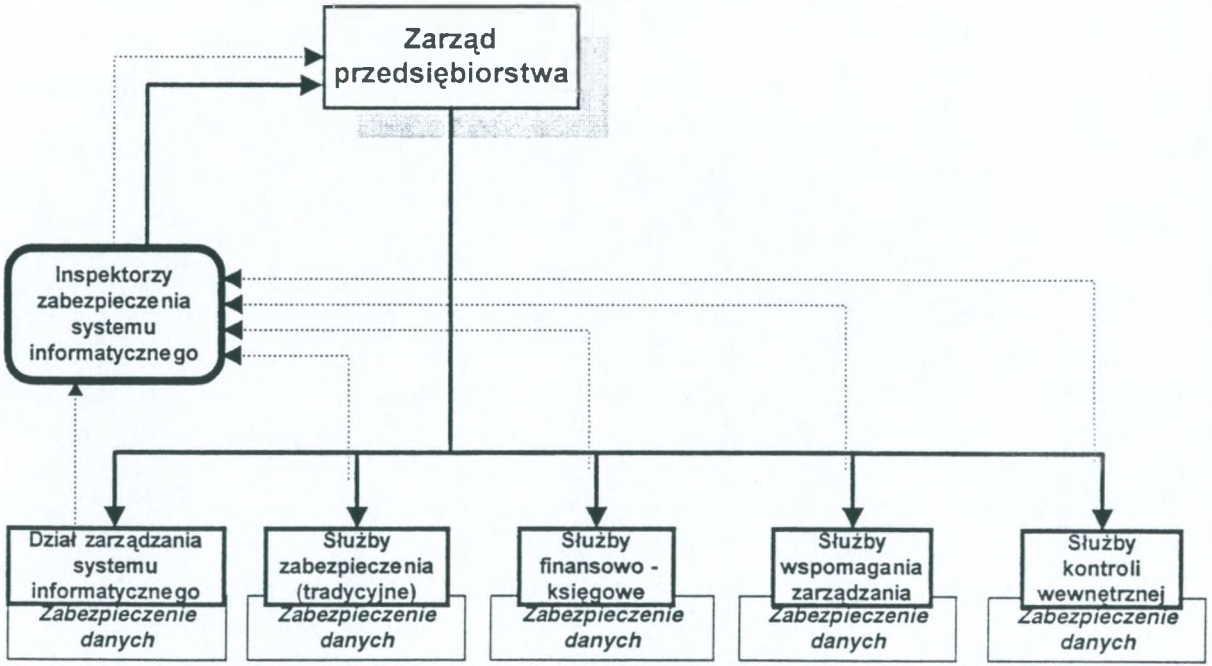
Rys. 2. Polityka zabezpieczeń jako wypadkowa działania różnorakich czynników

Wprowadzenie polityki zabezpieczenia systemu informatycznego w życie wymaga od kierownictwa zorganizowania w przedsiębiorstwie odpowiednich służb zabezpieczenia.

3. ORGANIZACJA SŁUŻB ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO W PRZEDSIĘBIORSTWIE

Za realizację polityki zabezpieczenia jest odpowiedzialne kierownictwo przedsiębiorstwa oraz służby (inspektorzy) zabezpieczenia. Zadaniem tych służb jest koordynacja działań i przepływu informacji między różnymi działami przedsiębiorstwa [2]. Przykładowo, funkcja zabezpieczenia danych może być rozproszona w wielu działach przedsiębiorstwa (rys. 3). Od umiejscowienia służb zabezpieczenia w strukturze organizacyjnej przedsiębiorstwa będzie zależał charakter przepływu informacji o stanie zabezpieczenia danych.

Należy podkreślić, że struktura organizacyjna przedsiębiorstwa z punktu widzenia zabezpieczenia systemu informatycznego oraz przepływ informacji o stanie zabezpieczenia informatycznego muszą być zdefiniowane w polityce zabezpieczenia.



Rys. 3. Przepływ informacji o zabezpieczeniu danych w przedsiębiorstwie

——— - zależności organizacyjne, ·····► - raporty o stanie zabezpieczenia danych

Organizacja służb zabezpieczenia, ich struktura, wielkość, umiejscowienie w strukturze organizacyjnej i decyzyjnej przedsiębiorstwa zależy od wielu czynników. Przykładowo, w dużych firmach może być organizowany odrębny dział zabezpieczenia, podległy bezpośrednio zarządowi, w mniejszych instytucjach funkcje inspektora pełni osoba (sekcja) włączona do działu informatycznego. Szczegółowe omówienie problemu organizacji służb zabezpieczenia wykracza poza zakres niniejszego opracowania. Obszerną analizę tych zagadnień można znaleźć, np. w [2].

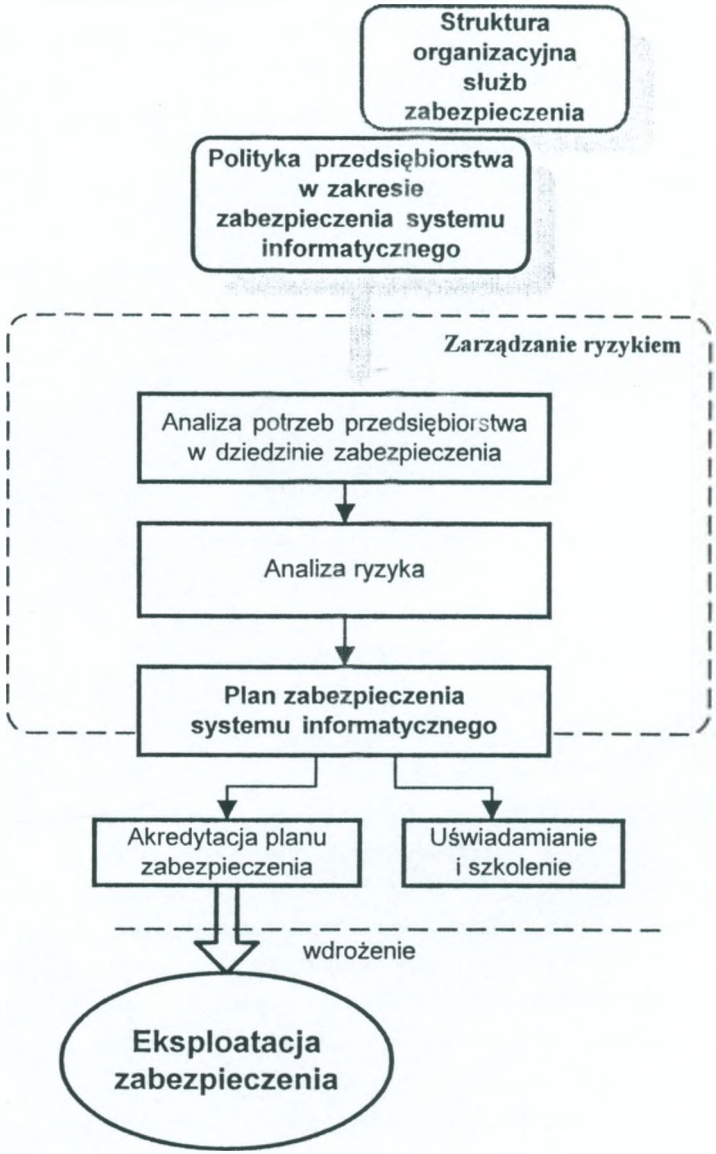
4. ZARZĄDZANIE ZABEZPIECZENIEM SYSTEMU INFORMATYCZNEGO

Jeśli system informatyczny decyduje o funkcjonowaniu nowoczesnego przedsiębiorstwa, to problem jego zabezpieczenia należy traktować jak jeden z zasadniczych elementów strategii działania firmy. Realizacja polityki zabezpieczenia systemu informatycznego wymaga zdefiniowania procesów zarządzania zabezpieczeniem.

Proces zarządzania zabezpieczeniem systemu informatycznego można podzielić na dwa zasadnicze podprocesy:

- podproces planowania zabezpieczenia (wraz z jego implementacją);
- podproces eksploatacji zabezpieczenia.

Rys. 4. Proces zarządzania zabezpieczeniem systemu informatycznego



Rys. 5. Proces planowania zabezpieczenia

Realizacja procesów planowania i eksploatacji zabezpieczenia musi być zgodna z określoną w przedsiębiorstwie polityką zabezpieczenia systemu informatycznego. Stwierdzenie niezgodności z polityką w którejś z faz zarządzania zabezpieczeniem powinno powodować uruchomienie mechanizmów planowania zabezpieczenia. Na rys. 4 przedstawiono zależności między podstawowymi procesami zarządzania zabezpieczeniem systemu informatycznego.

Na rys. 5 pokazano kolejne fazy procesu planowania zabezpieczenia systemu informatycznego.

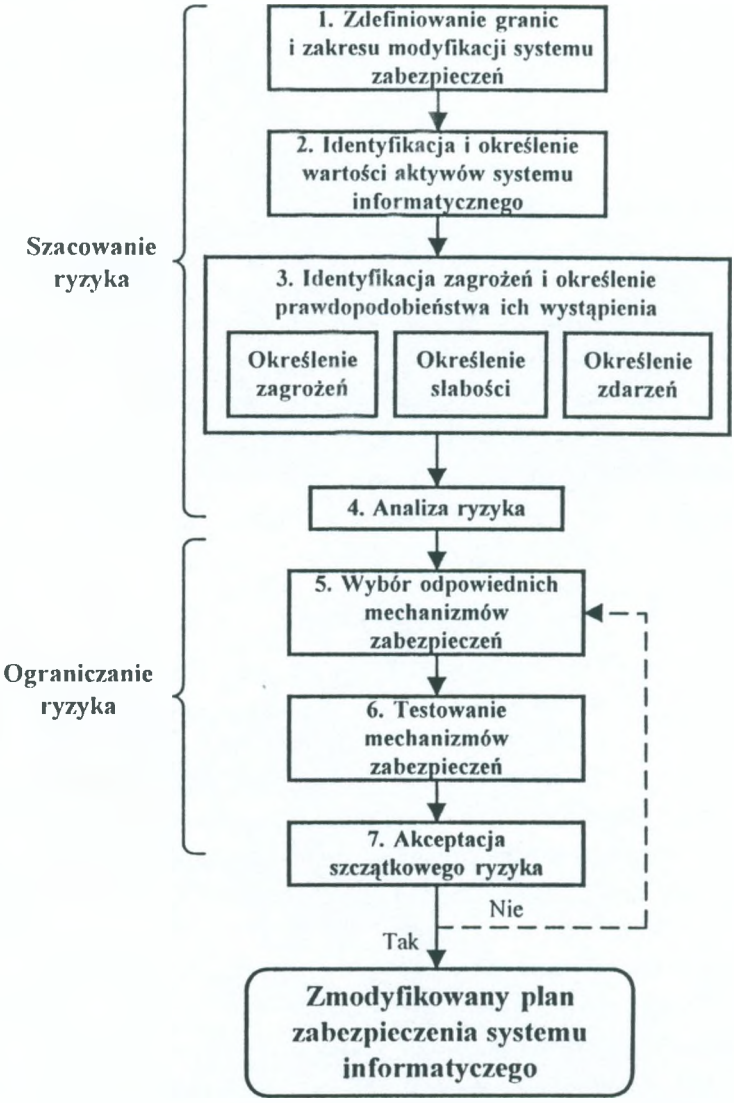
4.1. Planowanie zabezpieczenia

4.1.1. Zarządzanie ryzykiem

Proces zarządzania ryzykiem jest kluczowym elementem planowania zabezpieczenia. W wyniku przeprowadzenia działań, zgodnych z podanym na rys. 6 schematem, powstanie **plan zabezpieczenia systemu informatycznego przedsiębiorstwa.**

Wszelkie działania podejmowane w systemie informatycznym niosą w sobie ryzyko. Całościowa identyfikacja zagrożeń i określenie potrzeby ich kontrolowania lub akceptowania na wyznaczonym poziomie nosi nazwę **analizy ryzyka**. Rezultatem analizy ryzyka jest określenie poziomów ryzyka (**szacowanie ryzyka**) dla wszystkich aktywów systemu informatycznego. Całość przyjętych zabezpieczeń ma na celu **ograniczenie ryzyka** do akceptowalnego poziomu. Osiągnięcie stanu równowagi między zidentyfikowanymi mechanizmami zabezpieczeń a stosownymi działaniami podjętymi w celu ochrony systemu informatycznego przedsiębiorstwa jest procesem **zarządzania ryzykiem**.

Na rys. 6 zaprzentowano uproszczony proces zarządzania ryzykiem, złożony z siedmiu etapów, kolejno omówionych w dalszej części artykułu.



Rys. 6. Proces zarządzania ryzykiem

- **Szacowanie ryzyka**

Etap 1 - zdefiniowanie granic i zakresu modyfikacji systemu zabezpieczenia

Proces ten określa granice (jaka część systemu informatycznego) oraz zakres (jak bardzo szczegółowa modyfikacja) podjętego procesu zmiany systemu zabezpieczenia realizowanych w procesie zarządzania ryzykiem.

Określenie granic dokonywanych zmian pozwoli uniknąć niepotrzebnej pracy i wpłynie dodatnio na jakość analizy ryzyka. Zmiany mogą obejmować całość lub część systemu informatycznego. Należy zdefiniować, które z aktywów systemu informatycznego:

- majątek (sprzęt, oprogramowanie, dane...),
- czynnik ludzki (personel, użytkownicy, osoby z zewnątrz...),
- czynniki środowiskowe (budynki, instalacje...),
- funkcje (użytkowe, sterujące...)

będą zmieniane w danym procesie modyfikacji systemu zabezpieczenia.

Przy określaniu zakresu modyfikacji należy dokonać zróżnicowania stopnia szczegółowości zmian dla różnych obszarów systemów informatycznych. W przypadku małych systemów zmiany mogą obejmować całą strukturę, a stopień szczegółowości może być we wszystkich obszarach stały. W dużych systemach zmiany mogą koncentrować się w obszarach, w których działają określone aplikacje, znajduje się styk z sieciami zewnętrznymi itp.

Etap 2 - identyfikacja i określenie wartości aktywów systemu informatycznego

Określenie wartości aktywów systemu informatycznego umożliwi wskazanie obszarów, w których znajduje się najcenniejszy majątek, a co się z tym wiąże, w których system zabezpieczenia powinien być najskuteczniejszy. Określenie wartości musi obejmować straty, jakie

może ponieść przedsiębiorstwo w wyniku ujawnienia, modyfikacji zniszczenia lub braku dostępu do aktywów. Proces identyfikacji aktywów powinien polegać na utworzeniu list składników majątku i przyporządkowaniu każdej pozycji potencjalnego uszczerbku, jaki mogłoby ponieść przedsiębiorstwo w wyniku utraty dostępności, integralności i poufności. W procesie tym powinny brać udział odpowiednie służby przedsiębiorstwa, takie jak: dział finansowo-księgowy, ekonomiczny, planowania i informatyczny.

Szacowanie wartości aktywów, z punktu widzenia systemu zabezpieczenia, może być przeprowadzone różnymi metodami. Ogólnie, można je podzielić na ilościowe i jakościowe. Zgoda co do przyjętej metody jest koniecznym warunkiem określenia kryteriów analizy ryzyka. Opis metod pomiaru ryzyka, którego jednym z elementów jest określenie wartości, można znaleźć w [6]. Jedną z metod jakościowych może być 5-stopniowa skala wartościowania:

pomijalna - niska - średnia - wysoka - katastrofalna.

W metodzie ilościowej dla kolejnych poziomów skali można przyjąć szacunkowy koszt utraty dostępności, integralności lub poufności. Przykładowo:

< 1,000 $ = pomijalna,
< 10,000 $ = niska,
< 100,000 $ = średnia,
< 1,000,000 $ = wysoka,
> 1,000,000 $ = katastrofalna.

Należy podkreślić, że dla określenia wartości aktywów metoda ilościowa może okazać się niewystarczająca - niektóre ze składników majątku trudno oszacować (przykładowo, utrata dobrego imienia firmy). Należy zatem dopuścić niejednorodność metody określania wartości.

Efektem końcowym procesu powinna być lista aktywów systemu informatycznego z przyporządkowanymi wartościami wynikającymi z utraty poufności, integralności (modyfikacje), niedostępności

(np. zniszczenia). Formularz może przybrać następującą postać przedstawioną w tabl. 1.

Tablica 1

Zestawienie aktywów systemu informatycznego

Aktywa	Koszt utraty dostępności	Koszt utraty integralności	Koszt utraty poufności

Usunięcie z listy elementów, dla których wynikowa wartość mieści się w kategorii jakościowej "pomijalna" lub "niska" (lub ich odpowiedników ilościowych) umożliwi uzyskanie listy aktywów systemu informatycznego, które wymagają ochrony.

Etap 3 - identyfikacja zagrożeń, słabości i zdarzeń

Ten etap procesu zarządzania ryzykiem można podzielić na trzy fazy:

1) analizę zagrożeń,
2) analizę słabości (systemu informatycznego),
3) analizę zdarzeń (wpływu na system).

Efektem przeprowadzenia powyższych analiz jest jednoznaczne wskazanie tych działań osób trzecich, które mogą spowodować szkody w systemie informatycznym, określenie prawdopodobieństwa ich wystąpienia oraz wskazanie słabości systemu, których wykorzystanie może być podstawą tych działań.

1. Analiza zagrożeń

Analiza zagrożeń polega na gromadzeniu informacji o wszystkich możliwych zagrożeniach dla aktywów systemu informatycznego.

Ważne jest, aby nie zostało pominięte żadne istotne zagrożenie, bo może to wpłynąć na niewłaściwy dobór mechanizmów zabezpieczeń. Analiza zagrożeń obejmuje jakościowe oszacowanie poziomu prawdopodobieństwa ich wystąpienia (przyjmując np. 5-stopniową skalę wartościowania prawdopodobieństwa, analogiczną do omawianej w etapie 2 przykładowej skali lub prostszą, 3-stopniową skalę - - "wysokie", "średnie" i "niskie").

Każdy istotny element systemu informatycznego (zgodnie z używaną tu terminologią - aktywa systemu informatycznego) powinien być analizowany pod kątem zagrożeń, które mogą przyczynić się do jego uszkodzenia lub utraty. Szczególną uwagę należy zwrócić na identyfikację sposobów, jakimi dane zagrożenie może się objawić. Przykładowo, działaniami, które mogą prowadzić do uzyskania nieupoważnionego dostępu może być *playback* sesji rejestrowania użytkownika, złamanie hasła, dołączenie nieautoryzowanego wyposażenia do sieci LAN itp.

Dokumentem końcowym tej fazy jest zestawienie listy aktywów systemu informatycznego z potencjalnymi zagrożeniami prowadzącymi do naruszenia dostępności, integralności i poufności. Dołączenie listy potencjalnych szkód stanowi podstawę analizy zagrożeń. Dla każdego zidentyfikowanego zagrożenia należy utworzyć formularz podany w tabl. 2.

Tablica 2

Analiza wpływu danego zagrożenia NNN
na aktywy systemu informatycznego

Aktywa	Koszt utraty dostępności	Koszt utraty integralności	Koszt utraty poufności	Potencjalne szkody

2. Analiza słabości systemu informatycznego

Celem tego podetapu jest odpowiedź na pytanie: "Jak dalece poszczególne aktywa systemu informatycznego są narażone na utratę dostępności, integralności lub poufności"? Wynikiem analizy słabości jest dodatkowa charakterystyka aktywów.

Materiał wejściowy analizy stanowi lista słabości systemu. Istotnym jej elementem jest oszacowanie wagi poszczególnych słabości narażających system na utratę dostępności, integralności lub poufności. Skala oszacowania może obejmować trzy poziomy: "wysoki", "średni" i "niski".

Efektem analizy jest zestawienie aktywów systemu informatycznego, zagrożeń i stopni narażenia dostępności, integralności i poufności danego elementu określonych w przyjętej skali wartościowania (uzgadniając wcześniej tę skalę). Dla każdej, zidentyfikowanej słabości należy utworzyć formularz o postaci zaprezentowanejw tabl. 3.

Tablica 3

Analiza wpływu danej słabości MMM
na aktywa systemu informatycznego

Aktywa	Zagrożenie	Stopień narażenia dostępności	Stopień narażenia integralności	Stopień narażenia poufności

3. Analiza zdarzeń (wpływu na system)

Efektem przypadkowego lub rozmyślnego działania przynoszącego szkodę aktywom systemu informatycznego jest zdarzenie. Zdarzeniem może być np.:

- niedostępność lub zniszczenie majątku w postaci danych lub oprogramowania;

- nieupoważniona modyfikacja danych lub oprogramowania;
- nieupoważniony dostęp do danych lub oprogramowania, który powoduje straty wymierne (np. bezpośrednie lub pośrednie koszty) albo niewymierne (np. utratę dobrego imienia firmy, narażenie życia, naruszenie prywatności).

Dla każdej pary aktywa/zagrożenie należy określić potencjalne szkody, z uwzględnieniem związanych z nimi słabości systemu. Danymi wyjściowymi dla tej analizy są zestawienia otrzymane w dwóch poprzednich fazach. Analiza powinna wskazać te elementy systemu, które są najbardziej zagrożone, a zdarzenia z nimi związane powodują największe szkody.

Zestawienie będące połączeniem danych pochodzących z analizy zagrożeń i słabości z uszeregowaniem według typów zagrożeń powinno stanowić podstawę do dyskusji. W jej efekcie z listy zostaną usunięte te elementy, dla których zagrożenie nie ma istotnego wpływu na bezpieczeństwo systemu. Końcowe zestawienie otrzymane w tej fazie procesu stanowi punkt wyjścia do analizy ryzyka (tabl. 4).

Tablica 4

Zestawienie par zagrożeń i aktywów

Zagrożenie	Aktywa	Zdarzenie	Miara wpływu zdarzenia

Etap 4 - analiza ryzyka

Ryzyko stanowi miarę narażenia systemu informatycznego oraz związanego z nim przedsiębiorstwa na szkody. Ryzyko jest funkcją:

- prawdopodobieństwa realizacji zagrożenia na skutek świadomego lub nieświadomego działania;

- słabość systemu, która może być wykorzystana przez zagrożenie, powodując niepożądane zdarzenie;
- potencjalnego kosztu naprawy szkody powstałej w wyniku niepożądanego zdarzenia, tzn. szacowanej wartości aktywów systemu informatycznego.

Celem tego etapu procesu jest identyfikacja i oszacowanie ryzyka, na które jest narażony system informatyczny i jego składniki. W wyniku tej analizy jest możliwa identyfikacja i wybór odpowiednich mechanizmów zabezpieczeń.

Istnieje wiele sposobów pomiaru i poglądowego przedstawienia ryzyka [2,3]. W zależności od przyjętej metodyki, miara ryzyka może być ilościowa lub jakościowa, w układzie jedno- lub wielowymiarowym albo kombinacji tych form. Przykładowo, ryzyko może być mierzone wielkością strat wyrażoną w dolarach lub jakościowo, gdzie ryzyko jest wyznaczane przez dany poziom z przyjętej skali. Należy tu podkreślić, że przyjęta metoda pomiaru ryzyka powinna być zgodna ze stosowaną w poprzednich etapach metodyką szacowania (np. wartości składników majątku). W jednowymiarowej metodzie pomiaru rozważa się tylko niektóre elementy, np.:

ryzyko = wielkość strat x częstość strat.

W powyższym przykładzie można znormalizować poziomy ryzyka (wysokie, średnie i niskie). Taka sama skala obowiązuje dla obu składników powyższej kalkulacji. Przy przyjęciu tak uproszczonej skali, taki sam poziom ryzyka będzie efektem dwóch zagrożeń, z których pierwsze charakteryzuje wysokie prawdopodobieństwo wystąpienia i niski koszt, a drugie - niskie prawdopodobieństwo i wysoki koszt usuwania szkody. Kierownictwo przedsiębiorstwa musi zdecydować wtedy, która z tych sytuacji jest dla systemu bardziej krytyczna.

Poniżej zostanie zaprezentowany bardziej rozbudowany przykład szacowania ryzyka, wynikający z przyjętej w poprzednich etapach metodyki. Przedstawiono go w postaci dwuwymiarowej tabl. 5.

Tablica 5

Oszacowanie ryzyka dla wszystkich par zagrożenia/zdarzenia

Zagrożenie	Aktywa	Miara zdarzenia	Prawdo-podobieństwo	Ryzyko

Punktem wyjścia analizy ryzyka jest analiza zagrożeń, na podstawie której dokonano wyboru zagrożeń o znacznym potencjalnym wpływie na działanie systemu i przedsiębiorstwa. Dla tych zagrożeń szacowane jest prawdopodobieństwo wystąpienia. W zależności od natury danego zagrożenia, można skorzystać z różnorodnych źródeł informacji. Mogą to być np. statystyki takie, jak: liczba uszkodzeń łącza sieciowego w ciągu roku, parametr MTFB (średni czas między wystąpieniem dwóch kolejnych uszkodzeń) dla systemu itp. Podstawą szacowania prawdopodobieństwa jest jednak **analiza słabości**.

Oszacowane prawdopodobieństwo wystąpienia zagrożenia jest dodawane do listy wynikającej z analizy zdarzeń. Po wypełnieniu tablicy dla wszystkich zagrożeń należy określić ryzyko związane z każdym z nich (ostatnia kolumna tabl. 5).

Oszacowanie ryzyka opiera się na wartości aktywów systemu informatycznego oraz poziomach zagrożeń i słabości. Iloczyn miary wpływu (zdarzenia) i prawdopodobieństwo wystąpienia wskaże poziom ryzyka:

ryzyko = miara zdarzenia (szacowana wielkość szkód) x
x prawdopodobieństwo zdarzenia

Format dokumentu wyjściowego może być taki, jak w tabl. 5.

- **Ograniczanie ryzyka**

Etap 5 - wybór odpowiednich mechanizmów zabezpieczeń

Przyjęcie odpowiednich mechanizmów zabezpieczeń umożliwia sprowadzenie ryzyka do akceptowalnego poziomu. Przy wyborze mechanizmów zabezpieczeń należy brać pod uwagę różne czynniki. Do typowych ograniczeń w procesie wyboru należą poniżej wymienione czynniki.

- **Czynnik czasowy** - mechanizmy ochrony muszą być wdrożone i działać w akceptowalnym okresie. Takim okresem może być czas życia systemu lub akceptowalny termin, przed upływem którego dopuszcza się narażenie systemu na wskazane ryzyko.
- **Czynnik finansowy** - sumaryczny koszt mechanizmu nie powinien być większy niż wartość aktywów systemu informatycznego, które ma chronić. Nie zawsze należy jednak taką sytuację odrzucać. Wartość ryzyka jest mierzona nie tylko wartością składnika majątku i wielkością potencjalnej szkody, ale także prawdopodobieństwem wystąpienia zdarzenia. Jeden z tych elementów może być krytyczny i wtedy kosztowny mechanizm należy zastosować. Generalnie, ograniczeniem jest budżet przeznaczony na system zabezpieczenia.
- **Czynnik techniczny** - instalowanie dodatkowych zabezpieczeń w istniejącym systemie może być utrudnione z uwagi na ograniczenia techniczne. Ograniczenia te mogą skłonić do wyboru odpowiednich procedur programowych, a nie sprzętowych albo innych, pozasystemowych mechanizmów ochrony.
- **Czynnik socjologiczny** - socjologiczne ograniczenia zawierają w sobie specyfikę kraju, przedsiębiorstwa lub nawet działu tego przedsiębiorstwa. Nie można ich ignorować, ponieważ wdrożenie mechanizmów zabezpieczeń zależy od aktywnego uczestnictwa personelu. Brak akceptacji może spowodować, że mechanizmy nie będą efektywne.

- **Czynnik środowiskowy** - wpływ na wybór mechanizmów mogą mieć ograniczenia środowiskowe takie, jak: dostępna powierzchnia, ekstremalne warunki klimatyczne, ukształtowanie terenu.
- **Czynnik prawny** - wpływ na wybór mechanizmów zabezpieczeń może mieć stan prawodawstwa: zasady ochrony danych personalnych i kodeks karny dla przestępstw popełnianych za pomocą i na szkodę systemów informatycznych, a także inne uregulowania, np. przepisy przeciwpożarowe czy kodeks pracy.

Początkowa lista mechanizmów zabezpieczeń powinna powstać w powiązaniu ze zidentyfikowanymi zagrożeniami, dla których w poprzednim etapie przeprowadzono pomiar ryzyka. Dla nich należy wykonać test akceptowalności ryzyka. Proces wyboru i testu akceptowalności musi mieć charakter iteracyjny. W przypadku gdy poziom ryzyka po zastosowaniu mechanizmu jest zbyt wysoki, należy dokonać przeglądu alternatywnych mechanizmów. W przypadku niemożności pogodzenia poziomu ryzyka z listą dostępnych (z uwzględnieniem wyżej wymienionych ograniczeń) mechanizmów jego zmniejszania, przedsiębiorstwo musi dokonać rewizji wymagania dotyczącego poziomu akceptowalności ryzyka.

Wykorzystując zestawienie zagrożenie/słabość/ryzyko utworzone w poprzednim etapie należy wybrać te mechanizmy, które eliminują lub ograniczają słabości, a zatem zmniejszają ryzyko. Dla wybranych mechanizmów należy tak znormalizować koszt, aby móc porównać go z wartościami przyjętymi w poprzednich etapach i odnieść do wskaźnika ryzyka lub innych elementów tego zbiorczego parametru.

- **Etap 6 - implementacja i testowanie mechanizmów zabezpieczeń**

Implementacja i testowanie mechanizmów zabezpieczeń powinny przebiegać zgodnie z założonym planem. Celem tego etapu jest

uzyskanie pewności, że mechanizm został prawidłowo wdrożony, nie pozostaje w konflikcie z innymi funkcjami systemu informatycznego i mechanizmami zabezpieczeń oraz gwarantuje oczekiwany poziom zabezpieczenia.

Pracę należy rozpocząć od utworzenia planu wdrożenia mechanizmów zabezpieczeń. Plan powinien uwzględniać takie czynniki, jak: dostępne fundusze, plan szkoleń personelu itp. Zasadniczym elementem planu powinien być harmonogram testowania każdego mechanizmu. W harmonogramie powinno się przewidzieć testy wpływu i interakcji z innymi mechanizmami zabezpieczeń. Testy współdziałania powinny dać gwarancję braku konfliktu z innymi mechanizmami zabezpieczeń lub funkcjami sieci lokalnej. Jeśli mechanizm nie zakłada wspólnego działania z innymi mechanizmami, to w pierwszej fazie należy testować go niezależnie od innych mechanizmów. Dopiero po uzyskaniu pozytywnych wyników należy przeprowadzić testy interakcyjne. Trzeba też sporządzić szczegółową dokumentację uzyskanych wyników. Dokumentacja powinna zawierać instrukcję dla użytkowników, a także procedury bezpiecznego rozpowszechniania mechanizmu w sieci lokalnej i zmiany procedur zarządzania.

- **Etap 7 - akceptacja ryzyka szczątkowego - implementacja planu zabezpieczeń**

Po wdrożeniu wybranych mechanizmów zabezpieczeń pozostaje ryzyko szczątkowe. Dzieje się tak dlatego, że żaden mechanizm zabezpieczenia nie jest doskonały, a ponadto niektóre zagrożenia i słabości nie są objęte ochroną rozmyślnie (np. powodują małe ryzyko lub koszt wdrożenia jest zbyt wysoki).

Pierwszym krokiem w procesie akceptacji ryzyka jest identyfikacja wszystkich elementów ryzyka szczątkowego. W następnym kroku ryzyka szczątkowe należy podzielić na te, które są, zgodnie z polityką przedsiębiorstwa, "akceptowalne" i na te "nieakceptowalne".

Klasyfikacja ta powinna powstać na podstawie:

- obserwacji działania przedsiębiorstwa w warunkach praktycznych;

- szczególnej obserwacji relacji między aktywami systemu informatycznego, zagrożeniami i ryzykiem;
- rozpoznania zależności między elementami ryzyka: ich wzajemne relacje mają wpływ na efekt końcowy.

Z oczywistych względów nieakceptowalny poziom ryzyka nie może być tolerowany, należy zatem rozważyć wprowadzenie dodatkowych mechanizmów zabezpieczeń. W każdym z takich krytycznych przypadków decyzja, czy ryzyko osiągnęło "akceptowalny" poziom i może być poniesione, czy też koszt dodatkowych mechanizmów zabezpieczeń jest uzasadniony, stanowi decyzję ekonomiczną.

W efekcie procesu akceptacji powstaje grupa istniejących stale elementów ryzyka, które można formalnie zidentyfikować i całkowicie określić w odniesieniu do odpowiednich mechanizmów zabezpieczeń. Zostaje wyznaczony ostateczny poziom "akceptowalnego ryzyka". Jest on wynikiem decyzji zarządu przedsiębiorstwa.

W określonym czasie poziom ryzyka odpowiada wyrażonym potrzebom oraz wymaganiom określonym w danym przedsiębiorstwie. W perspektywie krótko- lub średnioterminowej przedsiębiorstwo musi zapewnić odpowiednie narzędzia i pracowników gwarantujące utrzymanie, bez większych odchyleń, wyznaczonego poziomu, co oznacza monitorowanie systemu praktycznie w czasie rzeczywistym.

4.1.2. Uświadomienie i edukacja

Powinien być opracowany program upowszechniania zasad systemu zabezpieczenia na wszystkich poziomach organizacji przedsiębiorstwa.

Celem programu edukacyjnego jest:

- uświadomienie pracownikom celów polityki zabezpieczeń prowadzonej w przedsiębiorstwie;
- całkowite zrozumienie wytycznych w zakresie zabezpieczenia systemu informatycznego;
- wpojenie pracownikom zasad odpowiedniego postępowania.

Szkolenie powinno obejmować następujące zagadnienia:

- przedstawienie podstawowych informacji z dziedziny zabezpieczenia;
- wyjaśnienie celów polityki zabezpieczenia, wytycznych, dyrektyw i podstawowych mechanizmów, co powinno doprowadzić do zrozumienia pojęć zagrożeń oraz mechanizmów przeciwdziałania zagrożeniom;
- przedstawienie klasyfikacji informacji;
- prezentację mechanizmów ograniczenia dostępu do urządzeń systemu informatycznego (uprawniony personel, zamki w drzwiach, identyfikatory, rejestratory wejść) oraz do danych (kontrola dostępu, prawa zapisu/odczytu);
- uświadomienie potrzeby rejestrowania naruszeń i prób dostępu;
- przedstawienie planu wdrożenia zabezpieczenia systemu informatycznego;
- przedstawienie procedur, zakresu odpowiedzialności i opisu poszczególnych zadań;
- omówienie czynności kontrolnych, samokontroli i audytu zewnętrznego;
- przedstawienie zagadnień związanych z zarządzaniem zmianami i instalacjami w obrębie systemu informatycznego.

Szkolenie w pierwszym rzędzie powinno objąć kierownictwo przedsiębiorstwa na wszystkich jego szczeblach organizacyjnych. Na kierownikach spoczywa odpowiedzialność za przeprowadzenie szkolenia podległych im pracowników. **Uświadomienie w zakresie zabezpieczenia musi prowadzić do zmiany zachowań użytkowników systemu informatycznego.**

4.1.3. Akredytacja

Akredytacja jest przyjęciem i nadaniem uprawnień do użytkowania planu zabezpieczeń zgodnego z założeniami polityki zabezpieczenia.

Akredytacja jest ważna w limitowanym przedziale czasowym i dla ściśle zdefiniowanego środowiska systemu informatycznego; każda jego zmiana wymaga rewizji akredytacji.

Proces akredytacji składa się z przeglądu dokumentacji i odbioru technicznego. Przegląd dokumentacji obejmuje sprawdzenie jej kompletności, wewnętrznej spójności i zgodności z innymi dokumentami. Odbiór techniczny opiera się na kontroli zgodności ze standardami i może być powierzony specjalizowanym instytucjom certyfikującym. Po przeprowadzeniu procesu akredytacji można przystąpić do eksploatacji planu zabezpieczenia.

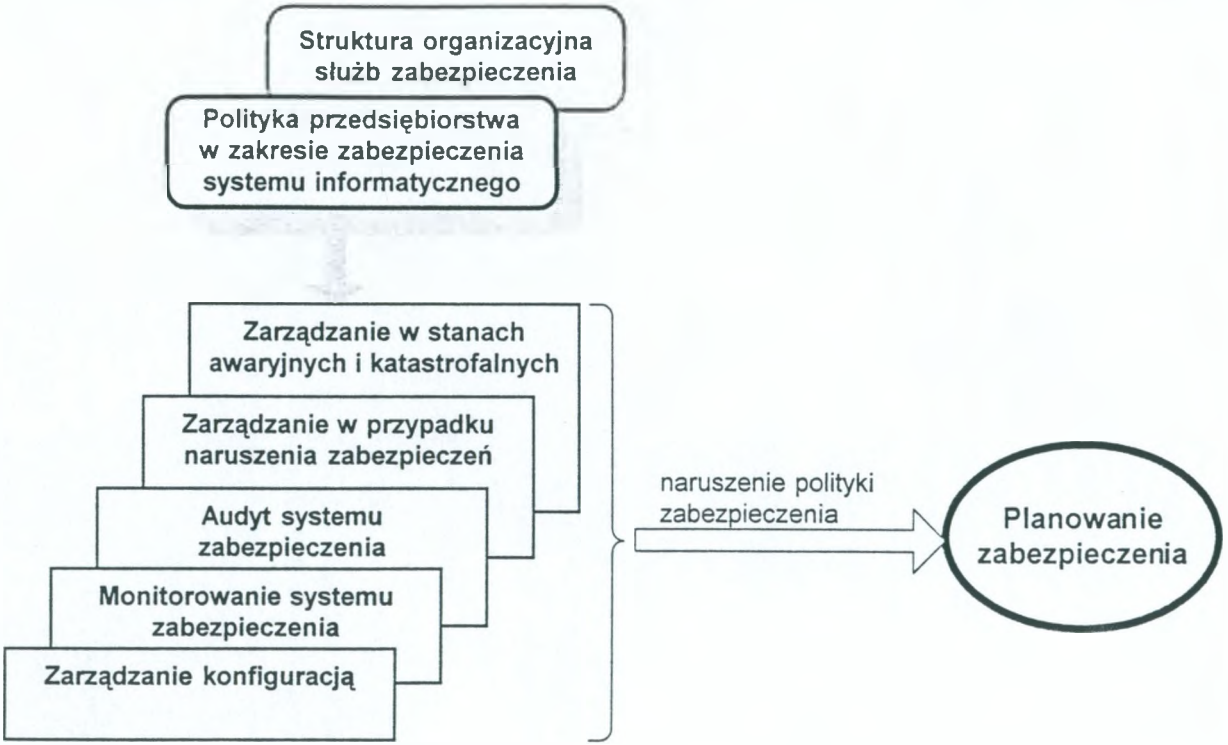
4.2. Eksploatacja zabezpieczenia

Ten proces zarządzania zabezpieczeniem jest zwykle pomijany w opracowaniach, ale pełni bardzo ważną rolę. Istniejące i wdrożone w efekcie modyfikacji planu mechanizmy zabezpieczeń wymagają utrzymania (przez utrzymanie rozumie się bieżącą obsługę systemu zgodną z wymaganiami producenta). Celem działań utrzymaniowych jest zapewnienie prawidłowego funkcjonowania systemu zabezpieczenia w czasie jego eksploatacji.

Procesy eksploatacji zabezpieczenia zilustrowano na rys. 7. W niniejszym artykule zostaną przedstawione cele, jakie poszczególne procesy eksploatacji zabezpieczenia powinny spełniać. Szczegółowe omówienie stosownych procedur realizujących procesy eksploatacji wykracza poza zakres tego artykułu.

4.2.1. Zarządzanie konfiguracją

Zarządzanie konfiguracją jest procesem śledzenia zmian zachodzących w systemie informatycznym. Głównym celem tego procesu jest zapewnienie, że wprowadzane zmiany nie zmniejszają efektyw-



Rys. 7. Proces eksploatacji zabezpieczenia

ności mechanizmów zabezpieczeń i ogólnego bezpieczeństwa przedsiębiorstwa. Jeśli jednak w systemie informatycznym muszą zostać dokonane zmiany, które mają wpływ na stan zabezpieczenia przedsiębiorstwa, to zarządzanie konfiguracją powinno uruchomić procesy szacowania poziomu zabezpieczenia i ewentualnej modyfikacji planu zabezpieczenia. Innym celem procesu zarządzania jest wprowadzanie stosownych zmian w procedurach wyjścia ze stanów awaryjnych i katastrofalnych.

4.2.2. Monitorowanie systemu zabezpieczenia

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

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

4.2.3. Audyt systemu zabezpieczenia

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

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

4.2.4. Procedury postępowania w przypadku naruszenia zabezpieczenia systemu informatycznego oraz w stanach awaryjnych i katastrofalnych

Naruszenie zabezpieczenia systemu informatycznego wymaga podjęcia właściwych kroków. Przedsiębiorstwa muszą mieć plan: wyjścia systemu ze stanu katastrofy i postępowania w przypadku naruszenia zabezpieczenia.

Zarządzanie w przypadku naruszenia zabezpieczenia jest procesem definiowania, opracowania i udokumentowania planu awaryjnego, uaktywnianego bezpośrednio po wykryciu zdarzenia, w wyniku którego system informatyczny nie może funkcjonować z normalną wydajnością. Plan ten służy ograniczaniu zasięgu konsekwencji poważnego naruszenia zabezpieczenia. Tylko przygotowany plan działań i wymaganych decyzji umożliwia szybką reakcję i pomaga ograniczyć zasięg szkód.

Procedura postępowania w sytuacjach naruszenia zabezpieczenia zawiera dwa elementy:

- procedury postępowania związane bezpośrednio z zaistniałym naruszeniem zabezpieczenia;
- tworzenie kopii bezpieczeństwa.

Procedura postępowania musi także obejmować prowadzenie chronologicznej dokumentacji wszystkich zdarzeń i podejmowanych działań. Zapis taki umożliwi wyśledzenie źródła zdarzenia, a ponadto pozwoli na uniknięcie podobnego zdarzenia w przyszłości. W ten sposób niepożądane zdarzenie spełni pozytywną rolę, zwiększając gotowość kierownictwa do przeznaczenia dodatkowych nakładów na zabezpieczenie.

Należy podkreślić znaczenie analizy *post mortem*, która powinna odpowiedzieć na następujące pytania:

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

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

Procedura wyjścia ze stanów awaryjnych lub katastrofalnych jest zespołem działań, które muszą zostać podjęte w celu odtworzenia zniszczonego w wyniku katastrofy systemu informatycznego i doprowadzenia go do stanu normalnej aktywności. Zarządzanie w stanach awarii lub katastrofy obejmuje: określenie kryteriów stanu awarii lub katastrofy, wprowadzenie planów awaryjnych, działania podjęte w celu przywrócenia poprzedniego stanu, opis podjętych działań.

Szczegółowe propozycje planu postępowania w przypadku naruszenia zabezpieczenia oraz planu wyjścia ze stanów awaryjnych i katastrofalnych wykraczają poza zakres niniejszego artykułu.

5. PODSUMOWANIE

W artykule zaprezentowano koncepcję realizacji polityki zabezpieczenia systemu informatycznego przedsiębiorstwa z uwzględnieniem procesów zarządzania zabezpieczeniem. W tej koncepcji wyeliminowano dwie podstawowe słabości dotychczasowego podejścia do problemów zabezpieczeń systemów informatycznych.

Po pierwsze, dotychczasowe koncepcje tworzenia polityki zabezpieczenia koncentrowały się głównie (jeśli nie wyłącznie) na aspektach technicznych. Wykorzystywały zautomatyzowane narzędzia zarządzania ryzykiem. W wielu przypadkach tak sformułowana polityka zabezpieczenia okazała się niewystarczająca. Zabezpieczanie systemów informatycznych bowiem jest problemem z dziedziny zarządzania, a nie techniki, zatem, w procesie tworzenia polityki zabezpieczenia systemu informatycznego, systemy eksperckie mogą być jedynie narzędziem pomocniczym.

Po drugie, dotychczasowe opracowania systemów zabezpieczeń koncentrowały się na fazie planowania zabezpieczenia, pomijając całkowicie fazę jego eksploatacji. Zarządzanie zabezpieczeniem systemu informatycznego jest procesem ciągłym, rzadko zdarza się, że mechanizmy zabezpieczeń są wprowadzane do systemu "od początku". Mechanizmy zabezpieczeń są modyfikowane, warunki działania systemu informatycznego ciągle zmieniają się, pojawiają się nowe zagrożenia. Wszystkie te czynniki muszą być monitorowane w procesach eksploatacji zabezpieczenia. Procesy eksploatacji powinny być zatem wyodrębnione i dobrze zdefiniowane, tak aby plan zabezpieczenia systemu informatycznego przedsiębiorstwa funkcjonował zgodnie z założeniami, przyjętymi w polityce zabezpieczenia.

Przedstawiona w niniejszym artykule koncepcja zarządzania zabezpieczeniem może stanowić podstawę formułowania polityki zabezpieczenia dla systemu informatycznego dowolnego przedsiębiorstwa.

Każdy proces zarządzania można opisać, uwzględniając trzy poziomy ogólności polityki zabezpieczenia: cele, strategie i działania. W przedstawionej koncepcji definicja procesów zarządzania zabezpieczeniem zawiera jedynie pierwszy poziom - cele; strategie i działania są ściśle związane indywidualnymi potrzebami przedsiębiorstwa, zatem mieszczą się w zakresie opracowań szczegółowych, co znajduje się poza tematyką niniejszego artykułu.

Opracowania szczegółowe, które opierając się na omówionej w niniejszym artykule koncepcji zarządzania zabezpieczeniem zawierają zdefiniowane dla poszczególnych procesów procedury działań, powstają obecnie w Instytucie Łączności (praca statutowa nr 073017). Opracowania dotyczą polityki zabezpieczenia systemów informatycznych IŁ i Ministerstwa Łączności.

WYKAZ LITERATURY

1. BS 7799: 1995 Code of Practice for Information Security Management. BSI, 1995.
2. Caeli W., Longley D., Shain M.: Information Security Handbook. Macmillan Press, Londyn 1994.
3. Gilbert I.: Guide for Selecting Automated Risk Analysis Tools. Special Publication 500-174. Gaithersburg, MD: National Institute for Standards and Technology, October 1989.
4. ISO/IEC TR 13335-1: Guidelines for the Management of IT Security. ISO/IEC Technical Report, 1996.
5. Krull A. R.: GSSP (Generally-Accepted System Security Principles): A Trip to Abilane? Computers & Security, Vol. 15, No. 7, 1996.
6. Ozier W.: Issues in Quantitive Versus Qualitative Risk Analysis. Data-Pro 6055, McGraw-Hill, Inc, March 1994.
7. PrPN-I-02000: Technika informatyczna - Zabezpieczenia w systemach informatycznych - Terminologia.

Эльжбета Андрукевич

УПРАВЛЕНИЕ БЕЗОПАСТНОСТЬЮ СИСТЕМЫ ИНФОРМАТИКИ

Р е з ю м е

Приводена модель управления безопастности системы информатики. Рассмотрено основные принципы политики безопастности систем информатики предприятия. Процесс управления безопастности систем подразделено на планирование и эксплуатацию безопастности. Подробно оговаривается элемент фазы планирования, процесс управления риском. Описываются процессы експлуатации безопастности к которым принадлежат: управление конфигурацией системы, мониторинг системы, процедуры принимания решений в случае обнаружения нарушения системы информатики, в состояниях аварии системы а также при стихийных бедствиях.

Elżbieta Andrukiewicz

IT SECURITY MANAGEMENT

S u m m a r y

The model of IT Security Management is presented. The basic principles for creating IT Security policy are discussed. The security management process is divided into two processes: planing and operation. The most important issue of planning process - risk management - is discussed in details. Several elements of the operation process: configuration management, security system monitoring, incident handling, contingency planning and disaster recovery are presented.

Elżbieta Andrukiewicz

LA GESTION DE PROTECTION D'UN SYSTEME INFORMATIQUE

Résumé

L'article présente un modèle de gestion des systèmes de protéction d'un système informatique. Les principes de base de création de la politique de protéction des systèmes informatiques des entreprises. Le procès de gestion est divisé en deux parties: de planification et d'exploitation des protéctions. Les plus important des élements d'une phose de planification - le procédé de gestion d'un risque - est décrit en détail. Les procédés d'exploitation des protéction c'est àdire: gestion de configuration, supérvision du système de protéction, procédures de conduites en cas de vialation d'une protection du système informatique ainsi que en cas des détérioration et des catastrophes sont décrits aussi.

Elżbieta Andrukiewicz

INFORMATIONSSYSTEM-SICHERUNGS-MANAGEMENT

Zusammenfassung

Das Modell des Informationssystem-Sicherungs-Managements wird präsentiert. Grundlagen für Schaffen der Politik der Informationssystem-Sicherung werden diskutiert. Der Sicherungsmanagement-Prozeß ist in zwei Prozesse geteilt. Diese sind: der Planung- und der Betriebsprozeß. Auf das wichtigste Element des Planungsprozesses: Riskmanagement wird näher eingegangen. Einige Elemente der Betriebsprozesses: Konfiguration-Management, Sicherheitssystem-Überwachung und Verfahrensgrundsätze im Fall des Sicherheitstörungs und in Ausfall- und Störungszustand werden betrachtet.

Arnold Kawecki

621.391.812.61.029.64

THE CORRELATION OF RAIN RATE WITH MICROWAVES ATTENUATION

The question of rain inhomogenity in space and time and also of the rain structure (the size and the shape of the drop) is presented. This inhomogenity makes difficult the measurement of rain parameters and the investigation of rain correlation with signal attenuation on microwave transmission links. On ground of this correlation the prediction models are elaborated, which are applied for evaluation of wave attenuation in microwave links. The models are based on rain-rate distribution. The results of the research in this subject, which have been obtained in the Institute of Telecommunications, are included in Final Report of COST 235 project. It has been shown experimentally low point rain-rate correlation with path attenuation and significant correlation with this attenuation of path averaged rain-rate, based on data from several rain gauges.

1. INTRODUCTION

The rain is cosidered as an obstacle on the path of propagating elmg wave. In case of wave frequencies above 10 GHz (3 cm wavelength) the energy of wave is absorbed and scattered significantly by rain drops. The resulting attenuation of the wave along the path depends on drops concentration, drops diameter distribution, vertical fall speed of the drops and on space profile of the rain along the path. The full description of the rain in space in time requiers great number of measuring instruments. For radiocommunication purposes the rain-rate, measured in point is the parameter of rain which is used in various applications, particularly rain-rate distribution is used for attenuation prediction in microwave links design [1].

2. THE STRUCTURE OF RAIN

The rain is an atmospheric phenomenon of great variability in space and time. The rain rate R, which depends on drop size distribution and drop fall speed, is a parameter which partly describes this phenomenon in selected point as follows:

$$R = 0.6 \cdot 10^{-3} \pi \int D^3 V(D) N(D) dD, \quad [mm/h] \tag{1}$$

where D is the drop diameter, V(D) is the fall speed of drop with diameter D and N(D) - the number of drops with this diameter in unit volume. The integration is performed over all drop sizes [2]. Air updraugts can reduce the fall speed of drops and consequently the rain rate R.

The drop size distribution is determined by fine structure of the rain . The process of drops creation begins in the cloud and continues during the fall. Small drops join with faster falling larger drops and the largest drops break-up. The drop size distribution changes in space during the fall and also depends on type of cloud.

The most simple drop-size distribution is that proposed by Marshall and Palmer (MP):

$$N(D) = N_o \exp(-\Lambda D) \qquad \Lambda = aR^b, \tag{2}$$

where N(D) is the number of drops of diameter D (mm) per unit volume (m^3) and per unit increment of drop diameter (mm) and N_o, a,b are constants. This exponential distribution overestimates the number of small drops [7].

A more general distribution is represented by a modified Γ-distribution:

$$N(D) = \Lambda_1 D^p \exp(-\Lambda_2 D^q), \tag{3}$$

where Λ_1 and Λ_2 may depend on R and p, q are constants [7]. This distribution is the product of two functions. It indicates that for $p > 1$ the number of drops has a maximum, which has been shown expe-

rimentally to lie between D = 0.5 and 1 mm. In convective rain (generated in cumulonimbus clouds), the maximum tends to be sharper.

Several drop size distributions have been applied. The MP distribution noted above is best applicable to widespread rain. Others apply the "thunderstorm" distribution (J-T) for convective rain and "drizzle" distribution (J-D) for very light rain but it has been found that the most representative of the average distribution is that of Laws and Parsons (LP) [7].

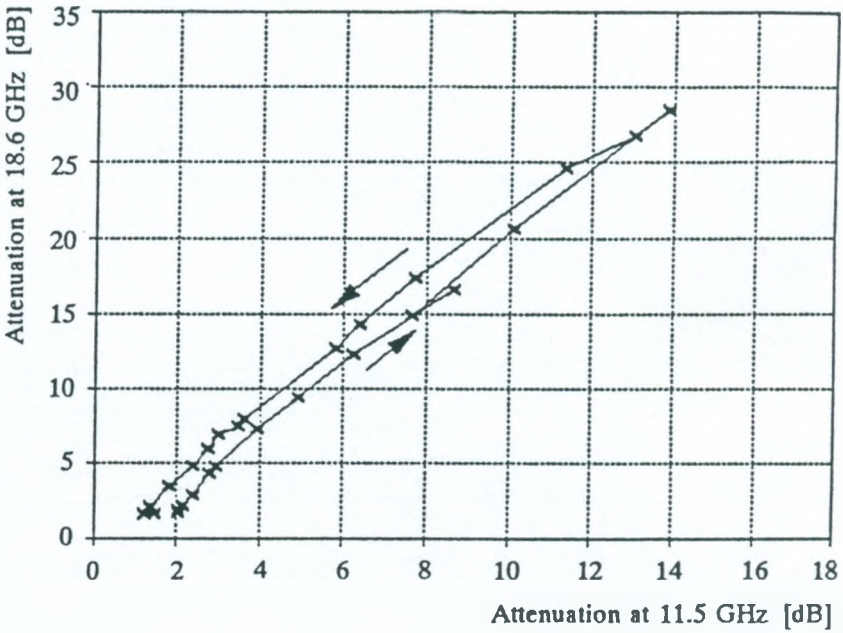


Fig. 1. Attenuation at 18.6 GHz versus attenuation at 11.5 GHz during the passage of the path by rain cell

The change of the drop size distribution in space can be noted during the storm when often at the beginning, at low rain rate, very large drops predominate.

The wave attnuation depends on the ratio of the wavelength and the drop diameter. The change of the drop-size distribution changes the attenuation at both frequencies but this change is not linear.

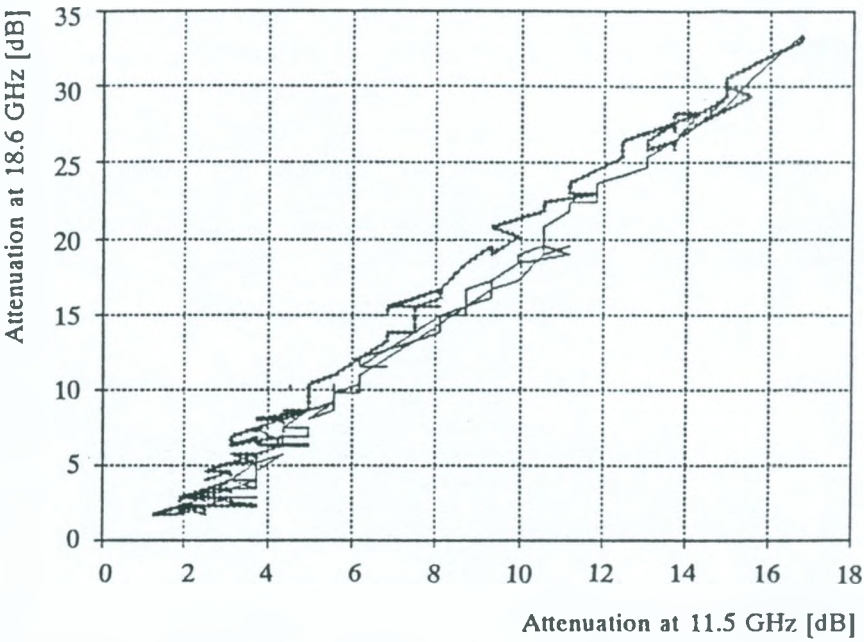


Fig. 2. Attenuation at 18.6 GHz versus attenuation at 11.5 GHz during the passage of the path by rain cell (4-sec samples)

A good illustration of the drop size distribution variation in space is the comparison of signal attenuation at 18.6 GHz and at 11.5 GHz during the passage of a rain column through the common propagation path, presented in fig. 1. The data in fig. 1 are ordered pairs of consecutive 1-minute signal samples, each of which is the average of 15 samples with 4 second repetition time [5, 6].

The lower part of the curve on fig. 1 shows the values of attenuation at 18.6 GHz versus corresponding values of attenuation at 11.5 GHz in period when the rain rate increases. The maximum

attenuation is attained at the 14-th minute of the passage of the rain column. The upper part of the curve relates to the period when the rain along the propagation path ceases with time.

Fig. 1 shows that despite the averaging of the samples in 1-minute period (which may correspond to several hundreds meters in space) the drop-size distributions in front and in the rear parts of the rain column are different. It is assumed that in this moderate shower the vertical air current did not affect the event significantly.

Fig. 2 shows the variation of attenuation during the same event but without smooting the samples in 1-minute period. In this figure, for clarity, the points are removed and the plot is divided in two parts: the solid line shows the increase of attenuation and the dotted line - the descrease.

3. THE INHOMOGENITY OF RAIN IN SPACE

The space inhomogenity of rain depends mainly on the type of rain. For simplicity, two types of rain are generally considered in radiocommunications: convective rain, (shower-type rain), created in vertical convection clouds and widespread rain, which originates in stratiform clouds. Convective rain in Europe is characterised by high rain rates reaching 100-200 mm/h in the core of the rain columns. The columns have diameters of 2-4 km and extend vertically to about 2 km above O°C isotherm. The other main feature of this type of rain is the great change in rain rate along the horizontal cros-section from very high values at the core to few mm/h at the edge of the column. In case of heavy storms the convective cells can create clusters of several close columns which extend more then 10 km.

The widespread rain in Europe is characterized by low rain rates, from 0.2 mm/h to several mm/h and can extend horizontally more than 100 - 1000 km. This rain originates from just under the 0°C isotherm in the melting snow zone. Rainfall rates exceed 10 mm/h

only very rarely and then with smaller horizontal extents. Such events are accompanied with heavy floods.

In widespread rain, the rainfall rate measured at a point, usually changes by about 30-60% on average within a few minutes and may cease for several minutes within 1 hour or two and then may continue again. These time variations are found to correspond with distance scales of about 2 km and 30-60 km while the average duration of rainfall rates exsceeding 1 mm/h has been found to be about 4 minutes [8]. This characteristic of widespread rain suggests that despite a general assumption about its small variability this type of rain is also variable in time.

The path attenuation A in dB at any moment depends on the rain rate profile R(l) along the path of length L, and is expressed by the integral, performed over the whole path:

$$A = k \int [R(l)]^{\alpha} \, dl, \quad [dB] \tag{4}$$

where k and α are frequency-dependent coefficients, calculated assuming a LP drop-size distribution, oblate spheroidal drop shape and a drop temperature 20°C [3].

In typical applications where only a single rain gauge is available, the path attenuation can be computed from the point rainfall rate with acceptable accuracy in cases where the path length is shorter then autocorrelation radius of the rain zone.

4. THE CORRELATION OF POINT RAIN-RATE WITH PATH ATTENUATION

Some insight into the problem of the inhomogenity of rain in space can be obtained from the investigations of the point rain rate correlation with path attenuation, which have been conducted in Miedzeszyn, Poland on a propagation path of 15.4 km length at frequencies 11.5 and 18.6 GHz [4, 5, 6]. Along the path 5 rain gau-

ges are situated as shown in fig. 3 where the rain rates in successive minutes at the five sites (Miedzeszyn, Julianow, Kepa, Powsin and Kierszek) during severe storm are presented. The path attenuation at 18.6 GHz is also shown (in black). In this example the line of columns passed the path in the same time. The duration of the storm was about 12 minutes after which a period of residual rain occurred, lasting about 70 minutes. Fig. 3 illustrates the rapid change in rain

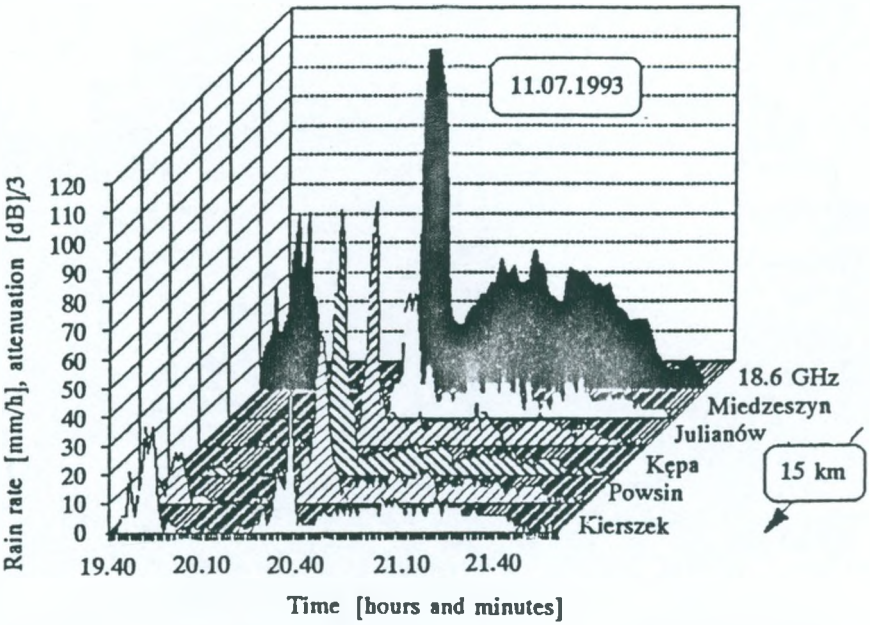


Fig. 3. Point rain-rates along 15 km path and path attenuation at 18.6 GHz during simultaneous passage of the path by line of intense rain cells

rate during the storm and also the variation in rain rate during the residual rain. The autocorrelation radius of rain rate is estimated to be about 2-3 km in the convective rain and about 2 km during the residual rain assuming that this radius in defined by autocorrelation level (1-1/e) = 0.63. The autocorrelation radius in the case of residual rain,

could be several times longer if it were defined at a lower level, for example at (1-2/e) = 0.26. The residual rain has features in common with intense widespread rain, although this originates from the "anvil" of cumulonimbus cloud. The anvil is the residual part of this cloud at the end of its life-time. Its horizontal spread is usually 50 x 30 km.

Fig. 4 shows another typical situation during the storm. The contribution of particular point rain rates can be compared with the path attenuation in each minute.

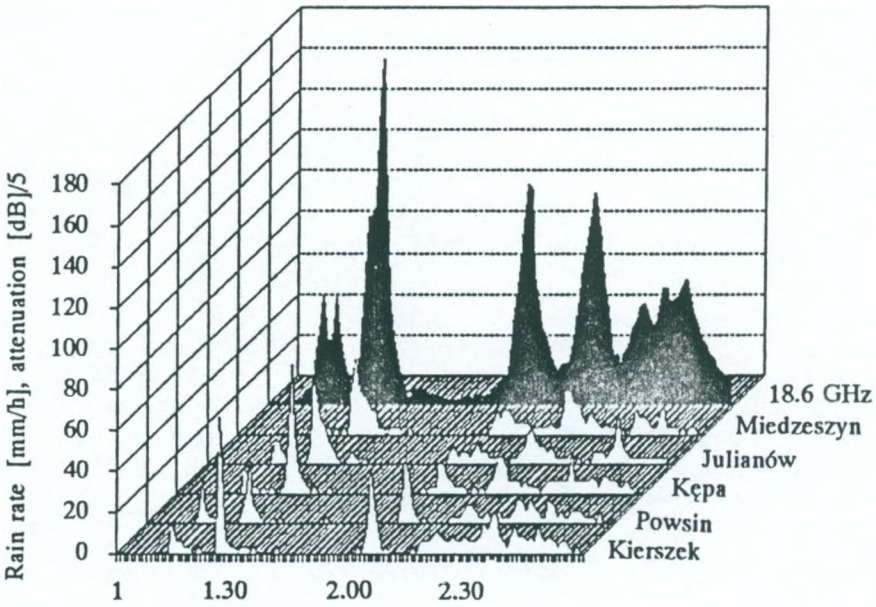


Fig. 4. Point rain rates in sites and path attenuation at 18.6 GHz during typical storm

The contribution of the point rain rates, measured at the different sites along the path to the resultant path attenuation can be evaluated from the correlation coefficient ρ^2.

Table 1 presents the values of ρ^2 found from correlating the rain rate at each site with the path attenuation for the event shown in fig. 3 for high rain rate part (Showers line) and for the residual rain. The case of single rain column, which passed Julianów, is also included. The values of ρ^2 averaged over 11 events with convective rain are also given (Showers-aver.). The last column gives the correlation coefficients for the path averaged rain rate with path attenuation [6].

Table 1

Events	Miedzeszyn	Julianów	Kępa	Powsin	Kierszek	Path-aver
Showers line	0.54	0.61	0.65	0.68	0.66	0.86
Single shower	0.06	0.85	0.01	0.36	0.11	0.86
Residual rain	0.10	0.13	0.67	0.32	0.47	0.72
Showers-aver	0.20	0.34	0.33	0.36	0.38	0.63

The correlation of path averaged rain rate with path attenuation is in most cases higher then that of point rain rate at any site, with the exception of cases, when a single rain cell passes only one rain gauge. On average, ρ^2 is about 0.35 for the sites along the path and is lowest (0.2) at the end of the path (Miedzeszyn). The value of ρ^2 is highest (0.63) for path averaged rain rate.

As shown in table 1, for residual rain the point rain rate correlation with path attenuation is only moderate due to rain rate variation of about 40% in average within 5 min intervals and a rather smoothly-varying path attenuation. It seems that this observation is also valid for intensive widespread rain.

5. CONCLUSIONS

In conclusion, the spatial inhmogenity of rain imposes the constraint on the minimum number of rain gauges along a path, for the proper measurement of the rain-rate profile as confirmed by the higher correlations between path averaged rain-rates with path attenuation, compared with those for a single point.

This is particularly important for short term propagation campaigns when long term rain-rate distribution can not be achieved with single point rain-rate measurements. The use of data collected from several rain gauges for determination of average rain-rate distribution assures higher credibility in this distribution [4]. The choice of the distance between the rain gauges depends on demanded accuracy and economical limitations.

REFERENCES

1. COST 235: Radiowave propagation effects on next generation fixed-services terrestrial telecommunications systems. Final Report, Part 3.3. The Effects of hydrometeors, Managementt Commmitee, European Commission, 1996.
2. Hall M.P.M.: Effects of the Troposphere on Radio Communication. IEE, Peter Peregrinus Ltd., Stevenage, UK and New York 1979.
3. ITU-Rec. P 838: Specific attenuation model for rain for use in prediction models. 1992 - CCIR Recommendations, Geneva 1992.
4. Kawecki A.: Considerations on Performance Evaluation of Attenuation Prediction Models. Proc. of 21 th Meeting of Olympus Propagation Experiment, Louvain-La-Neuve, 17-19 May 1994.
5. Kawecki A.: Correlation of rain rate with wave attenuation at 11.5 and 18.6 GHz and attenuation frequency scaling factor during rain passage. Proc. Seventh URSI Commision F Symposium on Wave Propagation and Remote Sensing, 20-24 November 1995, Ahmedabad, India.
6. Kawecki A.: Some Aspects of Attenuation due to Rain Prediction and Rain Rate Correlation with Attenuation. Prace Instytutu Łączności, No. 104, pp. 67-93, 1995 (in English).

7. Olsen R.L., Rogers D.V., Hodge D.B.: The aR^b Relation in Calculation of Rain Attenuation. IEEE Trans. on Ant. and Prop., Vol. AP-26, No. 2, March 1978.
8. Wickert S.: Fine scale structures in time and space of rainfall rate. National Defence Research Institute (FAO), Sweden, FAO Report C 20448-E2, 1982.

Arnold Kawecki

KORELACJA INTENSYWNOŚCI DESZCZU Z TŁUMIENIEM MIKROFAL

Streszczenie

Przedstawiono zagadnienie niejednorodności deszczu w przestrzeni i w czasie oraz niejednorodności struktury (rozmiarów i kształtu kropel). Ta niejednorodność stwarza trudności w mierzeniu parametrów deszczu i badaniu korelacji deszczu z tłumieniem sygnału na trasach mikrofalowych linii radiokomunikacyjnych. Na podstwie tej korelacji określa się modele prognostyczne, pozwalające przewidywać tłumienie fali na trasie na podstawie rozkładu intensywności deszczu. Wyniki uzyskane w tym zakresie w Instytucie Łączności dołączono do "Końcowego sprawozdania projektu COST 235". Pokazano eksperymentalnie niską korelację punktowej intensywności deszczu z tłumieniem na trasie i znaczną korelację z tym tłumieniem intensywności deszczu uśrednionej na trasie, uzykanej na podstawie danych z kilku deszczomierzy.

Арнольд Кавецки

КОРРЕЛЯЦИЯ ИНТЕНСИВНОСТИ ДОЖДЯ С ОСЛАБЛЕНИЕМ МИКРОВОЛН

Резюме

Представляется проблема неоднородности дождя в пространстве и во времени,а также неоднородности структуры

(размеров и формы капель). Эта неоднородность сотворяет затруднения измерения параметров дождя и исследования корреляции дождя с ослаблением сигнала на микроволновых радиолиниях. Основываясь на этой корреляции определяются модели для прогноза ослабления волн на трассе радиолинии используя распределение интенсивности дождя. Результаты полученные по этой проблеме в Институте Связи, включены в текст Сводного Отчета по проекте COST 235. Измерения указывают небольшую корреляцию интенсивноси дождя в точке с ослаблением волны по трассе и значительную корреляцию с этим ослаблением трассовой интенсивности дождя, определенной с помощью нескольких дождемеров установленных вдоль трассы.

Arnold Kawecki

LA CORRELATION ENTRE L'INTENSITE DE LA PLUIE ET L'AFFAIBLISSEMENT DES MICROONDES

Résumé

Cet article présente le problème de la hétérogéneité de la pluie dans l'éspace et dans le temps ainsi que celle de la structure (la dimension et la forme des gouttes). Il y a des difficultés en processus de la mesure dues aux paramètres et des essais de la corrélation entre la pluie et l'affaiblissement du signal sur les trajets des lignes de radiocommunication à microondes. En prenant en compte cette corrélation les modèles prognostiques sont définis qui permettent la prévision de l'affaiblissement de l'onde sur le trajets en utilisant les données de la distribution de l'intensité de la pluie. Les résultaten question obtenus à Institute de Télécommunication de Varsovie font partie du "Compte-rendu final du projet COST 235". Comme un exemple est donée une petite corrélation entre l'intensité ponctuelle de la pluie et l'affaiblissement sur le trajet des ondes et aussi une corrélation considérable entre cet affaiblissement de l'intensité de la pluie en valeur moyen du trajet obtenu sur la base de données de quelques pluviomètres.

Arnold Kawecki

KORRELATION ZWISCHEN DER REGENINTENSITÄT UND DER MIKROWELLENDÄMPFUNG

Z u s a m m e n s e t z u n g

Es werden Fragen der räumlichen und zeitlichen Inhomogenität des Regens wie auch strukturelle (Größe und Form des Tropfens) Inhomogenitäten behandelt. Diese Inhomogenität macht Messen der Regenparameter und Untersuchen der Korrelation zwischen Regen und Signaldämpfung längs der Funkstrecken schwierig. Auf Grund der Korrelation werden Prognosen-Modelle, die Vorhersagen der Wellendämpfung längs der Strecke auf Grund der Regenintensitätverteilung ermöglichen. Die im Institut für Fernmeldewesen gewonnenen Resultate der Forschungen sind zum "Finalbericht der COST 235-Projekt" hinzugesetzt worden. Experimentell gezeigt wurde niedrige Korrelation zwischen Punkt-Regenintensität und Dämpfung längs der Strecke und hohe Korrelation zwischen dieser Dämpfung und der längs der Strecke aus einigen Regenmesser gewonnen Daten gemittelten Regenintensität.

Arnold Kawecki

621.371:551.510.52:621.396.43

WAVE PROPAGATION ATTENUATION CHARACTERISTICS IN PRESENCE OF RAIN ON 15.4 KM PATH NEAR WARSAW AT 11.5 AND 18.6 GHZ

Summary of the results obtained after propagation measurements, performed in the years 1989-93 on the path of 15.4 km long at freq. 11.5 and 18.6 GHz, is presented. Only the attenuation events due to rain are taken into consideration. This summary includes the annual rain rate distributions and attenuation distributions at both frequencies. Q-factors for calculation of the worst-month distribution in each year are presented in case of rain-rate and attenuation at 11.5 and 18.6 GHz. In the paper the attenuation frequency scaling factors are computed in case of attenuation distribution scaling and in case of instantaneus attenuation scaling. This last factor is computed basing on 12 events, concurrent at both frequencies. At the end the results of attenuation (due to rain) prediction tests, based on ITU-R model and also on Crane and Stutzman-Yon models are presented.

1. INTRODUCTION

The characteristics of wave propagation on 15.4 km path related to 11.5 and 18.6 GHz frequency bands, based on data measured in period 1989-93, are presented. These characteristics concern the relation between point rain rate and path attenuation of the wave. In this research 5 rain gauges were arranged along the path and path averaged rain rate distribution is applied. Such distribution is more credible then single point distribution, particularly in case of short term campaignes [5, 6].

During this 5-years period a great variability of rain events occured. This variability is evident from fig. 1 ÷ 3 where annual rain rate and attenuation (due to rain) distributions are presented and from

fig. 4 ÷ 6 where conversion functions Q(p) for the transformation of annual distribution to worst-month distribution in each year are shown.

The year 1990 was particular because of low rain rates and 1991 - because of very high rain rates, which occured in 3 months. The year 1992 was particular because low rain rates were equally distributed in worm season including April and November and only single but very intensive event occurred in the summer. This resulted in very curved Q(p) conversion function. The year 1989 was very close to avereage for period 1989-93.

It is worth to mention that the arrangement of 5 rain gauges along the path did not assure that all significant attenuation events have corresponding rain events. Such case occurred in the year 1992 when single, strong precipitation column passed the path between the rain gauges, causing high attenuation without significant rain rate in any measuring point (compare fig. 4 with fig. 5).

Obtained empirical Q(p) conversion functions related to rain rate distribution and attenuation distributions at 11.5 and 18.6 GHz distributions are presented togather in fig. 7 with ITU-R model for comparison.

Fig. 8 presents empirical attenuation distribution frequency scaling factor compared with the ITU-R model suitable for this case [8]. The considerable discrepancy between the model and experimental data at low attenuation levels results from inadequate dense signal quantisation at 11.5 GHz. which increased assessed null level during data processing.

The scaling factor function for instantaneous attenuation scaling was obtained from the set of 12 concurrent attenuation events at both frequencies which do not exceed the linear interval of receiver characteristic (fig. 9).

The relation of attenuation at 18.6 GHz versus attenuation at 11.5 GHz during the passage of the rain column through the path,

shown in fig. 10, reveals some hysteresis effect, caused by the change of rain drop size distribution during this passage [9].

In frames of the research the test of models for attenuation (due to rain) prediction was performed. ITU-R model as well Stutzman-Yon and Crane models were examined. Satysfying accurate for attenuation distribution assessments at both frequencies were two last models as shown in fig. 11 and 12.

2. RAIN RATE DISTRIBUTIONS

The rain rate was measured in 5 sites along the propagation path and average rain rate distribution represents this phenomenon. Rain gauges were of tipping-bucket type. One tip/min corresponds to rain rate of 2.8 mm/h.

Rain rates below this value till 0.28 mm/h were computed with application of program, which averaged single tips in the gaps shorter then 10 min. Longer gaps were considered as the breaks between the rain events.

Distant rain gauges were inoperative during cold months (3 -5 months). Local rain gauge in Miedzeszyn operated continuously and statistical reperesentation for cold months was obtained for period 1989-93. The lacking distributions for distant rain gauges were completed assuming that 5-years statistical reperesentation of these months in Miedzeszyn can be applied for completion of distant rain gauges statistics.

Rain rate distributions, annual and averaged for period 1989-93, are presented in fig. 1. The rain rate data are presented also in tables togather with attenuation distributions. The data averaged in period 1989-93 are given in tables 1, 2. Annual data are given in Appendix. The characteristics for period 1985-95 for single point - Miedzeszyn are presented in [7] .

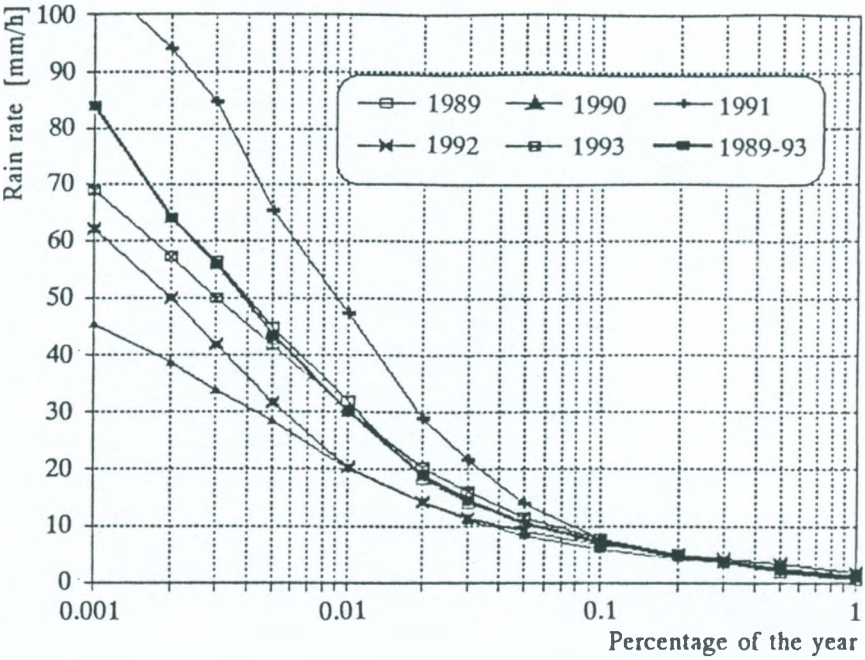


Fig. 1. Annual rain rate distributions in the years 1989-93 and average distribution

3. ATTENUATION DUE TO RAIN DISTRIBUTIONS

Statistics do not include the events with melting snow. Annual and averaged in period 1989-93 attenuation distributions at 11.5 and 18.6 GHz are presented in fig. 2 and 3. Table 1 presents the distributions related to period 1989-93 whereas annual distributions are given in Appendix.

Having in mind frequency scaling factor of attenuation distributions (see par. 5), which for frequencies 18,6 and 11.5 GHz is 2.32 at p = 0.01%, one can note that mutual situation of annual attenuation distributions in fig. 3 at 18.6 GHz corresponds with mutual situation of attenuation distributions at 11.5 GHz (fig. 2) in attenuation interval from 0 to about 20 dB.

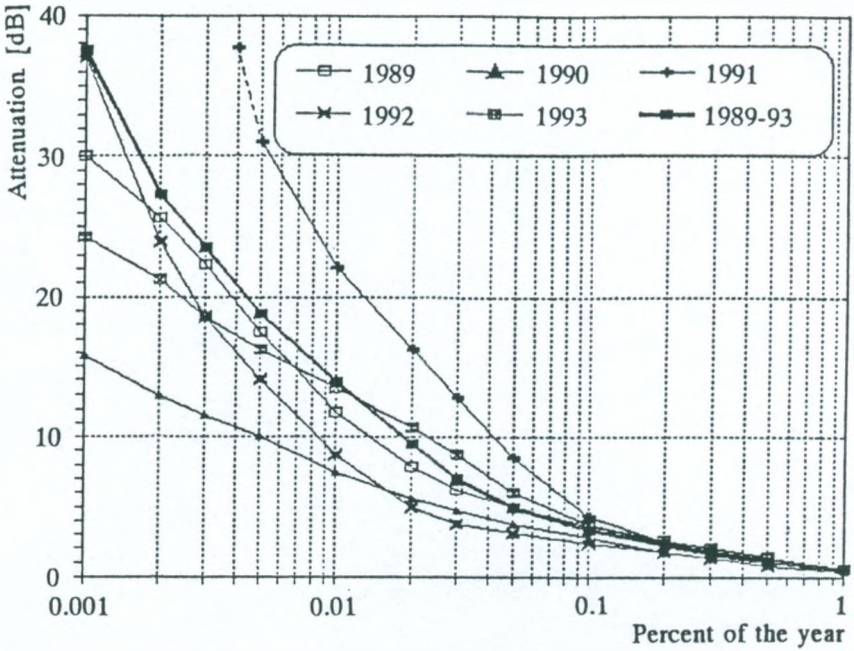


Fig. 2. Annual attenuation distribution in the years 1989-93 at 11.5 GHz and average distribution

Table 1

Attenuation distributions at 11.5 and 18.6 GHz and rain rate distribution for 1989-93

Percentage of time	0.001	0.002	0.003	0.005	0.01	0.02	0.03
Att. at 11.5 GHz [dB]	37.5	27.3	23.49	18.77	13.86	9.43	7.07
Att. at 18.6 GHz [dB]	-	-	-	42.68	32.25	21.85	16.63
Rain rate [mm/h]	84.12	63.96	55.96	43.66	29.95	19.06	14.53
Percentage of time	0.05	0.1	0.2	0.3	0.5	1	2
Att. at 11.5 GHz [dB]	4.99	3.31	2.23	1.7	1.08	-	-
Att. at 18.6 GHz [dB]	11.97	8.04	5.08	3.72	2.26	0.67	
Rain rate [mm/h]	10.51	7.12	4.87	3.82	2.55	1.19	0.39

Also rain rate distributions (fig. 1) correspond with attenuation distributions with exception of the year 1992 when heavy rain passed the path between rain gauges.

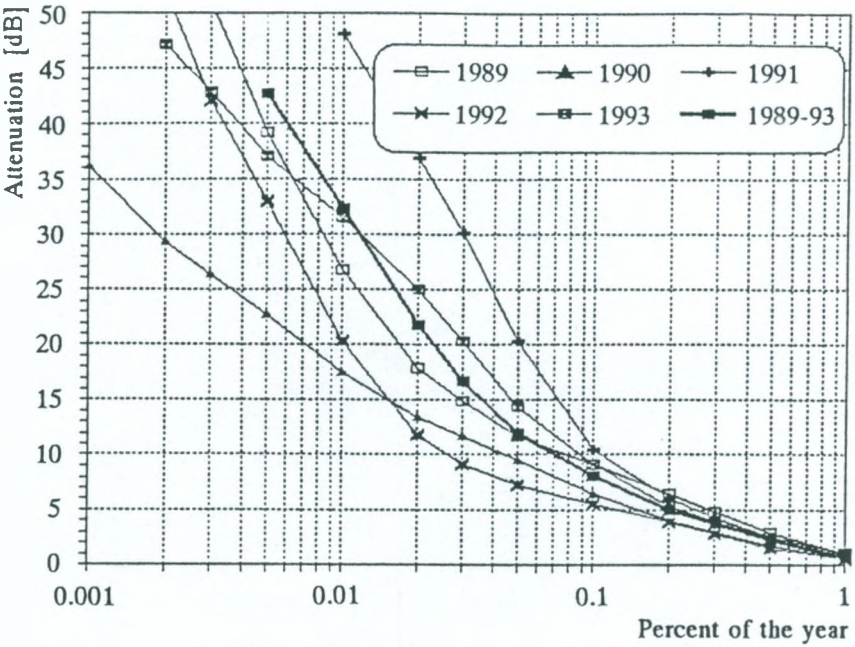


Fig. 3. Annual attenuation distributions in the years 1989-93 at 18.6 GHz and average distribution

4. THE ASSESSMENT OF THE Q-FACTOR FOR WORST-MONTH

ITU-R model Q(p) for conversion of annual distribution to worst-month distribution was applied where p - percentage of the year [4]:

The unknown parameters Q_1 and β were evaluated for each year and for average year applying nonlinear regression analysis. The results for rain rate are presented in table 2 and in fig. 4. The para-

meters related to attenuation at 11.5 and 18.6 GHz are shown in table 3 whereas Q(p) graphs are presented in fig. 5 and 6.

$$Q(p) = \begin{cases} Q_1 p^{-\beta} & \text{for} \quad \left(\frac{Q_1}{12}\right)^{\frac{1}{\beta}} < p < 3\% \\ 12 & \text{for} \quad p < \left(\frac{Q_1}{12}\right)^{\frac{1}{\beta}} \end{cases}$$

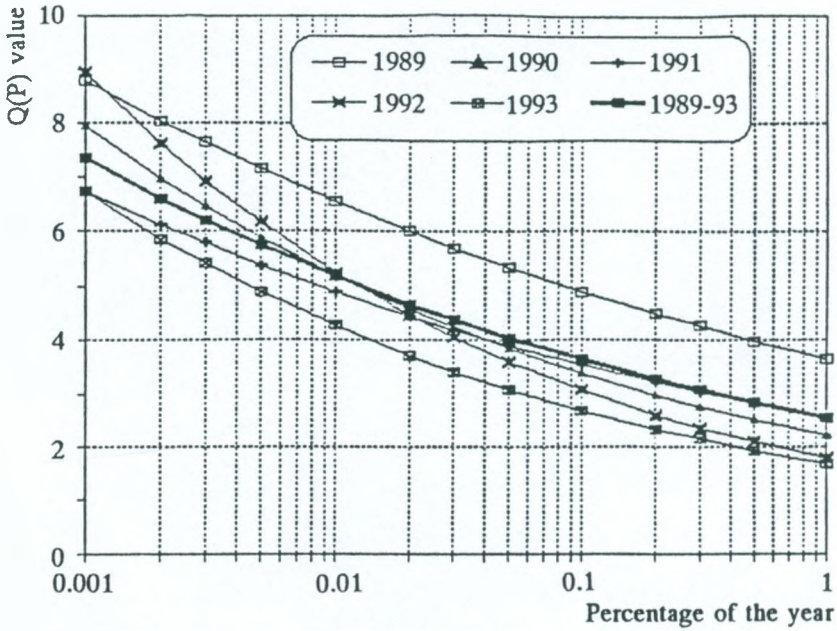


Fig. 4. Q(p) graphs for rain rate distributions in the years 1989-93

Obtained for period 1989-93 Q(p) experimental expressions are compared with ITU-R expression with parameters $Q_1 = 2.85$ and

β = 0.13 in fig. 7. These are very close to parameters obtained for rain rate distributions. The differences between parameters at 11.5 and 18.6 GHz can result as the consequence of limited attenuation interval at 18.6 GHz (0-47 dB).

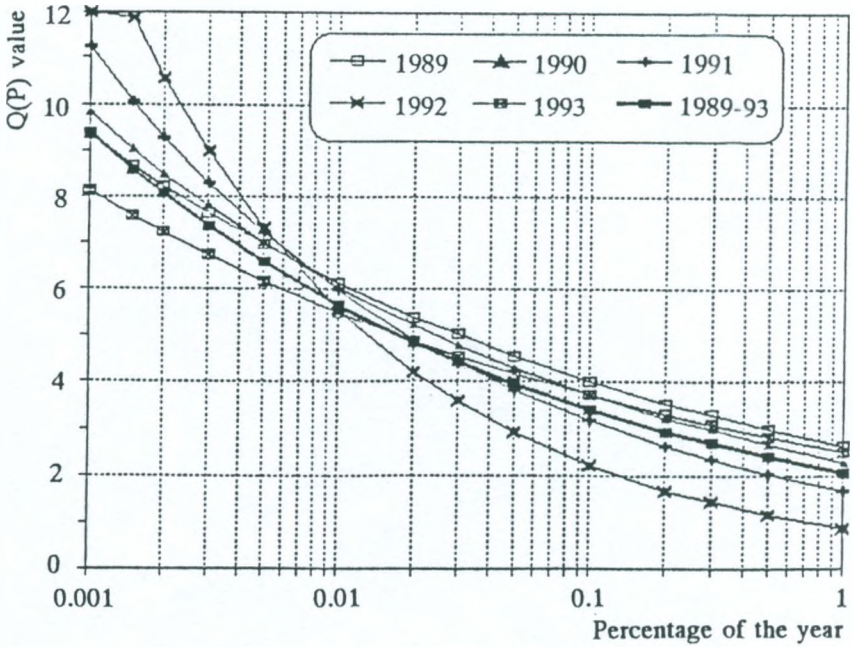


Fig. 5. Q(p) graphs for attenuations distributions at 11.5 GHz in 1989-93

Table 2

Rain rate distribution conversion factors Q_1 and β in the years 1989-93

1989		1990		1991		1992		1993		1989-93	
Q_1	3.65	Q_1	2.21	Q_1	2.56	Q_1	1.78	Q_1	1.69	Q_1	2.55
β	0.127	β	0.185	β	0.14	β	0.233	β	0.2	β	0.153

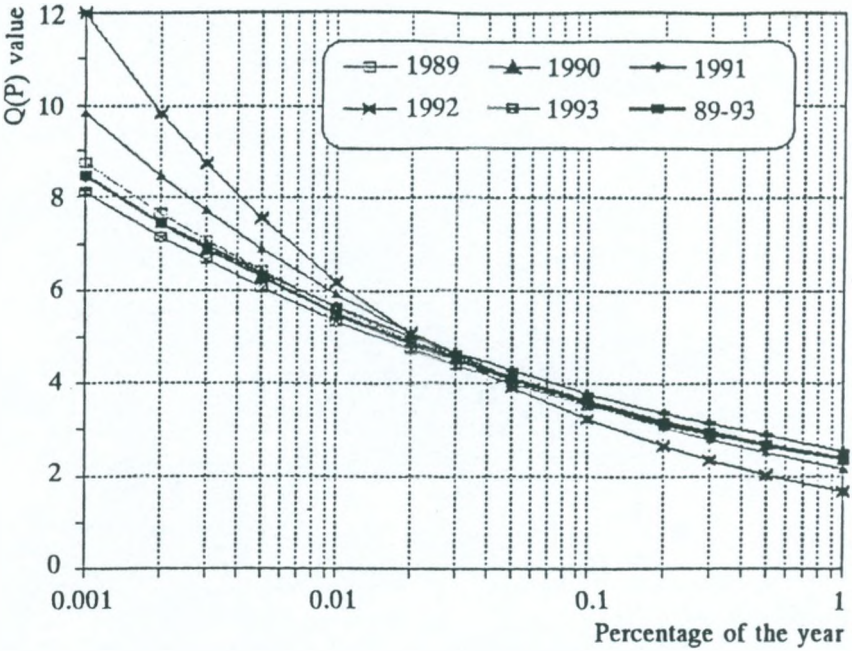


Fig. 6. Q(p) graphs for attenuation distributions at 18.6 GHz in 1989-93

Table 3

Conversion factors parameters Q_1 and β at 11.5 and 18.6 GHz

Frequency	Parameter	1989	1990	1991	1992	1993	1989-93
11.5 GHz	Q_1	2.64	2.30	1.68	0.88	2.57	2.05
	β	0.183	0.21	0.275	0.4	0.17	0.22
18.6 GHz	Q_1	2.35	2.15	2.55	1.67	2.34	2.356
	β	0.19	0.22	0.173	0.285	0.18	0.185

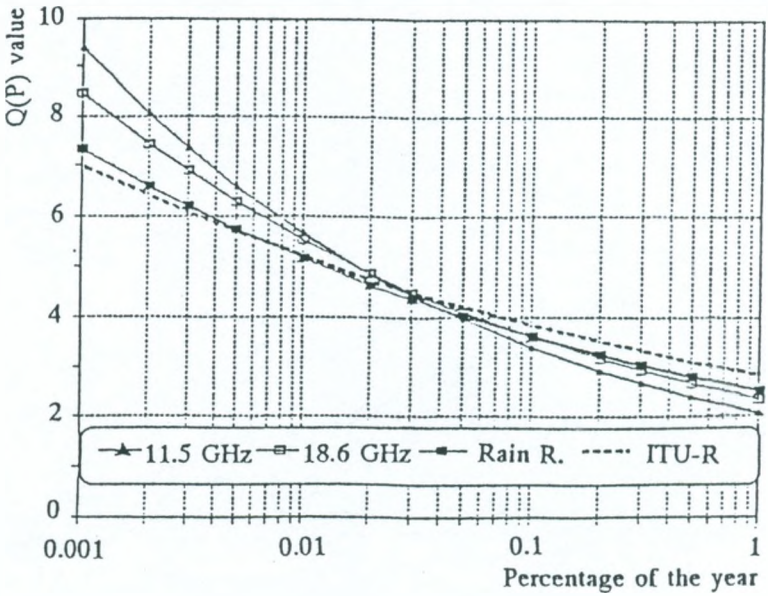


Fig. 7. Q(p) graphs comparison with ITU-R model

5. SCALING OF ATTENUATION DISTRIBUTION

Empirical scaling factors were compared with the model:

$$H(\Phi_1, \Phi_2, A_1) = 1.12 \cdot 10^{-3} (\Phi_2 / \Phi_1)^{0.5} (\Phi_1 A_1)^{0.55}$$

recomended by ITU-R [2], where $\Phi = f^2 / (1+10^{-4} f^2)$.

In this model for frequencies $f = f_1 = 11.5$ GHz and $f = f_2 = 18.6$ GHz the values $\Phi = \Phi_1 = 130.52$ and $\Phi = \Phi_2 = 334.4$. Thus $(\Phi_2 / \Phi_1)^{0.5} = 1.6$ and the model for our case has the form

$$H(\Phi_1, A_1) = 0.0018(\Phi_1 A_1)^{0.55},$$

where A_1 - the attenuation at 11.5 GHz exceeded in percentage p. The equiprobable value of A_2 is:

$$A_2 = A_1 (\Phi_2 / \Phi_1)^{1-H(\Phi 1, A1)} .$$

The empirical scaling factors were computed from attenuation distributions, averaged in period 1989-93, obtained at both frequencies (fig. 8). For $p < 0.005\%$ experimental scaling factor could not be found, because of limited signal measuring interval of 18.6 GHz receiver. The discrepancy between the model and the experiment for $p > 0.1\%$ results from the overestimation of low attenuation values at 11.5 GHz.

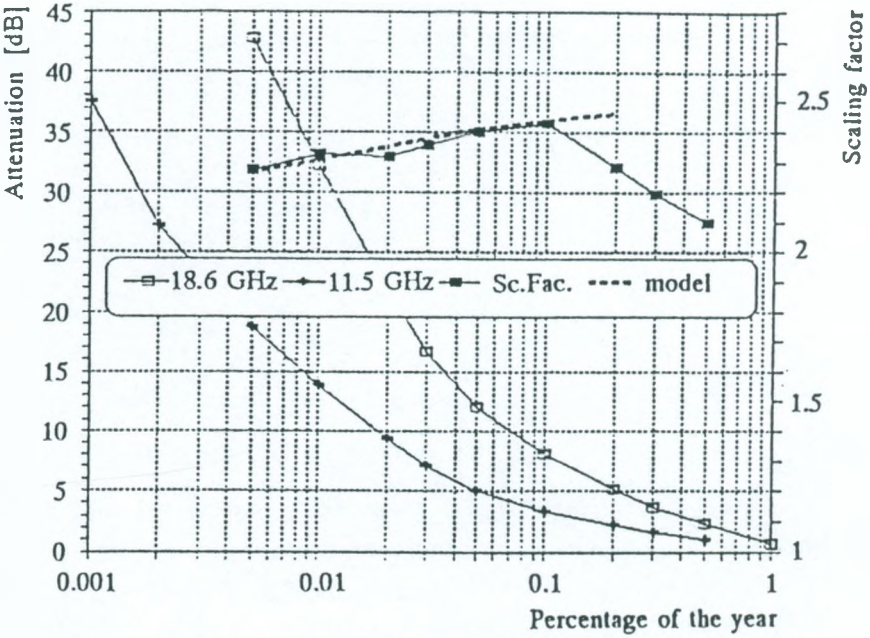


Fig. 8. Scaling factor 18.6/11.5 GHz of attenuation distributions

6. SCALING OF INSTANEOUS ATTENUATION VALUES

The scaling factor for instantaneous attenuation values was obtained from the set of concurrent events at both frequencies which

didn't exceed the linear interval of receiver characteristic. The attenuated signal samples (1 per 4 sec) were averaged in 1-min intervaland then linear regression function was computed (fig. 9). The number of 1-min samples pairs was 207. The linear regression function of attenuation at 18.6 GHz (A_2) in terms of attenuation at 11.5 GHz (A_1) is:

$$A_2 = y_o + a_1 A_1 .$$

The computation showed that $y_o = 0.23$ dB therefore it was assumed that both variables are proportional. In such case $a_1 = 2.36$. At revers regression the coefficient is almost equal $1/a_1 = 0.424$. The result is accurate because the correlation coefficient, ρ squared is 0.987 and standard error of a_1 assessment is 0.011.

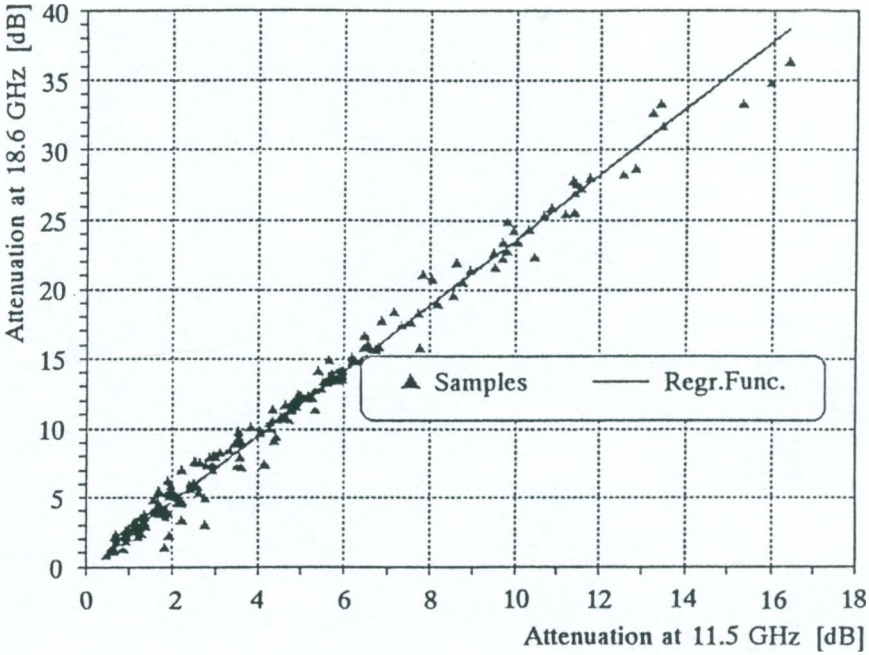


Fig. 9. Regression of attenuation at 18.6 GHz in terms of attenuation at 11.5 GHz

This value (a_1 = 2.36) corresponds with distributions scaling factor value at p = 0.01%. The dispersion of A_2 / A_1 ratio during the event depends mainly on changes of rain drops size distribution during the passage of the rain through the path.

The resulting hysteresis effect of this ratio in case of one event is presented in fig. 10.

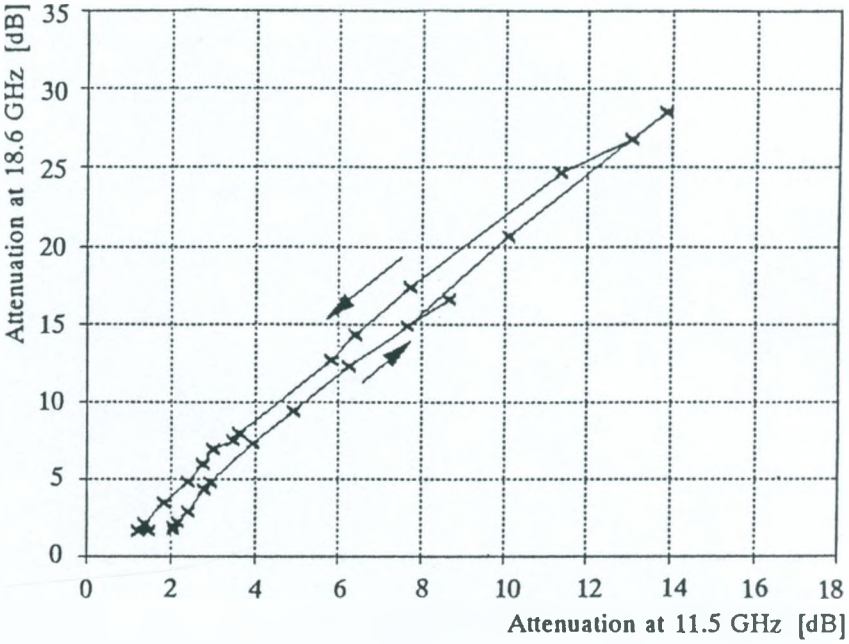


Fig. 10. Attenuation at 18.6 GHz versus attenuation at 11.5 GHz during passage of rain cell through the path

7. THE CHOICE OF ATTENUATION PREDICTION MODEL

Having attenuation distributions at 11.5 and 18.6 GHz averaged in 5-years period and credible rain rate distribution, averaged in the same period, the attenuation prediction models could be examined.

The ITU-R model and models of Crane (CRA) and of Stutzman-Yon (STYO) were selected, [1,2,8]. This last one is provided to Earth-space paths but assuming that the elevation angle is null, this simple and adaptive model can be applied to terrestrial paths. In this model the γ parameter, which gives the best fit to experimental data sets is 1/14 but in case of both terrestrial paths, situated in central Europe, the best value of this parameter is 1/33.

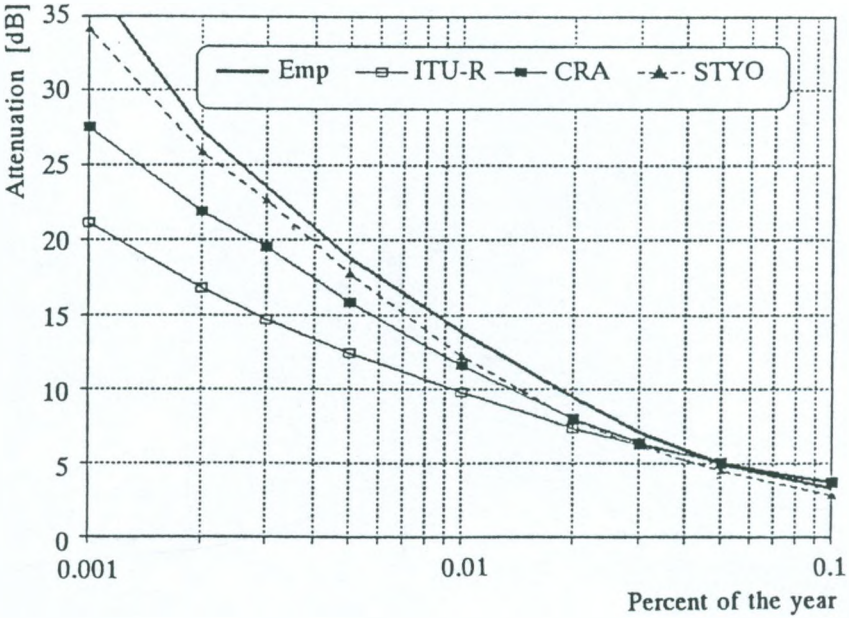


Fig 11. Empirical and predicted attenuation distributions at 11.5 GHz

The empirical and predicted attenuation distributions are presented in fig. 11 and 12. The accuracy of predictions was assessed according the recomendations of ITU-R [3] and the results of these assessments are shown in table 4. In this table RMS_1 denotes logaritmically weighted error [3] which reduces the meaning of deviation at low

attenuation levels and increases - at high levels. In case of Stutzman-Yon model $\gamma = 1/33$ was applied at both frequencies but additional calculation has been made at 18.6 GHz for $\gamma = 1/22$ (denoted * 18 GHz). It shows better fit to experimental data. The change of this coefficient is justified. The percentage p of rain rate interval applied for prediction at 18.6 GHz is limited to 0.005% and at 11.5 GHz - to 0.001%. The lack of the event with high rain rates (which occured in the year 1992) is more sensible at p = 0.001% then at p = 0.005%. Therefore higher time constant value $1/\gamma$ for prediction at 11.5 GHz then at 18.6 GHz is justified. The model is not very sensitive to changes of this parameter. The investigation shows that Stutzman-Yon model is distincly the best.

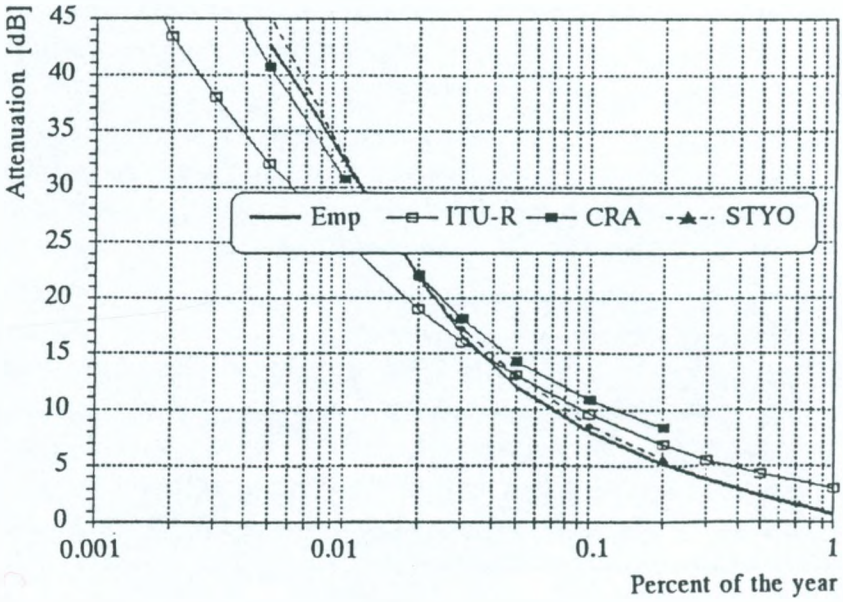


Fig. 12. Empirical and predicted attenuation distributions at 18.6 GHz

Table 4

The errors of attenuation prediction

Para-meter	ITU - R		STUTZMAN - YON			CRANE	
	11.5 GHz	18.6 GHz	11.5 GHz	18.6 GHz	*18.6 GHz	11.5 GHz	18.6 GHz
AVR	-4.9 dB	-1.6 dB	-0.7 dB	1.8 dB	-0.4 dB	-2.6 dB	1.9 dB
RMS	27.9%	23.4%	8.1%	11.2%	8.7%	15.1%	34.5%
RMS_t	40.2%	23.6%	8.1%	11.0%	9.2%	19.2%	25.2%

8. CONCLUSIONS

1. The obtained annual rain-rate distributions are in agreament with corresponding attenuation distributions. It shows that the measurements were properly performed. The averaged distributions are representative for central Poland.
2. The computed Q(p) functions show that the less curved is Q(p) function for rain-rate (the exponent $\beta = 0.153$) and most curved is that for attenuation at 11.5 GHz ($\beta = 0.22$). The Q(p) function for rain-rate is very close to that presented by UIT.
3. The obtained attenuation scaling factor agrees with that obtained with UIT formula in the interval of p for $p > 0.005\%$ and $p < 0.1\%$. If the dynamic of attenuation measurements at 18.6 GHz could be higher in the measuring system, then the p interval would be increased from the left side ($p < 0.005\%$) and if the accuracy of the measuremnts could be higher then this interval would be increased from the right side ($p > 0.1\%$). The desired dynamic of attenuation measuremnts at 18.6 GHz should be ca 2.2 times higher then that at 11.5 GHz and the measurements accuracies shold be ca 0.1 dB at 11.5 GHz and ca 0.2 dB - at 18.6 GHz.

4. The attenuation prediction models, tested with application of obtained representative rain-rate distribution, show that this prediction for the area of central Poland is very accurate in case of Stutzman-Yon model. In case of UIT model the accuracy is comparable or better in comparison with accuracies presented in literature.

REFERENCES

1. Crane R. K.: Prediction of attenuation by rain. IEEE Trans. Com., Vol. 28, No. 9, 1980.
2. ITU-R, Rec. 530-6: Propagation data and prediction methods required for the design of terrestrial and line-of-sight systems. Geneva 1995.
3. ITU-R, Rec. P.311-7: Acquisition, presentation and analysis of data in studies of tropospheric propagation. Geneva 1994.
4. ITU-R, Rec. PN.841: Conversion of annual statististics to worst month statistics. Geneva 1995.
5. Kawecki A.: Some aspects of attenuation due to rain prediction and rain rate correlation with attenuation. Prace Instytutu Łączności, nr 104, 1995.
6. Kawecki A.: Wave attenuation characteristics of the 11.5 GHz Earth-space path in Warsaw region. Ann. Telecommun., Vol. 48, No. 5-6, 1993.
7. Kawecki A.: Wieloletnie charakterystyki intensywności deszczu w Miedzeszynie na potrzeby radiokomunikacji. Prace Instytutu Łączności, nr 106, 1996.
8. Stutzman W. L., Yon K. M.: A simple rain attenuation model for earth-space radio links operating at 10-35 GHz. Radio Science, Vol. 21, No 1, 1986.
9. Sweeney D. G., Pratt T., Bostian C.: Hysteresis Effects in Instantaneous Frequency Scaling of Attenuation on 20 and 30 GHz Satellite Links. Electronic Letters, No. 1, 1992.

APPENDIX 1

Part I: Terrestrial line-of-sight path

TABLES 1, 2, 3, 4 and 5
Rain attenuation statistics

Transmit station			
TX name	Piaseczno		
TX country	Poland		
TX latitude (deg)	21.03		
TX longitude (deg) E	52.07		
TX altitude amsl (m)	111		
TX antenna height ag (m)	31.5		
TX 3 dB beam width (deg)	1.4		
Receive station			
RX site name	Miedzeszyn	Rain gauge type ••	tipping-bucket
RX country	Poland	RG resolution (mm/h)•••	2.8
RX latitude	21.19	RG integration time	60
RX longitude	52.17	RG location relative to RX (m)	20
RX altitude amsl (m)	92.5	Path length (km)	15.4
RX anntena height ag (m)	40	Terraintype (land/sea/mixed)	land
RX 3-dB antenna beam width, (deg)	1.25	Path profile	
RX antenna type	parabolic dish		
RX antenna diameter D (m)	1.5	Start date (yyyy.mm.dd)	1989.01.01
RX antenna feed type	horn	End date (yyyy.mm.dd)	1993.12.31
RX radome (Y/N)	N	Duration d (days)	1722
RX figure of merit (dB/K)		Frequency (GHz)	11.5 GHz
RX clear-sky level XPD (dB)		Polarisation tilt	horisontal
RX maximum side-lobe (dB) angle < 4 (deg)		Attenuation presented as excess	
RX relative level of maximum side lobe (dB)		or total (E/T)	E
RX dynamic range (dB)	40 dB		
RX integration time (s)			
Data sample interval (s)	4		
Calibration interval (days)•	60		
Data resolution (dB)	0.5 dB		

• Single point check - each day

•• Four other RG of the same type at distances 2700, 4900, 8700,12100

••• Rain rates computed for R in the interval $0.3 < R < 2.8$ mm/h by averaging single tips in the gaps < 10 min

APPENDIX 2

Part I: Terrestrial line-of-sight path

TABLES 1, 2, 3, 4 and 5
Rain attenuation statistics

Transmit station	
TX name	Piaseczno
TX country	Poland
TX latitude (deg)	21.03
TX longitude (deg) E	52.07
TX altitude amsl (m)	111
TX antenna height ag (m)	31.5
TX 3 dB beam width (deg)	0.87

Receive station			
RX site name	Miedzeszyn	Rain gauge type **	tipping-bucket
RX country	Poland	RG resolution (mm/h)***	2.8
RX latitude	21.19	RG integration time	60
RX longitude	52.17	RG location relative to RX (m)	20
RX altitude amsl (m)	92.5	Path length (km)	15.4
RX anntena height ag (m)	40	Terrain type (land/sea/mixed)	land
RX 3-dB antenna beam width, (deg)	0.75	Path profile	
RX antenna type	parabolic dish		
RX antenna diameter D (m)	1.5	Start date (yyyy.mm.dd)	1989.01.01
RX antenna feed type	horn	End date (yyyy.mm.dd)	1993.12.31
RX radome (Y/N)	N	Duration d (days)	1736
RX figure of merit (dB/K)		Frequency (GHz)	18.6 GHz
RX clear-sky level XPD (dB)		Polarisation tilt	horisontal
RX maximum side-lobe (dB) angle < 4 (deg)		Attenuation presented as excess or total (E/T)	E
RX relative level of maximum side lobe (dB)			
RX dynamic range (dB)	47 dB		
RX integration time (s)			
Data sample interval (s)	4		
Calibration interval (days)*	60		
Data resolution (dB)	0.5 dB		

* Single point check - each day

** Four other RG of the same type at distances 2700, 4900, 8700 and 12100 m

*** Rain rates computed for R in the interval $0.28 < R < 2.8$ mm/h by averaging single tips in the gaps < 10 min

Table 1

Attenuation distributions at 11.5 and 18.6 GHz
and rain rate distribution in 1989

Percentage of time	0.001	0.002	0.003	0.005	0.01	0.02	0.03
Att. at 11.5 GHz [dB]	30	25.63	22.3	17.48	11.69	7.87	6.25
Att. at 18.6 GHz [dB]	-	-	51	39.09	26.75	17.9	14.91
Rain rate [mm/h]	83.99	64.02	56.53	44.9	32.03	18.15	14.06
Percentage of time	0.05	0.1	0.2	0.3	0.5	1	2
Att. at 11.5 GHz [dB]	4.91	3.66	2.65	2.08	1.38	-	-
Att. at 18.6 GHz [dB]	11.79	9.12	6.43	4.81	2.95	1	-
Rain rate [mm/h]	10.46	7.36	4.87	3.29	1.97	0.66	0.29

Table 2

Attenuation distributions at 11.5 and 18.6 GHz
and rain rate distribution in 1990

Percentage of time	0.001	0.002	0.003	0.005	0.01	0.02	0.03
Att. at 11.5 GHz [dB]	15.74	12.96	11.47	10.02	7.44	5.56	4.69
Att. at 18.6 GHz [dB]	36.22	29.28	26.35	22.79	17.39	13.4	11.67
Rain rate [mm/h)	45.41	38.89	33.89	28.53	20.12	14.35	11.17
Percentage of time	0.05	0.1	0.2	0.3	0.5	1	2
Att. at 11.5 GHz [dB]	3.82	2.87	1.78	1.3	0.82	0.32	-
Att. at 18.6 GHz [dB]	9.53	6.5	4.01	3	1.66	0.5	-
Rain rate [mm/h]	8.41	6.02	4.25	3.27	2.22	1.1	0.36

Table 3

Attenuation distributions at 11.5 and 18.6 GHz
and rain rate distribution in 1991

Percentage of time	0.001	0.002	0.003	0.005	0.01	0.02	0.03
Att. at 11.5 GHz [dB]	-	-	-	31	22.11	16.2	12.76
Att. at 18.6 GHz [dB]	-	-	-	-	48	36.91	30.17
Rain rate [mm/h]	105.91	93.86	84.74	65.42	47.31	29.07	21.74
Percentage of time	0.05	0.1	0.2	0.3	0.5	1	2
Att. at 11.5 GHz [dB]	8.54	4.34	2.53	1.89	1.13	0.43	-
Att. at 18.6 GHz [dB]	20.29	10.45	6.01	4.26	2.52	1.04	-
Rain rate [mm/h]	13.97	7.77	4.92	3.73	2.44	1.16	0.4

Table 4

Attenuation distributions at 11.5 and 18.6 GHz
and rain rate distribution in 1992

Percentage of time	0.001	0.002	0.003	0.005	0.01	0.02	0.03
Att. at 11.5 GHz [dB]	37	24	18.65	14.1	8.7	4.99	3.83
Att. at 18.6 GHz [dB]	-	52	42	32.96	20.36	11.83	9.15
Rain rate [mm/h]	61.98	50	41.88	31.73	20.43	14.22	11.69
Percentage of time	0.05	0.1	0.2	0.3	0.5	1	2
Att. at 11.5 GHz [dB]	3.11	2.42	1.74	1.32	0.8	-	-
Att. at 18.6 GHz [dB]	7.27	5.52	3.94	2.85	1.47	0.48	
Rain rate [mm/h]	8.98	6.72	5.05	4.3	3.36	1.87	0.65

Table 5

Attenuation distributions at 11.5 and 18.6 GHz
and rain rate distribution in 1993

Percentage of time	0.001	0.002	0.003	0.005	0.01	0.02	0.03
Att. at 11.5 GHz [dB]	24.28	21.33	18.58	16.2	13.42	10.61	8.69
Att. at 18.6 GHz [dB]		47	42.74	37.01	31.47	25.03	20.37
Rain rate [mm/h]	68.95	57.33	49.97	41.57	30.31	20.55	16.33
Percentage of time	0.05	0.1	0.2	0.3	0.5	1	2
Att. at 11.5 GHz [dB]	6.09	3.83	2.37	1.82	1.29	0.52	-
Att. at 18.6 GHz [dB]	14.3	9.08	5.37	3.87	2.58	1.09	-
Rain rate [mm/h]	11.65	7.79	5.06	3.83	2.45	1.16	0.44

Arnold Kawecki

CHARAKTERYSTYKI TŁUMIENIOWE PROPAGACJI FAL NA CZĘSTOTLIWOŚCIACH 11,5 I 18,6 GHz PODCZAS DESZCZU NA TRASIE 15,4 KM W POBLIŻU WARSZAWY

S t r e s z c z e n i e

Przedstawiono podsumowanie wyników badań propagacji mikrofal w pasmach 11,5 i 18,6 GHz, przeprowadzonych w latach 1989-93 na trasie długości 15,4 km w okolicach Warszawy. Pod uwagę zostały wzięte jedynie przypadki tłumienia fal wywołanego przez deszcze. Podsumowanie zawiera rozkłady intensywności deszczu i tłumienia fal na obydwu częstotliwościach w kolejnych latach, a także obliczone wartości współczynnika Q, służącego do przekształcenia rocznych rozkładów na rozkłady dla najgorszego miesiąca

w roku w przypadku zarówno intensywności deszczów, jak i tłumień fali. Określono również współczynnik częstotliwościowego przekształcenia rozkładów tłumienia oraz chwilowych wartości tłumienia. W tym ostatnim przypadku współczynnik obliczono na podstawie 12 przypadków tłumienia, które wystąpiły w obydwu częstotliwościach jednocześnie. Otrzymane wyniki porównano z modelem UIT częstotliwościowego przekształcenia rozkładów tłumienia. Podano też wyniki oceny modeli do przewidywania rozkładów tłumienia fali w przypadku modelu: UIT, Crane'a i Stutzmana-Yona.

Арнольд Кавецки

ХАРАКТЕРИСТИКА РАСПРОСТРАНЕНИЯ ПО ЗАТУХАНИЮ МИКРОВОЛН НА ТРАССЕ 15,4 КМ В БЛИЗИ ВАРШАВЫ ВО ВРЕМЯ ДОЖДЯ НА ЧАСТОТАХ 11,5 ГГц И 18,6 ГГц

Резюме

В публикации представлены характеристики распространения микроволн полученные на основании исследований проведенных в периоде 1989-93 на экспериментальной трассе длиной 15,4 км. Рассчитывались характеристики только для случаев ослабления вызванного дождем. Полученные характеристики представляют распределения интенсивности дождя и ослабления волн на обоих частотах для очередних лет а также указывают значения фактора Q для преобразования годовых распределений на распределения для найхудшего месяца года в случае интенсивности дождя и ослабления волн. Вычислены тоже значения факторов для частотного пересчета распределений ослабления и мгновенных значений

ослабления. В последнем случае расчет фактора основан на 12 случаях ослабления волн происшедших одновременно на обоих частотах. Полученные результаты сопоставлены с моделью UIT для частотного пересчета распределений ослабления. На конец проведено оценку моделей для прогноза распределений ослабления волн в случае модели UIT а также моделей Крейна и Стутсмана-Иона.

Arnold Kawecki

LES CARACTERISTIQUES D'AFFAIBLISSEMENT DE LA PROPAGATION DES ONDES DES FREQUENCES DE 11,5 ET 18,6 GHz AN COURS DE LA PLUIE SUR L'ITINERAIRE DE 15,4 KM A VOISINAGE DE VARSOVIE

R é s u m é

On a démontré en résumé les résultats desessis de la propagation des microondes dans la bande de 11,5 et 18,6 GHz faits on cours des années 1989-1993 sur l'itinéraire de 15,4 km en longeur à voisinage de Varsovie. On a pris en considération seulement les cas de l'affaiblissement des ondes dus à la pluie. Ce résumé contient des données de la distribution de l'intensité de la pluie ainsi que celle de l'affaiblissement des ondes pour les deux fréquences en l'années consecutives et les valeurs calculées du coefficient Q qui serve à transformer les distributions annuelles sur les distributions pour le pire des mois d'un an pour le cas de l'intensité de pluie et celle de l'affaiblissement de l'onde. On a défini aussi le coefficient de fréquence de transformation des distributions de l'affaiblissement oinsi que celui des valeurs instantanes de l'affaiblissement. Pour ce dernier cas ce coefficient était calculé à la base des données de 12 cas d'affaiblissement qui se sout manifestés pour les deux fréquences simultaneussement.

Arnold Kawecki

DÄMPFUNGSKENNLINIEN DER WELLENAUSBREITUNG IM REGEN AUF DER STRECKE VON 15,4 KM UNWEIT VON WARSZAWA IN FREQUENZBANDER VON 11,5 GHz UND 18,6 GHz

Z u s a m m e n f a s s u n g

Zusammenfassng der Ergebnisse der Mikrowellen-Ausbreitungsmessungen in Frequenzbänder von 11,5 GHz und 18,6 GHz wird vorgestellt. Die Messungen sind 1989-93 auf der Strecke von 15,4 km in der Nähe von Warszawa durchgeführt worden. Nur die durch Regen verursachte Wellendämpfung wird berücksichtigt. Zusammenschaltung enthält Regenintensitäts- und Wellendämpfungs-Verteilung in nachstehenden Jahren in beiden Frequenzbändern und die Werte des für Regenintensität und für Wellendämpfung berechneten Q-Koeffizients für Konversion von Jahresverteilung in diese für den schlechtesten Monat des Jahres. Frequenzkonversion-Koeffizient von Dämpfungsverteilung und -momentanwerte sind bestimmt worden. Koeffizient der Dämpfungsmomentanwerte ist anhand 12 gleichzeitig in beiden Frequenzbändern auftretenden Ereignisse berechnet worden. Die gewonnene Ergebnisse sind mit ITU-Modell für Dämpfungsverteilung-Frequenzkonversion verglichen worden. Zum Abschluß werden Resultate von Dämpfung-Prediktion-Tests für ITU-, Crane- und Stutzman-Yon-Modell präsentiert.

KOMUNIKAT

Mirosław Pietranik

621.317:621.391.82:621.396

POLIGON DO POMIARÓW NATĘŻENIA POLA ZABURZEŃ RADIOELEKTRYCZNYCH

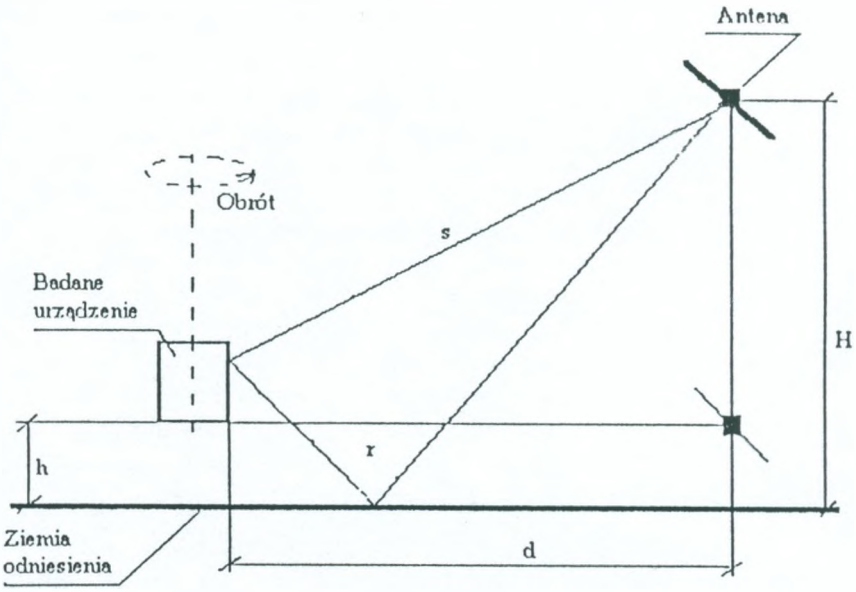
W artykule omówiono podstawowe wymagania, jakie musi spełniać poligon stosowany w pomiarach natężenia pola elektromagnetycznego w dziedzinie kompatybilności elektromagnetycznej, sposób sprawdzania jego poprawności konstrukcyjnej, uwagi o elementach decydujących o poprawności jego działania oraz wyniki pomiarów dla poligonu pomiarowego, zbudowanego na terenie Instytutu Łączności we Wrocławiu.

1. WSTĘP

Elektronizacja wszystkich dziedzin życia jest obecnie faktem nieodwracalnym. Wiąże się z nią lawinowy wzrost liczby różnorodnych urządzeń, które mają coraz większą czułość (ich elementy czynne pracują przy coraz niższych poziomach) i działają z coraz większą szybkością. W efekcie każde urządzenie działa w bardzo skomplikowanym środowisku elektromagnetycznym, bogatym w różnorodne sygnały, będąc zarówno jego ofiarą, jak i kreatorem przez wprowadzanie doń własnych sygnałów, stających się zaburzeniami dla innych urządzeń znajdujących się w tym środowisku.

Podstawowym parametrem charakteryzującym zewnętrzne środowisko elektromagnetyczne, w którym pracuje określone urządzenie, jest natężenie pola.

Układ pomiarowy, w którym dokonuje się oceny urządzenia pod kątem natężenia wytwarzanego przez nie pola zaburzeń pokazano na rys. 1. Jest to układ zalecany przez wszystkie normy obowiązujące w dziedzinie pomiarów zaburzeń [17, 18, 19].



Rys. 1. Podstawowa konfiguracja układu stosowanego przy pomiarach natężenia pola zaburzeń radioelektrycznych na otwartym poligonie pomiarowym

d - odległość między badanym urządzeniem i anteną pomiarową, wyznaczana w rzucie poziomym między skrajnymi (najbliższymi) obrysami urządzenia i anteny; d = 3 m lub 10 m [17, 18, 19], h - wysokość umieszczenia badanego urządzenia nad ziemią w czasie pomiarów; h = 0,8 ÷ 1 m [17, 18, 19], H - wysokość anteny pomiarowej, zmieniana w czasie pomiarów w przedziale od 1 m do 4 m

Badane urządzenia umieszcza się na izolowanej podstawce na wysokości 0,8 ÷ 1 m nad ziemią odniesienia. Pomiary wykonuje się dla obu polaryzacji pola: pionowej i poziomej, wyszukując w trakcie pomiarów maksymalne wskazania przez zmianę wysokości (H) anteny odbiorczej w przedziale od 1 m do 4 m oraz przez obrót badanego urządzenia w płaszczyźnie poziomej wokół jego osi pionowej w przedziale do 360°.

Dokładność pomiarów natężenia pola zaburzeń zależy od wielu bardzo różnych czynników, z których główniejsze wymieniono w tablicy 1.

Tablica 1

Czynniki wpływające na dokładność pomiarów natężenia pola

Źródło błędów	Przyczyna
Poligon pomiarowy	- anomalie w przewodności ziemi odniesienia [3] - niewłaściwe wymiary pola pomiarowego [16] - odbicia od otaczających przedmiotów metalowych, budynków itp. [16] - użycie niewłaściwych materiałów do budowy ziemi odniesienia, osłon pogodowych, podpór itp. [1, 3] - obecność niekontrolowanych sygnałów obcych [3]
Antena	- "niepewność" współczynnika antenowego (brak informacji producenta o warunkach cechowania) [15, 16] - niedokładność oceny położenia przestrzennego anteny (wysokość, odległość od źródła zaburzeń, polaryzacja) [3]
Układ pomiarowy	- niedopasowanie kabla antenowego [13] - niewłaściwe ułożenie kabla antenowego (wpływ na charakterystykę anteny, w szczególności przy polaryzacji pionowej [13] - niepewne kontakty (częsta przyczyna wynikająca z ruchu anteny pomiarowej)
Człowiek	- wiedza o podstawach propagacji fal elektromagnetycznych - wiedza o wpływie czynników wymienionych powyżej

2. UWAGI O KONSTRUKCJI POLIGONU POMIAROWEGO

Większość norm z dziedziny kompatybilności elektromagnetycznej z zasady przyjmuje, że pomiary natężenia pola wykonuje się na

otwartym poligonie pomiarowym. Stosowanie do tego celu komór bezechowych lub komór GTEM jest uwarunkowane posiadaniem przez nie odpowiedniego atestu równoważności względem otwartego poligonu pomiarowego.

Poligon pomiarowy jest to część terenu o odpowiednio przygotowanej powierzchni ziemi (tzw. ziemi odniesienia), z doprowadzoną energią zasilania, z podporami dla badanego obiektu (stół obrotowy), odpowiednimi osłonami pogodowymi itp.

2.1. Lokalizacja

Poligon pomiarowy powinien znajdować się na płaskim terenie o odpowiednich wymiarach, wolnym od różnych obiektów powodujących niekontrolowane odbicia fali elektromagnetycznej. Najlepiej jeśli znajduje się on na terenie osłoniętym od ulic i ruchliwych punktów miasta, wolnym od obcych źródeł zaburzeń. Jako osłony mogą być wykorzystane także ściany otaczających poligon pomiarowy budynków. Muszą one jednak znajdować się w takiej odległości, aby ewentualne odbicia od nich nie wpływały na wynik pomiarów natężenia pola elektromagnetycznego. Z doświadczenia wynika, że odległość równa 20 m lub większa gwarantuje takie warunki. Należy także pamiętać o zapewnieniu odpowiedniej odległości od przedmiotów odbijających, znajdujących się nad wybranym terenem. Ogólnie zakłada się, że wystarczy zapewnić odległość większą niż 3 m w stosunku do najwyżej położonych elementów układu pomiarowego. Zazwyczaj takie ograniczenie nasuwa najwyższe położenie anteny pomiarowej. Przy podanych w normach wysokościach położenia anteny pomiarowej oznacza to, że nad płaszczyzną ziemi, aż do wysokości 7 ÷ 9 m, nie powinno być żadnych elementów metalowych (związanych np. z konstrukcją dachu osłaniającego poligon pomiarowy).

Ważnym elementem decydującym o wyborze lokalizacji poligonu pomiarowego jest poziom zewnętrznych sygnałów, które mogą

w istotny sposób utrudniać pomiary natężenia pola zaburzeń od badanego obiektu.

2.2. Wymiary

Oceny niezbędnych wymiarów i kształtu ziemi odniesienia poligonu pomiarowego można dokonać za pomocą kryterium Fresnela, korzystając z zależności podanych w [2, 14]. Tak zwana elipsa Fresnela określa najbardziej istotną część terenu, odbicia, od której warunkują wartość mierzonego natężenia pola. W tablicy 2 zestawiono wymiary elipsy Fresnela właściwe dla podstawowych odległości pomiarowych stosowanych w miernictwie natężenia pola zaburzeń radioelektrycznych, przy założeniu, że obiekt badany jest umieszczany na wysokości 1 m lub 2 m nad ziemią odniesienia, a antena pomiarowa jest przesuwana w pionie w przedziale od 1 m do 4 m. Największe wymiary elipsy Fresnela są związane z najniższą częstotliwością pomiarową, równą 30 MHz.

Tablica 2

Wymiary płaskiego terenu, w obrębie którego nie powinno być żadnych elementów odbijających fale elektromagnetyczne [15, 16]

Odległość pomiarowa [m]	Wysokość położenia badanego obiektu [m]	Wysokość anteny pomiarowej [m]	Wymiary osi elipsy	
			większej [m]	mniejszej [m]
3	1	4	9,9	9,5
	2	4	11,3	11,0
10	1	4	15,3	12,0
	2	4	16,3	13,0

W normach [5 ÷ 9] istnieje rozbieżność w ocenie minimalnych wymiarów poligonu pomiarowego. I tak, największe wymiary są

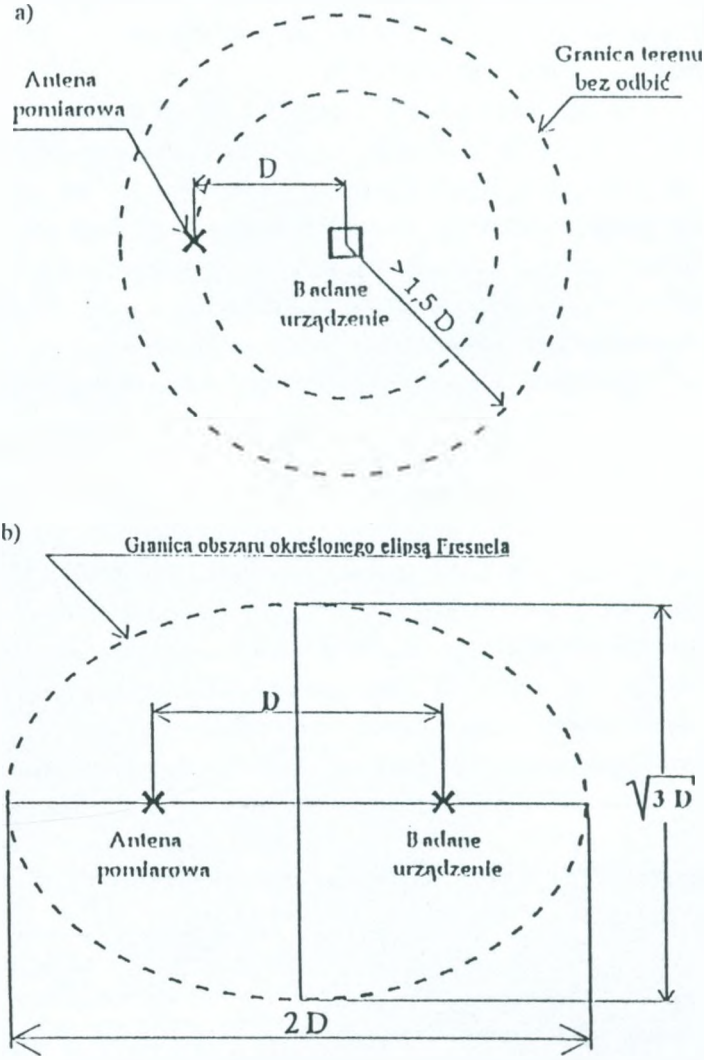
zalecane w normach amerykańskich [1], a najmniejsze w publikacjach CISPR [7 ÷ 9]. Jako norma podstawowa jest traktowana publikacja nr 16 CISPR [8] i jej ustalenia stanowią wytyczne dla innych publikacji CISPR, a w konsekwencji dla norm europejskich EN. W publikacji tej sformułowano inne wymagania dla małych urządzeń (ustawianych w czasie pomiarów na stole pomiarowym na wysokości 1 m), a inne dla dużych obiektów stacjonarnych ustawianych bezpośrednio nad płytą ziemi odniesienia na wysokości 10 cm. Zalecane przez nią wymiary poligonu pokazano na rys. 2.

2.3. Płyta ziemi odniesienia

Przy konstrukcji ziemi odniesienia należy rozpatrzyć:
- rodzaj materiału: płyta metalowa - pełna albo siatka;
- połączenie poszczególnych elementów płyty między sobą w jedną całość;
- połączenie płyty metalowej z realną ziemią;
- zabezpieczenie antykorozyjne.

Najlepiej na płytę ziemi odniesienia nadają się materiały nieferromagnetyczne, np. aluminium, miedź, mosiądz. Są to jednak materiały drogie. W większości przypadków bardzo dobre rezultaty daje zastosowanie ocynowanej siatki stalowej o polutowanych oczkach, pod warunkiem pogodzenia się z pewnym wpływem dużej przenikalności magnetycznej stali. Na ogół stosuje się siatkę o oczku od 8 mm do 12 mm zakopaną pod ziemią. Takie rozwiązanie ułatwia uzyskanie właściwej impedancji przejścia z przewodzącej płyty (siatki) do realnej ziemi. Należy jednak pamiętać o zwiększonej korozji.

Często stosuje się pokrycie metalowej siatki asfaltem, co zapewnia bardzo dobre zabezpieczenie antykorozyjne. Jednocześnie umożliwia utrzymanie płaskości ułożonej powierzchni, co jest bardzo ważnym czynnikiem przy eksploatacji poligonu pomiarowego (biorąc pod uwagę konieczność chodzenia po polu oraz ustawiania i przenoszenia



Rys. 2. Minimalne wymiary poligonu pomiarowego wg publikacji nr 16 CISPR [8]

a) dla urządzeń dużych, ustawianych bezpośrednio nad ziemią odniesienia;
b) dla urządzeń małych, ustawianych na stole wysokości 0,8 m

ciężkiego sprzętu: badanego oraz pomiarowego). Eliminuje to konieczność budowania wzmacniających ścieżek dojścia do stanowiska antenowego i do stołu obrotowego.

Zastosowanie asfaltu może być jednak źródłem błędów w pomiarach natężenia pola. Zagadnienie to zostało bliżej przeanalizowane przez Benneta [3]. Z podanych tam obliczeń wynika, że przy warstwie asfaltu grubości 5 cm ponad metalową płytą ziemi odniesienia w najgorszym przypadku może wystąpić błąd pomiaru natężenia pola około 6 dB w stosunku do pola pomiarowego z odsłoniętą płytą metalową. Należy się spodziewać, że podobne wpływy mogą uwidocznić się przy innych, podobnych materiałach zabezpieczających, takich jak np. beton.

2.4. Płaskość ziemi odniesienia

Płaskość płyty ziemi odniesienia można zdefiniować jako odległość w pionie między bliskimi punktami leżącymi odpowiednio na wypukłości i wklęsłości ziemi odniesienia. Przy czym tak zdefiniowana nierówność terenu wynika z dopuszczalnej różnicy dróg promieni odbitych od porównywanych punktów, równej $\lambda/4$ [16].

Odpowiednie obliczenia wykonuje się wg kryterium Raylegha. W tablicy 3 przytoczono uzyskiwane wg tego kryterium wyniki.

Tablica 3

Dopuszczalna nierówność powierzchni ziemi odniesienia [8, 15, 16]

Odległość pomiarowa D [m]	Wysokość badanego urządzenia nad ziemią [m]	Maksymalna wysokość anteny odbiorczej [m]	Maksymalna nierówność ziemi odniesienia	
			w długościach fali [λ]	przy f=1000 MHz [cm]
3	1	4	0,15	4,5
10	1	4	0,28	8,4

Parametr ten narzuca wymagania w zakresie ułożenia w poziomie płyty metalowej lub siatki. Oczywisty jest lekki, równomierny spadek terenu w celu odprowadzenia wody. Niedopuszczalne są natomiast bliskie, silne pofałdowania. Dla większości praktycznych zastosowań jest to dość łagodne wymaganie, łatwe do spełnienia w praktyce.

2.5. Osłony pogodowe

Zastosowanie osłon pogodowych jest oczywiste, jeśli się planuje wykorzystywanie poligonu pomiarowego przez większą część roku, niezależnie od warunków pogodowych. Podstawowym zagadnieniem jest tu podjęcie decyzji: jaka jego część ma być osłonięta, jakiej wielkości będą te osłony, z jakiego materiału będą wykonane i jakiej grubości. Liczba i konstrukcyjne wykonanie osłon (pomijając bardzo drogi przypadek umieszczenia całego poligonu pomiarowego w jednej, odpowiednio dużej hali pomiarowej) zależy od posiadanych środków finansowych. Bardzo często stosuje się dwie osłony: jedną wokół anteny pomiarowej, a drugą - wokół badanego obiektu (stołu obrotowego). W takiej sytuacji dobór materiału osłony jest bardzo istotny, ponieważ na drodze fali elektromagnetycznej (bezpośredniej i odbitej) może znaleźć się nawet kilka ścian.

Na ogół przyjmuje się, że w zakresie częstotliwości do 1 GHz osłony wykonane z drewna o specjalnym wysyceniu, z włókna szklanego lub innych podobnych tworzyw sztucznych nie wnoszą istotnego tłumienia dla fal elektromagnetycznych. Problemy mogą pojawić się dopiero w przypadku materiałów skłonnych do nadmiernego zawilgocenia lub gromadzenia osadów brudu. Wzrost przewodności, przy dużej stałej dielektrycznej (dla większości tworzyw sztucznych $\varepsilon = 2$ do 5), prowadzić może do istotnego wzrostu współczynnika odbicia (ugięcia fali elektromagnetycznej), a w konsekwencji do wzrostu niekontrolowanych błędów w pomiarach natężenia pola. Zagadnienie to jest szerzej omówione w [10]. Oporność materiału osłony odpo-

wiednio przygotowanego i utrzymywanego w czystości w czasie eksploatacji nie zmienia się w sposób istotny i na ogół ma dużą wartość, rzędu kilku megaomów na metr. Według [10] nawet mocno zawilgocone drewno ma oporność rzędu 1 MΩ/m, a suche rzędu 100 MΩ/m. Dlatego sama zmiana oporności materiału osłony nie jest decydującym czynnikiem. Istotną rolę odgrywa przede wszystkim stała dielektryczna materiału osłony i jej grubość [10]. Według [12] wybór niewłaściwego materiału na osłony pogodowe może powodować błędy w pomiarze natężenia pola około 3 do 5 dB.

2.6. Wyposażenie poligonu pomiarowego

- **Stół obrotowy**

Stół obrotowy jest bardzo dogodnym urządzeniem stosowanym zwłaszcza przy pomiarach emisji zaburzeń. Powierzchnia nośna stołu obrotowego powinna znajdować się na poziomie ziemi odniesienia z dobrym ich połączeniem galwanicznym, o małej impedancji dla najwyższych częstotliwości pomiarowych. Dla urządzeń lekkich, dla których normy przewidują pomiary po ustawieniu ich na wysokości od 0,8 m do 1 m nad powierzchnią ziemi odniesienia, stosuje się zwykłe stoły drewniane lub z tworzywa ustawiane na stole obrotowym.

- **Maszt anteny odbiorczej**

Maszt wykonuje się z materiału izolacyjnego. Przewód współosiowy, łączący antenę z odbiornikiem pomiarowym, powinien biec do transformatora antenowego zawsze w płaszczyźnie ortogonalnej do głównej osi anteny, co zapewnia symetrię układu antenowego względem ziemi. Przy czym należy go prowadzić najpierw poziomo na odległość minimum 1 m od anteny, a następnie pionowo w kierunku ziemi odniesienia. Od tego punktu aż do przyrządu pomiarowego należy go ułożyć wzdłuż ziemi odniesienia lub pod nią. Przewód ten

powinien być możliwie najkrótszy, ze względu na ewentualne tłumienie sygnału przy częstotliwościach bliskich 1 GHz.

- **Doprowadzenie sygnałów testowych i zasilania do stanowiska pomiarowego**

Wszelkie przewody biegnące do urządzeń pomiarowych i badanego urządzenia należy umieszczać pod płytą ziemi odniesienia lub tak daleko od poligonu pomiarowego jak to jest możliwe i prowadzić je pod kątem prostym do osi poligonu. Jeśli jest to niemożliwe, wówczas mogą one biec nad ziemią odniesienia, ale powinny ściśle przylegać do jej powierzchni i być dobrze uziemione.

- **Poziom zewnętrznych sygnałów zaburzeń (tła)**

Poziom tła powinien być wystarczająco niski w porównaniu z poziomem mierzonych sygnałów. Aby zapewnić dobre warunki pomiarowe, poziom tła powinien być co najmniej o 20 dB niższy od mierzonego sygnału zasadniczego. Ponieważ ten warunek nie zawsze może być spełniony, w wielu normach podaje się sposób postępowania w przypadkach, gdy ten odstęp jest rzędu 6 dB, a nawet mniejszy. Najdokładniej formułuje to publikacja nr 22 CISPR [9], a za nią norma EN 55022 [19].

- **Kontrola wpływu czasu i pogody**

Publikacja nr 16 CISPR [8] zaleca okresowe wykonywanie pomiarów współczynnika tłumienia poligonu pomiarowego w celu sprawdzenia wpływu osadów na osłonach pogodowych. Taki pomiar uwzględnia także kontrolę parametrów przewodów współosiowych oraz przyrządów zastosowanych w procesie pierwotnej kalibracji. Kontrolę należy przeprowadzać co 6 miesięcy, jeżeli wcześniej nie wystąpią objawy zmian w materiale osłon (np. zmiana koloru w przypadku tworzyw sztucznych).

3. ZASADY WERYFIKACJI POLIGONU POMIAROWEGO

Sprawdzenie poligonu pomiarowego dokonuje się przez pomiar tzw. znormalizowanego współczynnika tłumienia, oznaczonego dalej przez A_N (w literaturze anglojęzycznej stosuje się skrót: NSA - - *Normalized Site Attenuation*), który jest miarą strat mocy od punktu połączenia generatora sygnałowego z anteną nadawczą do punktu połączenia odbiornika pomiarowego z anteną odbiorczą. Tak zdefiniowany współczynnik jest określany dla konkretnego poligonu pomiarowego przez pomiar i porównywany z analogicznym współczynnikiem obliczonym dla idealnego poligonu pomiarowego.

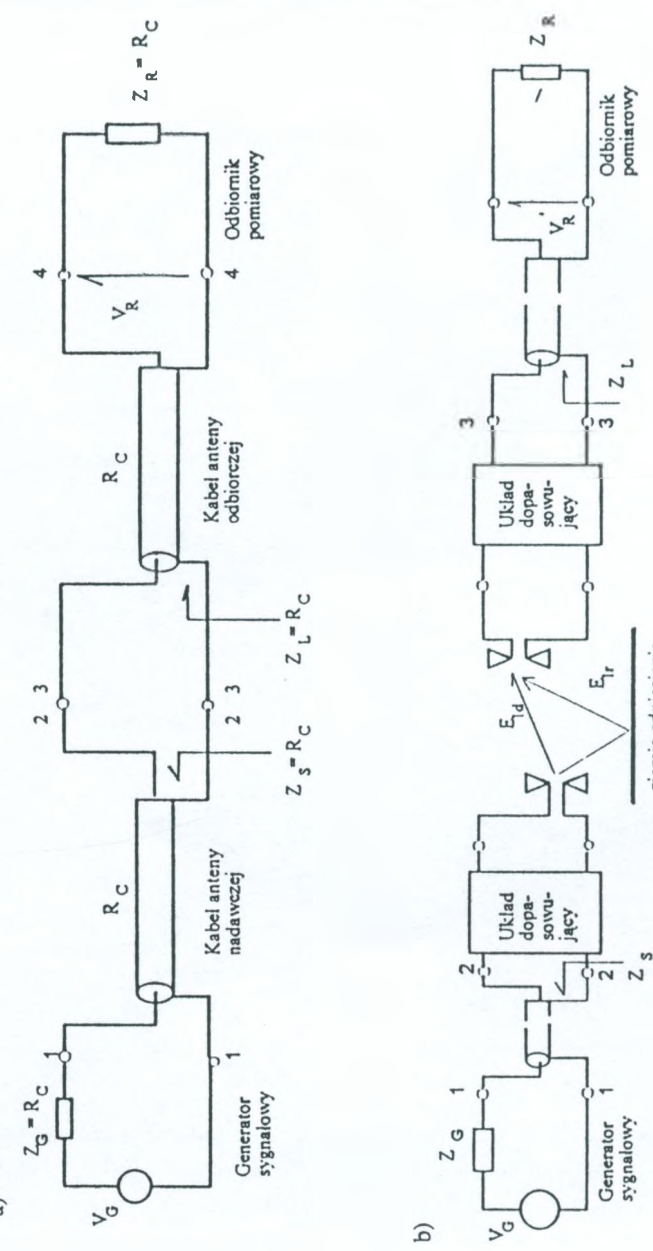
Zgodnie z publikacją nr 16 CISPR [8] i innymi podobnymi normami, jeśli różnica między wartością zmierzoną współczynnika tłumienia nie odbiega o więcej niż ±4 dB od wartości teoretycznej, to testowany poligon pomiarowy uważa się za spełniający wymagania, dzięki czemu może on być stosowany przy wszelkich pomiarach emisji zaburzeń elektromagnetycznych.

Na rys. 3 przedstawiono schematycznie dwa kolejne etapy postępowania w procesie wyznaczania współczynnika A_N:

1) pomiar napięcia V_R na wejściu odbiornika pomiarowego przy bezpośrednim połączeniu kabli obu anten (rys. 3a),
2) pomiar napięcia V'_R po dołączeniu kabli do obu anten ustawionych w odpowiedniej odległości na polu pomiarowym (rys. 3b).

Zatem współczynnik tłumienia A_N jest równy stratom wtrąceniowym układu znajdującego się między zaciskami anten: 2-2 i 3-3. Z takiej definicji wynika również to, że we współczynniku A_N uwzględnia się również parametry zastosowanych anten pomiarowych.

W artykule [4] znajduje się szczegółowy opis wyprowadzenia wzoru na tłumienność poligonu pomiarowego A_N. Autor podaje następujące końcowe zależności:



Rys. 3. Zasada pomiarów współczynnika tłumienności poligonu pomiarowego A_N

a) konfiguracja układu przy pomiarach strat w kablach; b) konfiguracja układu pomiarowego po włączeniu anten

$$A_N = \frac{|V_R/V'_R|^2}{AF_1 AF_2} = \frac{|V_R/V'_R|^2}{AF_1 AF_2} = \\ = \frac{1}{G_{HS}} \left(\frac{300 R_C s}{Z_0 f_M} \right)^2 , \tag{1}$$

gdzie:

AF_1 i AF_2 - współczynniki antenowe anteny nadawczej i anteny odbiorczej,

$Z_0 = 120\ \pi$ - impedancja wolnej przestrzeni [Ω],

f_M - częstotliwość [MHz],

$R_C = 50\ \Omega$ - impedancja charakterystyczna układu pomiarowego,

G_{HS} - zysk anten.

Dla anten o polaryzacji poziomej, znajdującej się nad doskonale przewodzącą ziemią:

$$G_{HS} = 1 + \left(\frac{s}{r} \right)^2 - 2 \frac{s}{r} \cos[k(r-s)] . \tag{2}$$

Dla polaryzacji pionowej:

$$G_{HS} = \left(\frac{d}{s} \right)^4 \left[1 + \left(\frac{s}{r} \right)^6 + 2 \left(\frac{s}{r} \right)^3 \cos[k(r-s)] \right] , \tag{3}$$

gdzie:

s - droga promienia bezpośredniego między antenami,

r - droga promienia odbitego od ziemi odniesienia,

$k = 2\pi/\lambda$.

Zależność (1) można przedstawić w następującej dogodniejszej formie po podstawieniu znanych wartości dla $R_C = 50\ \Omega$ i $Z_0 = 120\pi\ \Omega$:

$$A_N = 20\,lg\,d - 20\,lg f_M - 10\,lg G_{HS} + 32 \quad [\text{dB}]\,, \tag{4}$$

gdzie:

d - nominalna odległość pomiarowa.

Według Benetta [4] uzyskiwane za pomocą zależności (4) wartości współczynnika tłumienia poligonu pomiarowego A_N nie odbiegają o więcej niż 0,2 dB od wartości podawanych w [8].

Procedura pomiarowej weryfikacji poprawności poligonu jest opisana dokładnie w publikacji nr 16 CISPR. Według niej tłumienie poligonu pomiarowego określa się z następującej zależności:

$$A_N = V_R - V'_R - AF_1 - AF_2 - Q\,, \tag{5}$$

gdzie:

Q - współczynnik korekcyjny, uwzględniający wzajemną impedancję anten. Jest on istotny przy niższych częstotliwościach i bliższym położeniu anten. Jego wartości dla nominalnej odległości pomiarowej 3 m zestawiono w tablicy 4.

Tablica 4

Wartości współczynnika korekcyjnego Q

F [MHz]	30	35	40	45	50	60	70	80	90	100	120	125	140	150	160	175	180	200
Q [dB]	+3,1	+4,0	+4,1	+3,3	+2,8	+,0	-0,4	-1,0	-1,0	-1,2	-0,1	-0,2	-0,1	-0,9	-1,5	-1,8	-1,0	+0,1

Wartość V'_R odpowiada maksymalnym wskazaniom odbiornika pomiarowego w czasie przesuwania anteny odbiorczej spolaryzowanej poziomo w przedziale od 1 m do 4 m (przy odległościach pomiarowych 3 m i 10 m) lub w przedziale od 2 m do 6 m (przy odległościach 30 m i 100 m). Antenę spolaryzowaną pionowo przesuwa się w zakresie zmian wysokości jej środka od 2,75 m do 4 m (wynika to

stąd, że przy częstotliwości 30 MHz koniec jej dolnego ramienia powinien znajdować się nie bliżej niż 25 cm od ziemi).

Na ogół sprawdzanie poligonu pomiarowego rozpoczyna się po ustawieniu anten w polaryzacji poziomej. Wynik pomiaru A_N powinien znaleźć się w przedziale ±4 dB względem nominalnej krzywej cechowania poligonu pomiarowego, ponieważ przy tej polaryzacji cała procedura pomiarowa jest mniej wrażliwa na wszelkie anomalie związane z terenem pomiarowym. Takie anomalie świadczą o istotnych ograniczeniach występujących w otoczeniu poligonu pomiarowego.

Ostateczną weryfikację poligonu pomiarowego wykonuje się przy polaryzacji pionowej anten, ponieważ przy tej polaryzacji bardziej krytycznie przejawiają się wszelkie jego niedoskonałości.

4. PRZYKŁADOWA PROCEDURA SPRAWDZANIA OTWARTEGO POLIGONU POMIAROWEGO W ZAKRESIE CZĘSTOTLIWOŚCI OD 30 MHZ DO 1000 MHZ

Wartość współczynnika A_N wyznacza się z zależności (5). Zasadę pomiarów współczynnika zilustrowano na rys. 3, na którym zwrócono uwagę na dopasowanie impedancyjne w odpowiednich punktach torów pomiarowych. Generator sygnałowy jest dołączany do anteny nadawczej za pomocą kabla pomiarowego odpowiedniej długości. Antenę nadawczą umieszcza się na wysokości h przy wybranej jej polaryzacji. W przypadku strojonego dipola należy jego długość dostroić odpowiednio do wybranej częstotliwości.

Antenę odbiorczą umieszcza się w odległości d od anteny nadawczej na maszcie, który umożliwia zmianę jej wysokości w zakresie od H_{min} do H_{max}. Łączy się ją z odbiornikiem pomiarowym lub z analizatorem widma za pomocą kabla pomiarowego odpowiedniej długości. Polaryzację anteny odbiorczej ustawia się odpowiednio do polaryzacji anteny nadawczej, po dostrojeniu jej do długości rezonan-

sowej. W przypadku strojonego dipola o polaryzacji pionowej między ziemią i końcem dolnego ramienia anteny należy zachować prześwit 25 cm.

- **Przebieg pomiarów**

Pomiary przeprowadza się najpierw dla anten spolaryzowanych poziomo, a następnie dla spolaryzowanych pionowo, po umieszczeniu anteny nadawczej na wysokości h. W trakcie pomiarów należy kolejno wykonać niżej podane czynności.

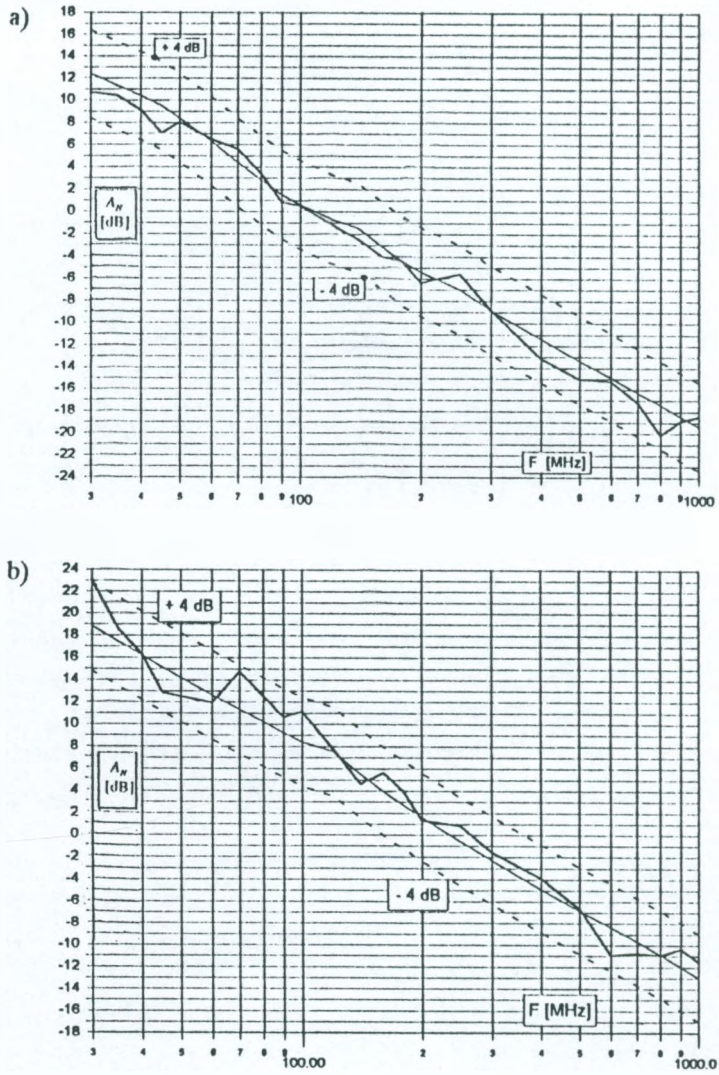
1. Wyregulować poziom wyjściowy generatora sygnałowego tak, aby otrzymać wskazania powyżej poziomu tła sygnałów obcych lub szumów własnych odbiornika pomiarowego względnie analizatora widma.
2. Zmieniać wysokość anteny odbiorczej H w zakresie od 1 m do 4 m.
3. Zanotować maksymalne wskazania odbiornika pomiarowego. Jest to wartość V_R' wstawiana do równania (5).
4. Odłączyć kable pomiarowe od anteny nadawczej i anteny odbiorczej. Połączyć je bezpośrednio, stosując odpowiednie złącze.
5. Zanotować poziom sygnału odpowiadający bezpośredniemu połączeniu kabli. Jest to wartość V_R występująca w równaniu (5).
6. Dla każdej częstotliwości i każdej polaryzacji wykonać czynności podane w pkt. 3 i 5, a uzyskane wyniki pomiarów wstawić do równania (5).
7. Wstawić do równania (2) wartości współczynników antenowych anteny nadawczej (AF_1) i anteny odbiorczej (AF_2), odpowiadające określonej częstotliwości pomiarowej.
8. Uwzględnić współczynnik korekcyjny wzajemnej impedancji Q (por. tabl. 4), który stosuje się tylko dla określonej geometrii przy polaryzacji poziomej strojonych dipoli umieszczonych w odległości 3 m; $Q = 0$ dla wszystkich pozostałych geometrii.
9. Rozwiązać równanie (5), wyznaczając wartość A_N dla określonej częstotliwości i określonej polaryzacji.

10. Odjąć wartości wyznaczone w pkt. 9 od wartości teoretycznej NSA, podanej w [8].
11. Sprawdzić, czy wartości wyznaczone w pkt. 10 są mniejsze od ±4 dB, jeśli tak, to uważa się, że poligon pomiarowy spełnia wymagania dla danej częstotliwości i danej polaryzacji.
12. Powtórzyć czynności pkt. 1÷11 dla kolejnych częstotliwości, kolejnych polaryzacji anten oraz odległości d.

5. POLIGON POMIAROWY INSTYTUTU ŁĄCZNOŚCI WE WROCŁAWIU

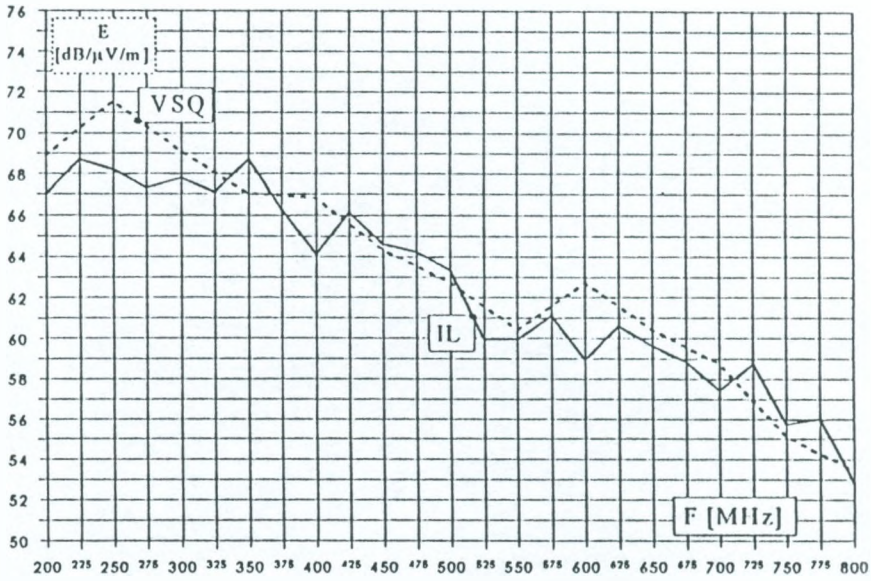
W 1995 r. na terenie posesji Instytutu Łączności we Wrocławiu, przy ul. Swojczyckiej 38, zbudowano otwarty poligon przystosowany do pomiarów natężenia pola zaburzeń radioelektrycznych z odległości 3 m i 10 m. Poligon ten odpowiada kryteriom ustalonym w publikacji CISPR nr 16-1:1993 (i równoważnej jej normie PrPN-CISPR 16-1). Różnica między zmierzoną wartością współczynnika A_N a jego wartością teoretyczną jest mniejsza od ±4 dB dla obu odległości pomiarowych (3 m i 10 m) i obu polaryzacji mierzonego pola (poziomej i pionowej). Na rys. 4 przedstawiono wyniki pomiarów współczynnika A_N dla polaryzacji pionowej, jako bardziej krytycznej. Obok wyników pomiarowych pokazano granice teoretycznej wartości współczynnika tłumienia poligonu pomiarowego A_N dla nominalnych odległości 3 m i 10 m. Dane wzięto z publikacji nr 16 CISPR [8]. Potwierdzeniem poprawności pola pomiarowego są wyniki pomiarów natężenia pola wzorcowego źródła zaburzeń (por. rys. 5).

Poligon pomiarowy został zbudowany na terenie otwartym, w pobliżu ruchliwej drogi, ale jest osłonięty od niej budynkiem. Dzięki temu uzyskano dość niski poziom tła zaburzeń przemysłowych (pochodzących głównie od układów zapłonowych przejeżdżających samochodów), rzędu 20 dB(μV/m). Tak niski poziom tła zaburzeń



Rys. 4. Zmiany współczynnika A_N w funkcji częstotliwości przy polaryzacji pionowej dla poligonu pomiarowego Instytutu Łączności O/Wrocław przy ul. Swojczyckiej we Wrocławiu

a) odległość 3 m; b) odległość 10 m



Rys. 5. Porównanie wyników pomiarów natężenia pola wytwarzanego przez wzorcowe źródło VSQ (certyfikat NAMAS)

VSQ - na poligonie wzorcowym w W. Brytanii, IL - wyniki pomiarów na poligonie pomiarowym Instytutu Łączności O/Wrocław

umożliwia przeprowadzanie pomiarów natężenia pola zaburzeń dla większości urządzeń i ocenę ich zgodności z praktycznie wszystkimi normami obowiązującymi w dziedzinie kompatybilności elektromagnetycznej [5, 18, 19].

Problemem mogą być jedynie sygnały stacji radiowych, telewizyjnych, służb ruchomych i telekomunikacyjnych (np. sygnał sieci CENTERTEL). Są to jednak sygnały wąskopasmowe, dobrze rozróżnialne (każdy miernik zaburzeń ma własny tor nasłuchowy), dzięki czemu ich wpływ na wyniki pomiarów konkretnego źródła zaburzeń może być wyeliminowany.

WYKAZ LITERATURY

1. ANSI C63.7 (1992): Guide for construction of open area test sites for performing radiated emission measurement.
2. Bem D. J.: Anteny i rozchodzenie się fal radiowych. WNT, Warszawa 1973.
3. Bennet W. S.: Error control in radiated emission measurements. EMC Technology, October 1982.
4. Bennet W. S.: Radiated emissions measurement; test site validation. EMC Test&Design, September 1992.
5. CISPR 10 (1990): Limits and methods of measurement of electromagnetic disturbance characteristics of industrial, scientific and medical (ISM) radio-frequency equipment.
6. CISPR 12 (1990): Limits and methods of measurement of radio interference characteristics of vehicles, motor boats and spark-ignited engine-driven devices.
7. CISPR 13 (1990): Limits and methods of measurement of radio interference characteristics of sound and television broadcast receivers and associated equipment.
8. CISPR 16-1 (1993): Specification for radio disturbance and immunity measuring apparatus and methods. Part 1: Radio disturbance and immunity measuring apparatus.
9. CISPR 22 (1993): Limits and methods of measurement of radio interference characteristics of information technology equipments.
10. Dash G., Strauss I.: Studies on the use of wood in open area test sites. IEEE Intern. Symp. on EMC, Seatle, Washington, 1988.
11. DeMarinas J.: Getting better results from an open test site. 8th Intern. Zurich Symp. and Technical Exhibition on EMC, Zurich 1988.
12. DeMarinis J.: Studies relating to the design of open field EMC test sites. IEEE Intern. Symp. on EMC, 1987.
13. DeMarinas J.: The antenna cable as a source of error in EMI measurements. IEEE Intern. Symp. in EMC, 1988.
14. Dołuchanow M. P.: Rozchodzenie się fal radiowych, PWN, Warszawa 1965.

15. Heirman D. N.: Investigating open area test site measurement. 7th Intern. Zurich Symp. and Techn. Exh. on EMC, Zurich 1987.
16. Heirman D. N.: The open area test site - still key to radiated emission testing. 10th Intern. Zurich Symp. and Techn. Exh. on EMC, Zurich 1993.
17. PrPN-CISPR 16-1: Kompatybilność elektromagnetyczna. Wymagania dla urządzeń i metod pomiarów zaburzeń radioelektrycznych i odporności na zaburzenia. Część 1: Urządzenia do pomiarów zaburzeń i odporności na zaburzenia.
18. PrPN-EN 55013: Kompatybilność elektromagnetyczna. Dopuszczalne poziomy i metody pomiarów zaburzeń elektromagnetycznych odbiorników radiofonicznych i telewizyjnych oraz ich urządzeń dodatkowych.
19. PrPN-EN 55022: Kompatybilność elektromagnetyczna. Dopuszczalne poziomy i metody pomiaru zaburzeń radioelektrycznych wytwarzanych przez urządzenia informatyczne.

Мирослав Петраник

ОТКРЫТЫЙ ПОЛИГОН ДЛЯ ИЗМЕРЕНИЯ НАПРЯЖЕННОСТИ ЭЛЕКТРОМАГНИТНОГО ПОЛЯ

Резюме

В статье дан краткий очерк открытого полигона используемого для измерения напряженности поля радиопомех согласно требованиям международных стандаратов МЭК. Описаны основные параметры полигона и методы их проверки с точки зрения правильности его постройки. Оговорены тоже эти элементы конструкции полигона которые влияют на его параметры. Среди них особенно нужно обратить внимание на место постройки полигона с учетом его эксплуатационной удобности расположением в близи лаборатории, наружными помехами и стоимости его постройки. Полигон Вроцлавского Отделения Института Связи выполняет требования стандарта СИСПР

16-1. В статье находятся итоговые результаты измерения подтверждающие правильноть этого полигона.

Mirosław Pietranik

OPEN TEST SITE USED IN EMC MEASUREMENTS

Summary

Paper gives short description of the open test site (OTS) used in measurement of the RFI emission according to the IEC and EN standards. The OTS built in the Institute of Telecommunications (Wroclaw Branch) fulfils the CISPR Publication 16-1 requirements. The paper gives some remarks concerning the basic requirements which OTS shall fulfil, the methods used to check the constructional correctness of the OTS, influences of the different constructional elements of the OTS such as localisation of the OTS, quality of the ground plane (sizes and roughness), external interference, accessories used during measurement, such as turntable, antenna, weather protection, etc.

Mirosław Pietranik

LE POLYGONE POUR MESURER L'INTENSITE DE LA PERTURBATION RADIOELECTRIQUE

Résumé

L'article présente les exigences de base pour un polygone utilisé pour mésurer l'intensité du champ électromagnétique dans le domaine de la compatibilité électromagnétique. Le procédé de la vérification de l'exactitude de construction de ce polygone est démontré ainsi que les remarques concernant les éléments qui décident de la correction du fonctionnement du polygone en question. Les résultats des mésures dans le polygone construit sur le terrain de l'Institute de Télécommunications à Wrocław.

Mirosław Pietranik

TESTPLATZ FÜR EMV-MESSUNGEN

Z u s a m m e n f a s s u n g

Im Beitrag werden wesentliche Anforderungen behandelt, die ein Testplatz für Messen der elektromagnetischen Feldstärke im EMV-Prüfungen erfüllen soll. Es wird Methode des Testen von Konstruktionskorrektheit beschrieben und auf für diese Korrektheit entscheidende Bausteine eingegangen. Meßergebnisse für den Testplatz, der auf dem Gelände der Institut für Fernmeldewesen in Wrocław erbaut wurde, werden vorgelegt.

AUTORZY

Dr inż. Elżbieta Andrukiewicz urodziła się w 1959 r. w Warszawie. W 1983 r. ukończyła studia na Wydziale Elektroniki Politechniki Warszawskiej, uzyskując tytuł magistra inżyniera telekomunikacji. W latach 1983-90 pracowała w Instytucie Łączności w Zakładzie Teletransmisji, zajmując się zagadnieniami związanymi z cyfrowymi urządzeniami teletransmisyjnymi. W 1987 r. uzyskała tytuł doktora nauk technicznych. Od 1991 r. jest członkiem Rady Naukowej Instytutu Łączności. Od 1997 r. pracuje w Instytucie Łączności, pełniąc funkcję zastępcy kierownika Samodzielnej Pracowni Zarządzania Siecią Komputerową IŁ. Zajmuje się zagadnieniami związanymi z zabezpieczaniem systemów informatycznych. Jest autorką licznych publikacji z tej dziedziny, a także ekspertem ISO w podkomitecie SC27/WG1 "Requirements, security services and guidelines".

Profesor dr hab. inż. Andrzej Wierzbicki urodził się 29 czerwca 1937 r. w Warszawie. W 1960 r. ukończył studia na Wydziale Łączności Politechniki Warszawskiej. Tam w 1964 r. uzyskał stopień doktora, a w 1968 r. doktora habilitowanego. W 1976 r. otrzymał tytuł profesora. Specjalizował się w modelowaniu i analizie wrażliwości systemów dynamicznych, teorii i metodach obliczeniowych optymalizacji - zwłaszcza nieliniowej, dynamicznej,

wielokryterialnej, komputerowym wspomaganiu decyzji, teorii gier i technikach negocjacji, cywilizacyjnych aspektach ery informacyjnej. Obecnie jest dyrektorem Instytutu Łączności w Warszawie. Jest przewodniczącym rad naukowych Przemysłowego Instytutu Automatyki i Pomiarów oraz Naukowej Akademickiej Sieci Komputerowej, członkiem Komitetu Automatyki i Robotyki oraz Komitetu Prognoz "Polska w XXI w." PAN. W latach 1975-78 był dziekanem Wydziału Elektroniki Politechniki Warszawskiej, w latach 1978-84 kierownikiem Działu Teorii Systemów i Decyzji Międzynarodowego Instytutu Stosowanej Analizy Systemowej (IIASA) w Laxenburgu k. Wiednia. W latach 1991-92 został wybrany członkiem Komitetu Badań Naukowych i przewodniczącym Komisji Badań Stosowanych KBN. W latach 1970-71 był profesorem wizytującym na Uniwersytecie Minnesota i Uniwersytecie Browna w St. Zjedn. AP, w latach 1989-90 profesorem Uniwersytetu Kioto w Japonii. W 1992 r. uzyskał nagrodę Georg Cantor Award Międzynarodowego Towarzystwa Wielokryterialnej Analizy Decyzji (IS MCDM). Jest autorem ponad 150 publikacji naukowych, w tym 10 książek.

Doc. dr inż. Arnold Kawecki - notkę biograficzną wydrukowano w *Pracach Instytutu Łączności*, nr 102, 1994.

Dr inż. Mirosław Pietranik - notkę biograficzną wydrukowano w *Pracach Instytutu Łączności*, nr 105, 1995.