

MINISTERSTWO ŁĄCZNOŚCI

---

BIBLIOTEKA  
Instytutu Łączności  
Nr \_\_\_\_\_

PRACE  
INSTYTUTU ŁĄCZNOŚCI

NR 97

WARSZAWA 1990

---

INSTYTUT ŁĄCZNOŚCI

## SPIS TREŚCI

1. Stanisław Miszczak, Andrzej Zieliński - Wspomnienie o Profesorze Stanisławie Dymowskim .....	3
2. Elżbieta Andrukiewicz - Protokoły kryptograficzne w sieciach teleinformatycznych .....	11
3. Zbigniew Kowalski (Habdank) - Analiza właściwości zmodyfikowanej tłumienności odniesienia .....	37
4. Jan Bogucki - Niejednorodne linie transmisyjne z rozkładem wykładniczym cosinus-kwadrat i parabolicznym ..	93
5. Ryszard Klimkiewicz, Piotr Tyrawa - Badania charakterystyk promieniowania anten pomiarowych zainstalowanych na śmigłowcu .....	103

## СОДЕРЖАНИЕ

1. Stanisław Miszczak, Andrzej Zieliński - Wspomnienie o Profesorze Stanisławie Dymowskim .....	3
2. Эльжбета Андрукевич - Криптографические протоколы в телеинформатических сетях .....	11
3. Збигнев Ковальски /Хабдank/ - Анализ свойств модифицированного относительного эквивалента затухания..	37
4. Ян Богущки - Неоднородные передающие линии с экспонентной косинус-квадрат и параболической характеристикой .....	93
5. Рышард Климкевич, Петр Тырава - Измерение характеристик направленности измерительных антенн установленных на вертолете .....	103

## CONTENS

1. Stanisław Miszczak, Andrzej Zieliński - Wspomnienie o Profesorze Stanisławie Dymowskim .....	3
2. Elżbieta Andrukiewicz - The cryptographic protocols in computer networks .....	11
3. Zbigniew Kowalski (Habdank) - Analysis of loudness rating attributes .....	37
4. Jan Bogucki - Nonuniform transmission lines with exponential cosine-squared and parabolic tapers .....	93

MINISTERSTWO ŁĄCZNOŚCI

---

BIBLIOTEKA  
Instytutu Łączności  
Nr \_\_\_\_\_

PRACE  
INSTYTUTU ŁĄCZNOŚCI

NR 97

WARSZAWA 1990

---

INSTYTUT ŁĄCZNOŚCI

Komitet Redakcyjny

Redaktor Naczelny - dr inż. Krystyn Plewko  
Z-ca Redaktora Naczelnego - doc. dr inż. Stanisław Sońta

Redaktorzy działów:

doc. dr inż. Alina Karwowska-Lamparska,  
mgr inż. Mirosław Żurawski

Adres Redakcji:

Instytut Łączności, 04-894 Warszawa-Miedzeszyn, ul. Szachowa 1

Copyright by Instytut Łączności, Warszawa 1990

ISSN 0020-451X

Wydawnictwo nieperiodyczne

Redaktor - mgr Krystyna Juskiewicz

Montaż tekstu - techn. Grażyna Woźnica



WSPOMNIENIE O PROFESORZE  
STANISŁAWIE DYMOWSKIM

W dniu 9 listopada 1988 roku w pełnym rozkwicie sił twórczych zmarł w Warszawie prof. dr hab. inż. Stanisław Dymowski, jeden z czołowych przedstawicieli współczesnego pokolenia polskiej telekomunikacji, znakomity uczony, człowiek niezwykle prawy i szlachetny, zafascynowany dziedziną, której poświęcił się z wielkim oddaniem, wnosząc w jej rozwój znaczący wkład, zwłaszcza w zakresie syntezy liniowych układów elektrycznych, teorii informacji, teorii sygnałów dyskretnych oraz zagadnień systemowych i konstrukcyjnych sieci teleinformatycznych. Miał 52 lata, gdy nagle ujawniona straszna i nieuleczalna choroba w ciągu kilku miesięcy przecięła pasmo jego życia.

Stanisław Dymowski urodził się w Warszawie 8 grudnia 1936 r. w rodzinie inteligenckiej o głębokich tradycjach patriotycznych i czynnym zaangażowaniu w walki niepodległościowe narodu polskiego. Dziadek jego, Brunon Dymowski, zmarły 1 kwietnia 1928 r., był uczestnikiem powstania styczniowego i został pochowany na cmentarzu rzymsko-katolickim w Lublinie w grobie powstańców z 1863 r. Ojciec, Kamil Dymowski, służył w wojsku powstańczym na Śląsku, a następnie - po

ukończeniu Korpusu Kadetów w Modlinie i Wydziału Chemii na Uniwersytecie Poznańskim - był zawodowym oficerem Wojska Polskiego w randze kapitana. Zginął w 1939 r., mając 37 lat. Matka, doc. dr hab. Zofia Dymowska, z domu Leźnicka, jest mikrobiologiem, dziś na emeryturze. Przez kilka dziesięcioleci pracowała w Państwowym Zakładzie Higieny w Warszawie, kierując Zakładem Parazytologii Lekarskiej. Po śmierci męża na jej barkach spoczywało wychowanie nieletnich dzieci, syna Stanisława i córki Barbary, dziś uznanego lekarza. Wychowała ich na szczerych patriotów, skromnych i pracowitych członków społeczeństwa.

Z prof. Dymowskim łączyła nas serdeczna przyjaźń.

Stanisław Dymowski, po uzyskaniu w 1954 roku świadectwa dojrzałości w warszawskim Liceum Ogólnokształcącym im. Józefa Poniatowskiego z oceną ogólną bardzo dobrą, podjął studia na Wydziale Łączności Politechniki Warszawskiej, na której 15 marca 1960 roku uzyskał dyplom magistra inżyniera łączności, również z ogólną oceną bardzo dobrą. Na tymże Wydziale doktoryzował się w 1965 roku na podstawie rozprawy pt. "Probabilistyczna analiza pewnych charakterystyk liniowych układów elektrycznych". W siedem lat później Rada Wydziału Elektroniki PW nadała mu stopień naukowy doktora habilitowanego na podstawie rozprawy pt. "O teorii syntezy liniowych pasywnych czwórników RC w strukturach kanonicznych".

Pracę zawodową rozpoczął, będąc jeszcze studentem, w 1957 roku w Katedrze Telegrafii Wydziału Łączności PW, najpierw na stanowisku młodszego asystenta, a następnie asystenta. 1 lutego 1961 roku przeniósł się do Zakładu Teorii Obwodów w Katedrze Podstaw Telekomunikacji PW, awansując na stanowisko starszego asystenta, a następnie adiunkta (1 marca 1966 r.). W latach 1961-1963 związany był równolegle z Katedrą Radiotechniki PW. 1 grudnia 1972 r. został powołany na stanowisko docenta, a 1 października 1973 r. Rektor PW powierzył mu funkcję kierownika Zakładu Teorii Obwodów w Instytucie Podstaw Elektroniki PW.

W rok później przeszedł do pracy w Instytucie Łączności, pozostając na Politechnice Warszawskiej na pół etatu (do

30 września 1981 r.). W Instytucie Łączności pracował do chwili swej przedwczesnej śmierci, pełniąc w tej czołowej placówce polskiej telekomunikacji szereg odpowiedzialnych funkcji. Przez pięć lat kierował Zakładem Transmisji Danych, dużym pięćdziesięcioosobowym zakładem naukowo-badawczym, przemianowanym w 1975 r. w Zakład Teleinformatyki. Równolegle był m.in. koordynatorem prac naukowo-badawczych w ramach problemu węzłowego "Rozwój jednolitej sieci telekomunikacyjnej państwa - systemy i urządzenia" oraz kierownikiem dwóch tematów: "Opracowanie, opanowanie produkcji i wprowadzenie do eksploatacji nowoczesnych systemów transmisji danych", "Budowa eksperymentalnego systemu pilotowego krajowej sieci transmisji danych", a następnie od 1976 r. również kierownikiem tematu "Systemy, urządzenia i sieci teleinformatyczne". Szczególnie dużo uwagi poświęcił tzw. magistrali teleinformatycznej. Była to doświadczalna sieć teleinformatyczna z komutacją pakietów z trzema węzłami komutacyjnymi w Warszawie (It), w Gdańsku i Katowicach. W związku z tym zagadnieniem oraz innymi, nie wymienionymi tu tematami prowadzonymi w kierowanym przez Niego zakładzie miał okazję nawiązać współpracę z Międzynarodowym Instytutem Stosowanych Badań Systemowych (IISAS) w Wiedniu oraz kontakty naukowe z Wyższym Instytutem Poczty i Telekomunikacji (ITSPA) w Rzymie, Państwowym Centrum Telekomunikacji (CNET) w Paryżu, oraz wieloma placówkami w Szwajcarii i Wielkiej Brytanii.

W styczniu 1980 roku objął w Instytucie Łączności funkcję pełnomocnika dyrektora ds. badań podstawowych i rozwoju kadry naukowej. Oprócz tych funkcji był w latach 1976-1980 kierownikiem Zespołu Koordynacyjnego "Transmisji Danych" w Komisji Naukowej ds. CCITT, jak również stałym przewodniczącym zespołu resortu łączności w Radzie Specjalistów Nr 7 Jednolitego Systemu Elektronicznych Maszyn Cyfrowych. Ponadto od 1976 roku brał czynny udział w pracach Sekcji Sieci Komputerowych Komitetu Informatyki PAN oraz w szeregu innych gremiach, m.in. w Stałej Komisji Łączności RWPG i różnych

Kolegiach Redakcyjnych, w tym przez kilka lat w Kolegium Redakcyjnym Przeglądu Telekomunikacyjnego. Na początku lat osiemdziesiątych został wybrany członkiem korespondentem Towarzystwa Naukowego Warszawskiego. W dniu 26 września 1985 roku Rada Państwa nadała mu tytuł naukowy profesora nadzwyczajnego nauk technicznych. Przez ostatnie dwa lata piastował stanowisko Sekretarza Naukowego Instytutu Łączności, będąc równocześnie wiceprzewodniczącym Rady Naukowej Ił.

W ciągu blisko trzydziestu lat swej działalności naukowej opublikował kilkadziesiąt prac. Są to prace oryginalne, będące rezultatem jego własnych dociekań teoretycznych i przeprowadzonych doświadczeń laboratoryjnych. Zamieszczał je w czołowych czasopismach naukowych w dziedzinie elektrotechniki teoretycznej, w tym głównie w Rozprawach Elektrotechniki PAN i Archiwum Elektrotechniki PAN. Tematyka tych publikacji jest odbiciem ewolucji jego zainteresowań naukowych w szeroko pojętym obszarze telekomunikacji.

W latach sześćdziesiątych opublikował m.in. następujące prace: "Widma Fouriera funkcji okresowych i funkcji okresowych w skończonym przedziale czasu" (1965), "O pewnej metodzie określenia korekcji próbek ergodycznego procesu stochastycznego" (1967) oraz "O pewnym przypadku realizacji dopasowanego falowo liniowego czwórnik RLC o bezzerowej funkcji przenoszenia" (1969). W latach siedemdziesiątych ukazała się m.in. jego praca pt. "Funkcje modulujące przebiegi elektryczne i niektóre ich właściwości" (1970), będąca oryginalną propozycją zdefiniowania unormowanej, liniowej przestrzeni funkcyjnej wszelkich modeli sygnałów elektrycznych przy przyjęciu jako normy w tej przestrzeni wielkości równoważnej wartości skutecznej sygnałów elektrycznych, a także napisana wspólnie z dr R.M. Biernackim praca pt. "Związek warunków Raisbecka i warunki residuów dla liniowych trójników RC" (1979).

Z lat osiemdziesiątych pochodzą m.in. następujące jego prace: "O pewnym przedstawieniu i właściwościach widma gęstości energii i funkcji autokorelacji przypadkowych sygnału dyskretnego" (1980), "Przekształcenia transmisyjne pierwszego



rzędu przypadkowych sygnałów dyskretnych" (1981), "Monofunkcyjne przekształcenia transmisyjne pierwszego rzędu przypadkowych sygnałów binarnych" (1981), "Przekształcenia transmisyjne p-tego rzędu przypadkowych sygnałów dyskretnych" (1981), "Częstotliwościowa dystrybuanta energetyczna przypadkowego sygnału dyskretnego" (1981) oraz "Modele matematyczne sygnałów izochronicznych generowanych przez terminale danych" (1982). Jest też współautorem zbiorowego dzieła pt. "Mathematik Handbuch für Technik und Naturwissenschaft" (Verlag Harri Deutsch, Zurich - Frankfurt a. Main, 1975). Wiele swoich prac prezentował na forum międzynarodowym. Należy do nich m.in. praca pt. "RC two-ports synthesis in canonical structures" (Proceedings of the Summer School on Circuits Theory, Prague 1974).

Znaczące pozycje w jego dorobku naukowym stanowią również niepublikowane rozprawy teoretyczne zrealizowane na zamówienie wojskowych placówek naukowych. Pierwsze jego prace dla potrzeb wojska pochodzą z początku lat sześćdziesiątych, ostatnie zaś z końca pierwszej połowy lat osiemdziesiątych.

W swoich pracach teoretycznych koncentrował się także na zagadnieniach teorii sygnałów, a w szczególności na metodach takiego przekształcania sygnałów cyfrowych, które umożliwiają optymalne dopasowanie transmitowanych sygnałów do kanału przesyłowego. Znajdował również czas na przyswojenie polskim specjalistom kilku znanych pozycji z literatury obcej. Był m.in. tłumaczem obszernej książki S. Mitra "Analysis and Synthesis of Linear Active Networks", która ukazała się nakładem WNT w 1974 r. pt. "Analiza i synteza układów aktywnych liniowych", dwóch kilkusetstronicowych prac D.N. Chorafasa "Statistical Processes and Reliability Engineering" (wydanie polskie: "Procesy statystyczne i niezawodność urządzeń". WNT, 1964) oraz C.W. Helstroma "Statistical of Signal Detection" (wydanie polskie: "Statystyczna teoria detekcji". WNT, 1964).

Integralnym nurtem działalności naukowej prof. Dymowskiego były zajęcia dydaktyczne, do których przywiązywał ogromną

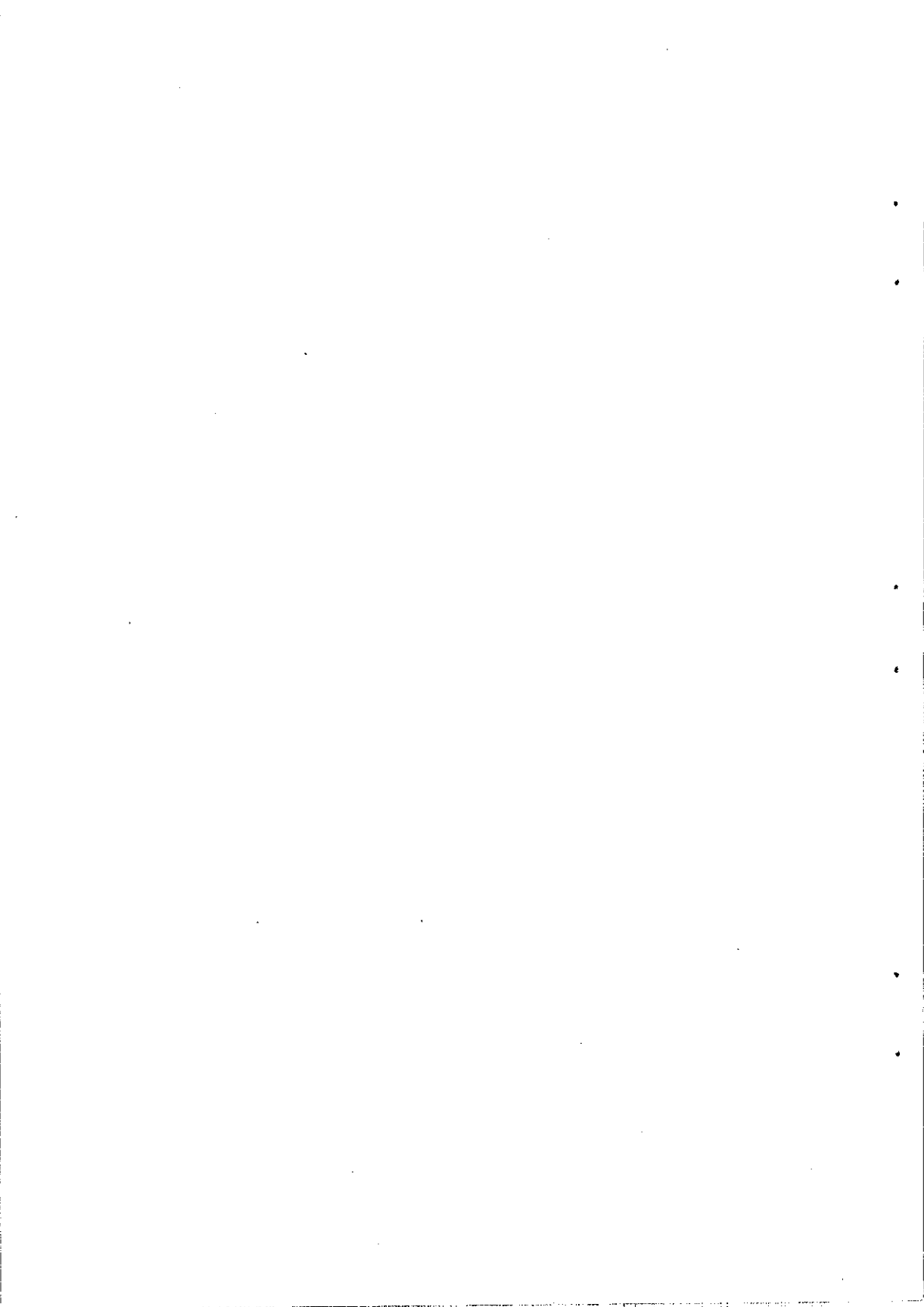
wagę. Prowadził je od 1960 roku do niemal ostatnich chwil swego życia. Był znanym i szanowanym wychowawcą wielu roczników inżynierów elektroników. Zajęcia dydaktyczne prowadził z podstawowych przedmiotów teoretycznych dla studentów Wydziału Łączności, a następnie Wydziału Elektroniki PW. Wykładał m.in. "Teorię obwodów", "Podstawy elektrotechniki teoretycznej" oraz "Teorię sygnałów i informacji". W swej pracy dydaktyczno-wychowawczej kładł zawsze nacisk na odpowiednią inżynierską interpretację omawianych zjawisk w wykładanych przedmiotach tematycznych. Stąd wynikało Jego ciągłe dążenie do modernizacji ujęcia wykładanych przedmiotów i bardzo aktywny udział w pracach, dotyczących modernizacji nauczania na Wydziale Elektroniki PW. Między innymi był inicjatorem organizacji laboratorium, ilustrującego podstawowe prawa teorii obwodów i w sposób ciągły modernizował metody prowadzenia ćwiczeń audytoryjnych, ilustrujących wykładane przez siebie przedmioty. Dydaktyce służyły również przygotowane przez Niego skrypty. Opracował m.in. pierwszy w Polsce skrypt z teorii informacji, wydany przez Politechnikę Warszawską pt. "Elementy teorii informacji" (1968 r.). Skrypt ten był trzykrotnie wznawiany i w zasadzie do 1976 roku stanowił podstawową pomoc naukową dla studentów Wydziału Elektroniki PW w zakresie przedmiotów "Teoria informacji" oraz "Teoria sygnałów i informacji". Również inny, opracowany przez Niego skrypt pt. "Zadania z teorii obwodów" był kilkakrotnie wznawiany.

W ostatnich kilku latach swej działalności dydaktyczno-wychowawczej opiekował się przede wszystkim dyplomantami i doktorantami Instytutu Telekomunikacji PW. Pod Jego kierunkiem jako promotora uzyskało stopnie doktora nauk technicznych kilku specjalistów z zakresu telekomunikacji. Ponadto był opiniodawcą kilkunastu rozpraw doktorskich i habilitacyjnych. Ze względu na swą aktywną postawę w stosunku do kształcenia młodej kadry naukowej, w Radzie Naukowej Instytutu Łączności pełnił od 1975 roku funkcję zastępcy przewodniczącego Komisji ds. Doktorskich, jak również uczestniczył w pracach Komisji Doktorskich powołowanych przez Radę Wydziału Elektroniki PW.

Za swą działalność dydaktyczno-wychowawczą oraz osiągnięcia w pracy naukowo-badawczej został wielokrotnie wyróżniany nagrodami Rektora Politechniki Warszawskiej, Ministra Łączności i Ministra Obrony Narodowej oraz Ministra Nauki, Szkolnictwa Wyższego i Techniki.

Śmierć prof. Stanisława Dymowskiego stanowi bolesną stratę dla polskiej telekomunikacji, a dla Jego bliskich kolegów i przyjaciół głęboki cios. Zachowamy Go na zawsze w naszej serdecznej pamięci.

prof. dr hab. inż. Stanisław Miszczak  
prof. dr inż. Andrzej Zieliński



Elżbieta Andrukiewicz

621.394.9

## PROTOKOŁY KRYPTOGRAFICZNE W SIECIACH TELEINFORMATYCZNYCH

Rękopis dostarczono do Komitetu Redakcyjnego dn. 1989.02.08

Zaprezentowano formalny opis protokołu kryptograficznego oparty na teorii języków i automatów liniowo ograniczonych. Stworzono język liniowo ograniczony, który definiuje protokół kryptograficzny. Dwa przekształcenia na językach - odwzorowania porządkujące i redukujące - umożliwiają sformułowanie prostego kryterium bezpieczeństwa protokołu kryptograficznego (Definicja 4). Zaproponowano klasyfikację opartą na typach relacji panujących między użytkownikami w sieci. Zastosowanie kryterium bezpieczeństwa do protokołów różnych grup zilustrowano licznymi przykładami. Dowiedziono ścisłej zależności między relacjami zachodzącymi w sieci a bezpieczeństwem protokołów kryptograficznych.

### 1. WPROWADZENIE

Rozwój sieci teleinformatycznych spowodował wzrost zainteresowania kryptografią - gałęzią wiedzy o sposobach utajniania informacji. Jednakże, specyfika sieci komputerowych obsługujących wielką liczbę użytkowników praktycznie uniemożliwia stosowanie tradycyjnych metod kryptograficznych. Nierealne stało się wyposażenie każdej potencjalnej pary nadawca - odbiorca w identyczne słowo - "klucz", służące do kodowania i dekodowania przesyłanych między nimi wiadomości (było to podstawowe wymaganie konwencjonalnej kryptografii).

W tych warunkach jedynym rozwiązaniem jest zastosowanie kryptografii publicznego klucza (ang. public-key cryptography). Kryptografia publicznego klucza zakłada istnienie pary kluczy, z której jeden - zwany publicznym (ogólnie dostępny w sieci) - służy do kodowania wiadomości, a drugi prywatny (znany tylko odbiorcy) - do dekodowania wiadomości.

Dystrybucja kluczy, tak uciążliwa w przypadku konwencjonalnej kryptografii, w przypadku kryptografii publicznego klucza ogranicza się do publikowania aktualnych spisów jawnych kluczy. Zasady kryptografii publicznego klucza sformułowano po raz pierwszy w [7].

Nie wdając się w szczegółowe rozważania na temat sposobu realizacji magazynu dystrybucji publicznych kluczy (szczegóły można znaleźć np. w [9]), przyjmuję, że wszystkie omawiane protokoły oparte są na tym modelu kryptograficznym.

Jakkolwiek kryptografia publicznego klucza eliminuje problem dystrybucji kluczy, pozostaje jednak zagadnienie, jak zapewnić autentyczność przesyłanych w sposób jawny kluczy. A zatem, samo kodowanie (utajnianie przesyłanych danych) nie stanowi warunku wystarczającego w systemach ochrony danych w sieciach teleinformatycznych; uwierzytelnienie kluczy i użytkowników, czyli zapewnienie autentyczności komunikacji, jest równie ważnym zadaniem takich systemów.

Procedury komunikacji w sieci powinny zapewnić zarówno uwierzytelnienie użytkowników i kluczy, jak tajność i integralność przesyłanych wiadomości.

Protokół kryptograficzny - zbiór reguł wymiany wiadomości między użytkownikami sieci - jest podstawą systemu ochrony danych w sieciach teleinformatycznych.

Przedmiotem dalszych rozważań będzie zagadnienie konstrukcji poprawnych matematycznie protokołów kryptograficznych. Formalny opis protokołów stanowi podstawę do analizy ich bezpieczeństwa w sieci (skuteczności ochrony przesyłanych w sieci danych).

## 2. PROTOKÓŁ KRYPTOGRAFICZNY I JEGO ŚRODOWISKO

Podstawowym założeniem, w rozważaniach na temat protokołów wymiany informacji, jest pewność samej metody kryptograficznej. Oznacza to, że nie ma możliwości poznania przesyłanej wiadomości drogą klasycznej kryptoanalizy szyfru. Jednakże, zastosowanie metod kryptograficznych w nowym środowisku, ja-

kim jest wielka sieć publiczna, stwarza nowe zagrożenia dla bezpieczeństwa prokołów.

Drugim założeniem jest publiczność sieci zapewniająca każdemu użytkownikowi swobodny dostęp do kanału i znajomość wszystkich informacji krążących w sieci w sposób jawny (w szczególności, publicznych kluczy).

Trzecie podstawowe założenie dotyczy istnienia przeciwnika - osoby, której cel stanowi złamanie protokołu. Jest to tzw. "przeciwnik aktywny", posiadający nie tylko bierny dostęp do przesyłanej w kanale (zakodowanej) wiadomości, ale dysponujący możliwościami znacznej ingerencji w postać wiadomości (może to być użytkownik sieci).

Biorąc pod uwagę powyższe założenia oraz specyfikę struktur protokołów, zagrożenia bezpieczeństwa protokołów można podzielić na zewnętrzne i wewnętrzne.

Zewnętrzne zagrożenia wynikają z zasad przepływu informacji w sieci. Wśród najważniejszych problemów konstrukcji systemu ochrony można wyróżnić: zagadnienie dystrybucji klucza (zarówno w systemach publicznego klucza, jak i dla protokołów z konwencjonalną kryptografią), przeciwdziałanie fałszerstwu publicznych kluczy oraz utracie prywatnego klucza, możliwości tworzenia pozaprotokolarnych związków między stronami protokołu. Problemy zewnętrznych zagrożeń są omawiane szczegółowo np. w [3], [9].

Zagrożenia wewnętrzne wynikają z samej struktury protokołu oraz relacji panujących pomiędzy użytkownikami sieci. Problemy te stanowią zasadniczy temat artykułu.

### 3. BUDOWA PROTOKOŁU

Formalny opis protokołu oparty jest na teorii automatów i języków liniowo ograniczonych<sup>1)</sup>. Tutaj zostanie przedstawiona tylko ogólna koncepcja budowy protokołu oraz formalnej analizy jego bezpieczeństwa. Całość omówiono w pracy [2].

1) Zarys teorii języków i automatów w ujęciu pracy [4] stanowi podstawę opisu protokołu kryptograficznego.

U podstawy definicji protokołu kryptograficznego leżą wnioski dotyczące samego przekształcenia kryptograficznego. Przekształcenie takie można zdefiniować jako podstawienie, dokonane na języku określonym jako język wiadomości. Klasa języków generowana przez to podstawienie jest ograniczona do klasy języków jednoelementowych. Z własności takiej klasy języków wynika, że jest ona zamknięta ze względu na operację złożenia języków (konkatenację). Fakt ten otwiera możliwość formalnego opisu ciągów przekształceń podstawiających języków, jakimi są protokoły kryptograficzne - dane podstawienie  $f$ , które tworzy słowo kodowe  $f(M)$  (gdzie  $M$  jest językiem wiadomości), jest symbolem nowego alfabetu  $\Sigma$ . Można zatem stwierdzić, że wszystkie symbole podstawień kodujących i dekodujących tworzą alfabet  $\Sigma$ . Słowa budowane nad tym alfabetem wyrażają złożenie podstawień dokonane na rzeczywistym słowie wiadomości. Dodatkowo, alfabet  $\Sigma$  zawiera symbole jawnych operacji składania słów języka wiadomości. Omawiana klasa języków jednoelementowych jest zamknięta ze względu na te przekształcenia.

Ważnym elementem określonego w ten sposób języka symbolicznego jest słowo puste - oznaczane symbolem  $\emptyset$ . Odpowiada on złożeniu przekształcenia kodującego i dekodującego dokonanego na języku wiadomości, równoważnemu przekształceniu tożsamościowemu na tym języku.

Na wstępie zdefiniuję dwa, istotne dla formalnego opisu protokołu, przekształcenia dokonywane na językach.

DEFINICJA 1. Określam alfabety:

$$V = \{a_1, \dots, a_n\}, \quad \bar{V} = \{\bar{a}_1 : a_1 \in V\}$$

$$\bar{V} \cup V = \Sigma \quad \bar{V} \cap V = \emptyset$$

Dla każdego słowa  $w \in \Sigma^*$ ,  $w = a_1 \dots a_n$  istnieje podstawienie porządkujące  $\pi$ :

$$\pi: \Sigma^* \rightarrow \Sigma^*$$



$$\mathcal{T}(a_k) = \begin{cases} \hat{a}_{k-1}, & \text{jeśli } \hat{a}_{k-1} \in w \ \& \ \hat{a}_{k-1} = a_r, \mathcal{T}(a_r) = a_k, k \leq r \leq l \\ a_k, & \text{jeśli } \hat{a}_{k-1} \notin w \end{cases}$$

$$\hat{a}_{k-1} = \begin{cases} \bar{a}_{k-1} & \text{jeśli } a_{k-1} \in V \\ a_{k-1} & \text{jeśli } a_{k-1} \in \bar{V} \end{cases}$$

Podstawienie  $\mathcal{T}$  jest homomorfizmem, zatem:

$$\mathcal{T}(w) = \mathcal{T}(a_1 a_2 \dots a_n) = \mathcal{T}(a_1) \mathcal{T}(a_2) \dots \mathcal{T}(a_n)$$

Podstawienie  $\mathcal{T}$  dokonane na języku  $L$  definiuje nowy język, składający się z uporządkowanych słów:

$$\mathcal{T}(L) = \{ z : z = \mathcal{T}(w) \ \& \ w \in L \}$$

Drugim, niezwykle przydatnym przekształceniem dokonywanym na językach jest przekształcenie redukujące:

DEFINICJA 2. Rozważam te same alfabety  $V$  i  $\bar{V}$ .

Definiuję relację redukującą:

$$a_i \bar{a}_i = \emptyset \quad \text{dla każdego } a_i \in V.$$

Odwzorowanie  $\Gamma$

$$\Gamma: \Sigma^* \rightarrow \Sigma^*$$

takie, że:

$$\Gamma(\emptyset) = \emptyset$$

$$\Gamma(wa_i) = \begin{cases} \Gamma(w)a_i, & \text{jeśli } w \neq w_1\bar{a}_i \\ \Gamma(w_1), & \text{jeśli } w = w_1\bar{a}_i \end{cases}$$

$$w_1 \in \Sigma^*$$

$$\Gamma(w\bar{a}_i) = \begin{cases} \Gamma(w)\bar{a}_i, & \text{jeśli } w \neq w_1a_i \\ \Gamma(w_1), & \text{jeśli } w = w_1a_i \end{cases}$$

jest homomorfizmem na zbiorze  $\Sigma^*$ .

Przystępując do formalnej definicji protokołów, określam sieć, w której użytkownicy  $A, B, \dots, Z$  wymieniają między sobą wiadomości, posługując się przekształceniami publicznego klucza. Można zdefiniować zbiory symboli tych przekształceń jako:

$$V = \{d_A, d_B, \dots, d_Z\} \cup \Omega \quad \text{oraz} \quad \bar{V} = \{e_A, e_B, \dots, e_Z\} \cup \bar{\Omega}$$

gdzie:

$e_I$  jest symbolem przekształcenia zwanego kluczem publicznym użytkownika  $I$ ,

$d_I$  jest symbolem prywatnego klucza użytkownika  $I$ ,

$\Omega$  jest zbiorem przekształceń jawnych definiowanych w protokole i należących do grupy przekształceń dekodujących,

$\bar{\Omega}$  jest zbiorem przekształceń jawnych należących do grupy przekształceń kodujących.

Dla przejrzystości opisu przyjmuję, że w każdym protokole uczestniczyć będą, wybrani spośród wszystkich, dwaj użytkownicy oznaczeni literami  $A$  i  $B$ . Mogą oni stosować jedynie własne klucze, a zatem, korzystając z postaci alfabetów podanych wcześniej:

$$V_{AB} = \{d_A, d_B\} \cup \Omega_{AB} \quad \bar{V}_{AB} = \{e_A, e_B\} \cup \bar{\Omega}_{AB}$$

Stroną, która rozpoczyna protokół jest użytkownik A, odpowiadającą - użytkownik B. Korzystając z powyższych oznaczeń, można określić języki, jakimi posługują się w protokole obaj użytkownicy:

DEFINICJA 3. Niech  $L_A$  ( $L_B$ ) jest językiem, który tworzy stronę A (strona B):

$$L_A = \left\{ \alpha_i : \alpha_i \in (\bar{V}_{AB} \cup \{d_A\} \cup \Omega_{AB})^*, i = 1, \dots, t \right\}$$

$$L_B = \left\{ \beta_i : \beta_i \in (\bar{V}_{AB} \cup \{d_B\} \cup \Omega_{AB})^*, i = 1, \dots, t \right\}$$

gdzie:

$t$  i  $t'$  są liczbą słów generowanych przez użytkowników A i B ( $t' = t$  lub  $t' = t-1$ ).

Dwustronnym protokołem kryptograficznym  $T_{AB}$  jest ciąg kolejno tworzonych słów, wymienianych między użytkownikami A i B w skończonej liczbie kroków  $t + t'$ :

$$T_{AB} = \left\{ w_{2i-1} : w_{2i-1} = \Gamma \left[ \Pi \left( \alpha_i \prod_{k=i-1}^1 (\beta_k \alpha_k) \right) \right], i=1, \dots, t \right\} \cup$$

$$\left\{ w_{2i} : w_{2i} = \Gamma \left[ \Pi \left( \prod_{k=i}^1 (\beta_k \alpha_k) \right) \right], i=1, \dots, t \right\}$$

gdzie:

$$\prod_{k=i}^1 (\beta_k \alpha_k) = \beta_i \alpha_i \beta_{i-1} \alpha_{i-1} \dots \beta_1 \alpha_1, \quad \alpha_i \in L_A, \beta_i \in L_B$$

Aby określić bliżej charakter języka otrzymanego przed chwilą, trzeba rozważyć jego przynależność do znanej klasy języków abstrakcyjnych. Ze względu na ogólność definicji należy znaleźć możliwie dużą klasę języków.

**TWIERDZENIE 1.** Język protokołu  $T_{AB}$  należy do klasy języków liniowo ograniczonych.

Ze względu na obszerność dowodu przedstawię tutaj jedynie jego ideę. Cały tok rozumowania zamieszczono w [2]. Aby udowodnić tezę twierdzenia, buduję automat liniowo ograniczony i dowodzę faktu, że język akceptowany przez ten automat jest identyczny z językiem protokołu. W trakcie dowodu, jako twierdzenie pomocnicze, zostało również udowodnione, że przekształcenia porządkujące i redukujące nie wyprowadzają poza klasę języków liniowo ograniczonych.

#### 4. FORMALNE KRYTERIUM BEZPIECZEŃSTWA PROTOKOŁU KRYPTOGRAFICZNEGO

Fakt umieszczenia protokołu kryptograficznego w sieci publicznej powoduje powstanie zagrożenia dla bezpieczeństwa wymiany informacji ze strony "przeciwnika aktywnego" (pojęcie to zostało wcześniej wprowadzone).

Zdefiniuję zestaw "przewag", jakimi dysponuje przeciwnik, dla uproszczenia oznaczony jako użytkownik Z:

1. Posiada on dostęp do wszystkich publicznych przekształceń - publicznych kluczy oraz zbiorów  $\Omega$  i  $\bar{\Omega}$ . Określam zatem język własny użytkownika Z generowany poza jakimkolwiek protokołem:

$$L(Z) = \{x : x \in (\bar{V} \cup \Omega \cup \{d_Z\})^*\}$$

2. Dysponuje zapisem wszystkich słów wymienionych w protokole  $T_{AB}$ .
3. Może inicjować łączność z obydwooma użytkownikami (A lub B). Innymi słowy - użytkownik Z może generować protokoły  $T'_{ZA}$  i  $T'_{ZB}$ , będą spreparowanym zapisem przesyłanych wcześniej wiadomości protokołu  $T_{AB}$ . Strona odpowiadająca prześle zwrotną wiadomość zgodnie z prawdziwym protokołem  $T_{ZA}$  ( $T_{ZB}$ ). Zapiszę formalnie protokół  $T'_{ZX}$  zniekształcony przez oszustwo użytkownika Z:

$$\begin{aligned}
 T'_{ZX} (X=A \text{ lub } B) = & \left\{ w_{2i-1} : (w_{2i-1} \in T_{ZX} \cup T_{AB}) \ \& \right. \\
 & \left. \&(w_{2i-1} = \bigwedge \left[ \prod_{k=1-1} (\alpha_1 \frac{1}{\prod} (\beta_k \alpha'_k))) \right], i=1, \dots, t \right\} \cup \\
 & \cup \left\{ w_{2i} : (w_{2i} \in T_{ZX} \cup T_{AB}) \ \& \right. \\
 & \left. \&(w_{2i} = \bigwedge \left[ \prod_{k=1} (\frac{1}{\prod} (\beta_k \alpha'_k))) \right], i=1, \dots, t \right\}
 \end{aligned}$$

Omawiana klasa języków jest zamknięta ze względu na operację sumy języków (którą zawiera powyższa definicja), zatem protokół  $T'_{ZX}$  można poddać przekształceniom określonym w Definicji 1 i 2.

W ten sposób można sformułować proste kryterium bezpieczeństwa protokołu kryptograficznego:

**DEFINICJA 4.** Protokół  $T_{AB}$  jest niepewny, jeśli istnieje słowo  $\tau \in T'_{ZX} \cup T'_{ZB}$  takie, że dla jakiegoś słowa  $x \in L(Z)$  zachodzi związek:

$$\bigwedge [\pi(x\tau)] = \delta$$

Oto komentarz do sformułowanego wyżej wniosku. Przekształcenie redukujące dokonane na uporządkowanym słowie  $\sigma = \pi(x\tau)$ , będącym całkowicie znanym użytkownikowi  $Z$ , daje pozytywną próbę złamania protokołu  $T_{AB}$ , ponieważ słowo  $\sigma$  koduje słowo wiadomości  $m \in M$  przekazywane protokołem  $T_{AB}$ .

Sformułowanie prostego kryterium decydującego o bezpieczeństwie badanego protokołu oraz wykazanie przynależności języka protokołu do klasy języków liniowo ograniczonych pozwala na szybkie i efektywne stwierdzenie, czy dany protokół jest bezpieczny. Przynależność do klasy języków liniowo ograniczonych daje gwarancję istnienia skończonego automatu sprawdzającego bezpieczeństwo protokołu.

Poniżej przedstawię przykłady zastosowania kryterium sformułowanego w Definicji 4.

## 5. KLASYFIKACJA PROTOKOŁÓW

Ze względu na relacje panujące między stronami nawiązującymi łączność, protokoły można podzielić na trzy grupy:

- 1) protokoły realizujące zasadę równouprawnienia obu stron,
- 2) protokoły uwzględniające uprzywilejowaną pozycję nadawcy,
- 3) protokoły z uprzywilejowaną pozycją odbiorcy.

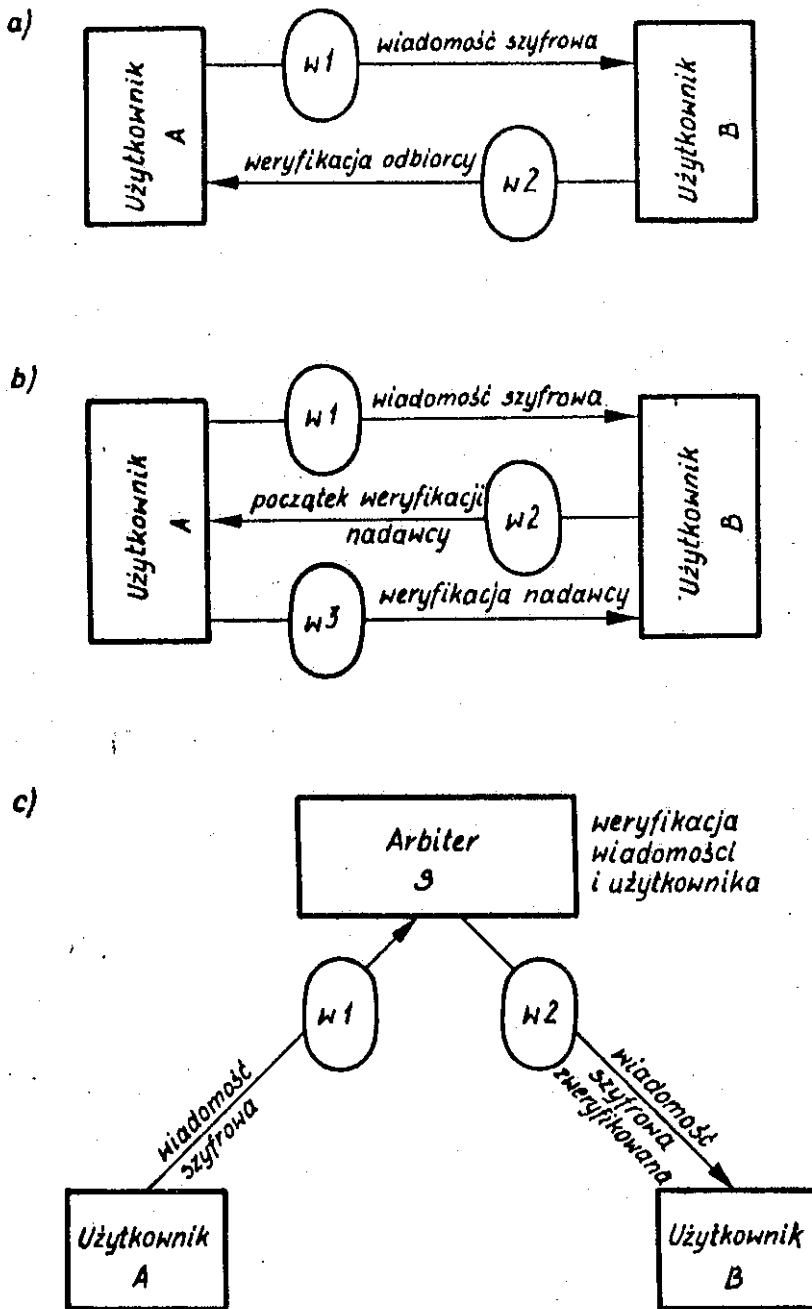
Ten podział protokołów (niewątpliwie, można przeprowadzać podział ze względu na inne cechy [2]) umożliwia obserwację wpływu relacji między nadawcą a odbiorcą wiadomości na bezpieczeństwo protokołu kryptograficznego.

Protokoły realizujące zasadę równouprawnienia rozmówców muszą uwzględniać konieczność naprzemiennej weryfikacji stron. Prawie wszystkie istniejące protokoły, wychodząc z założenia pełnej symetrii uprawnień, wprowadzają trzecią osobę - arbitra.

W schemacie uwzględniającym uprzywilejowaną pozycję nadawcy, odbiorca ma obowiązek udowodnienia swojej tożsamości oraz faktu otrzymania wiadomości. Jest to typowa sytuacja w komunikacji szefa z podwładnymi.

Rola nadawcy w protokołach z uprzywilejowaniem odbiorcy ogranicza się do przesłania wiadomości zawierającej dowód integralności danych oraz tożsamości właściciela. Protokoły tego typu stosowane są w systemach, w których przepływ informacji jest jednokierunkowy, a odbiorca nie musi być osiągalny natychmiast (np., w poczcie elektronicznej).

Na rys. 1 przedstawiono uproszczone schematy protokołów dla trzech typów relacji między użytkownikami.



Rys. 1. Typy protokołów kryptograficznych

a) z uprzywilejowaniem nadawcy; b) z uprzywilejowaniem odbiorcy; c) z równouprawnieniem stron

## 6. PROTOKOŁY Z UPRZYWILEJOWANĄ POZYCJĄ NADAWCY

Najczęściej spotykanym sposobem realizacji przywilejów nadawcy jest wprowadzenie zasady "handshake'u", tzn. przesłania zwrotnego tej samej wiadomości w następnym kroku protokołu. Przedstawię przykład najprostszego protokołu omawianej grupy. Protokół kaskadowy został zaproponowany w pracy [B]. Protokoły tej grupy nie posiadają przekształceń jawnych (zbiory  $\Omega$  i  $\bar{\Omega}$  są puste).

Przykład 1

Użytkownik A przesyła wiadomość podwójnie zabezpieczoną:

$$a) A \rightarrow B \quad (A, e_B d_A(m), B) \quad w_1 = \alpha_1 = e_B d_A$$

którą rejestruje użytkownik Z.

Inicjalizuje on łączność z B, powtarzając słowo  $w_1$ :

$$1) Z \rightarrow B \quad (Z, e_B d_A(m), B) \quad \alpha_1 \in T'_{ZB} \quad T'_{ZB}$$

Oczywiście, B odpowiada zgodnie z zasadą "handshake'u" słowem  $w_2 \in T'_{ZB}$

$$2) B \rightarrow Z \quad (B, e_Z d_B e_Z d_A(m), Z) \quad \beta_1 = e_Z d_B e_Z d_A$$

$$w_2 = \Gamma[\pi(\beta_1 \alpha_1)] = \Gamma[\pi(e_Z d_B e_Z d_B e_B d_A)] = e_Z d_B e_Z d_A$$

Dysponując postacią  $w_2 \in T'_{ZB}$  użytkownik Z składa je ze słowem  $x = e_B d_Z d_Z e_A \in L(Z)$  i otrzymuje:

$$\Gamma[\pi(xw_2)] = \Gamma[\pi(e_B d_Z d_Z e_A e_Z d_B e_Z d_A)] = \sigma$$

Zgodnie z Definicją 4, protokół ten można zdyskwalifikować, pomimo użycia w nim pewnej metody kryptograficznej.



Powyższy przykład pokazuje, jak ważne dla bezpieczeństwa komunikacji mogą okazać się przekształcenia jawne, których symbole należą do alfabetu ogólnego języka protokołów. Umożliwiają one działanie stronie podrzędnej - weryfikację tożsamości nadawcy bez kwestionowania jego uprzywilejowania. Przekształcenie wprowadzające do protokołu cyfrową sygnaturę zostanie przedstawione poniżej i użyte w protokołach wszystkich trzech kategorii.

Zgodnie z przyjętymi zasadami, litery A, B, ..., Z oznaczają użytkowników systemu. Odpowiednio, symbole a, b, ..., z są słowami identyfikowanymi jednoznacznie z użytkownikami A, B, ..., Z.

DEFINICJA 5. Zbiór  $X = \{ x: X \text{ jest użytkownikiem sieci, } X = A, B, \dots, Z \}$  zawiera wszystkie sygnatury używane w systemie. Przekształcenie pieczętujące dopisuje prefiks  $x$  do słowa wiadomości  $m \in M$ :

$$p_X : M \times \hat{X} \rightarrow \bar{M}$$

$$(\forall m \in M) (\forall x \in \hat{X}) p_X(m) = xm = \bar{m}$$

Przekształcenie wykrywające prefiks w słowie odebranych pozwoli uwierzytelnić stronę nadającą wiadomość:

DEFINICJA 6. Przekształcenie  $q_X$  wykrywa prefiks  $x$  w słowie odebranych  $\bar{m} \in \bar{M}$ .

$$q_X : \bar{M} \rightarrow M$$

$$(\forall \bar{m} \in \bar{M}) q_X(\bar{m}) = \begin{cases} m, & \text{jeśli } \bar{m} = xm \\ \text{niedefiniowane} & \\ \text{w przeciwnym wypadku} & \end{cases}$$

Oba przekształcenia sygnujące są operacjami dopisywania i usuwania słów, zatem są również operacjami należącymi do

klasy przekształceń definiowanych dla języków jednoelementowych i należą do alfabetu języka protokołów (zbiory  $\Omega$  i  $\bar{\Omega}$ ):

$$\bar{\Omega}_{AB} = \{p_A, p_B\} \quad \Omega_{AB} = \{q_A, q_B\}$$

Idea działania protokołu sygnującego jest następująca.

Odbiorca B otrzymuje słowo protokołu - w każdym kroku obowiązany jest sprawdzić, czy zdekodowana wiadomość posiada prefiks użytkownika A. Użytkownik A postępuje identycznie.

Przy analizie bezpieczeństwa protokołu sygnującego, powyższa definicja wymaga drobnej modyfikacji. Przekształcenie  $q_A$  służy wyłącznie identyfikacji użytkownika A w ramach legalnego protokołu  $T_{AB}$ . Z punktu widzenia przeciwnika Z bardziej interesująca jest operacja kasowania prefiksu, bez względu na jego znaczenie (pominięcie wariantu odrzucenia wiadomości w Definicji 6). Symbol  $q$  takiej operacji należy do określonego wcześniej języka  $L(Z)$ .

Poniższy przykład pokazuje niepewny protokół sygnujący (aczkolwiek algorytm złamania jest bardziej skomplikowany niż poprzednio). Niewielka modyfikacja tego protokołu umożliwia otrzymanie protokołu pewnego - wystarczy pominąć jedno przekształcenie kodujące o symbolu  $e$ . Dowód pewności protokołu uproszczonego zamieszczono w pracy [2].

#### Przykład 2

Użytkownik A inicjalizuje łączność z B, przesyłając wiadomość podwójnie zakodowaną:

$$a) A \rightarrow B \quad (A, e_B p_A e_B(m), B) \quad \alpha_1 = e_B p_A e_B$$

Użytkownik B odsyła potwierdzenie otrzymanej wiadomości:

$$b) B \rightarrow A \quad (B, e_A p_B e_A(m), A) \quad \beta_1 = e_A p_B e_A d_B q_A d_B$$

$$w_2 = \pi[\pi(\alpha_1 \beta_1)] = e_A p_B e_A$$

Złamanie tego protokołu może odbyć się następująco:

Z wykorzystuje słowo  $w_2$  do zainicjowania łączności z A:

$$1) Z \longrightarrow A \quad (Z, e_{AP_Z} e_{w_2}(m), A) \quad \alpha'_1 = e_{AP_Z} e_{AP_B} e_A = e_{AP_Z} w_2$$

W następnym kroku A wykrywa właściwy prefiks Z, a zatem odsyła potwierdzenie:

$$2) A \longrightarrow Z \quad (A, e_{ZP_A} e_{Zd_A} w_2(m), Z)$$

$$w'_2 = \Gamma \left[ \pi (e_{ZP_A} e_{Zd_A} q_Z d_A e_{AP_Z} w_2) \right] = e_{ZP_A} e_{Zd_A} w_2$$

W trzecim kroku protokołu  $T_{ZA}$  Z generuje słowo  $\alpha'_2$  oraz słowo protokołu  $w'_3$ :

$$3) Z \longrightarrow A \quad (Z, e_{AP_Z} d_A q w_2(m), A)$$

$$\alpha'_2 = e_{AP_Z} d_Z q d_Z \quad w'_3 = \Gamma \left[ \pi (\alpha'_2 w'_2) \right] = e_{AP_Z} d_A q w_2$$

Odbiorca A znowu otrzymuje słowo protokołu, którego nie może zakwestionować, zatem odpowiada potwierdzeniem:

$$w_4 = \Gamma \left[ \pi (\beta_2 w'_3) \right] = \Gamma \left[ \pi (e_{ZP_A} e_{Zd_A} q_Z d_A e_{AP_Z} d_A q w_2) \right] = e_{ZP_A} e_{Zd_A} d_A q w_2$$

$$4) A \longrightarrow Z \quad (A, e_{ZP_A} e_{Zd_A} d_A q w_2(m), Z)$$

Teraz Z tworzy słowo  $x$  i łamie protokół  $T_{AB}$ , gdyż, zgodnie z Definicją 4:

$$x = d_Z q d_Z \quad x \in L(Z)$$

$$\begin{aligned} \Gamma \left[ \pi (x w_4) \right] &= \Gamma \left[ \pi (d_Z q d_Z e_{ZP_A} e_{Zd_A} d_A q w_2) \right] = \\ &= \Gamma \left[ \pi (d_Z q d_Z e_{ZP_A} r_Z d_A d_A q e_{AP_B} e_A) \right] = \\ &= \Gamma (d_Z e_Z q p_A d_Z e_Z d_A e_A d_A e_A q p_B) = \emptyset \end{aligned}$$

## 7. PROTOKOŁY Z UPRIZYWILEJOWANIEM ODBIORCY

Budowa protokołu z uprzywilejowaniem odbiorcy jest podobna do konstrukcji omawianych poprzednio protokołów z uprzywilejowaniem nadawcy. Modyfikacji wymaga jedynie metoda uwierzytelnienia nadawcy oraz wiadomości. W miejsce prostej zasady "handshake'u" wiadomości można wprowadzić metodę polegającą na zwrotnym przesłaniu przez nadawcę parametru identyfikacyjnego utworzonego przez odbiorcę.

DEFINICJA 7. Niech  $\Phi = \{0,1\}$  oznacza alfabet języka wiadomości  $M$ .  $A$  i  $B$  są dowolnymi użytkownikami sieci. Przekształcenie identyfikujące użytkownika  $B$ , oznaczone symbolem  $id_B$ , jest różnicą symetryczną słowa wiadomości  $m$ , będącego własnością użytkownika  $A$ , oraz wybranego ciągu znaków identyfikatora  $idb$ :

$$id_B: \Phi^* \times \Phi^* \rightarrow \Phi^*$$

$$(\forall m \in \Phi^*) (\forall idb \in \Phi^*) : id_B(m, idb) = m \oplus idb = \bar{m}$$

DEFINICJA 8. Przekształcenie  $id'_A$  odzyskujące identyfikator jest różnicą symetryczną posiadanej przez użytkownika  $A$  wiadomości oraz otrzymanego w protokole  $T_{AB}$  słowa  $m$ :

$$id'_A: \Phi^* \rightarrow \Phi^*$$

$$(\bar{m} \in \Phi^*) \quad id'_A(\bar{m}, m) = idb$$

Z własności przekształcenia różnicy symetrycznej wynika, że zmiana jakiegokolwiek elementu słowa binarnego pociągnie za sobą zmianę w identyfikatorze i spowoduje odrzucenie przesłanego słowa.

Podane wcześniej wnioski dotyczące formalnego języka protokołów upoważniają, w przypadku protokołu z identyfikatorem, do niewielkiej modyfikacji alfabetów  $\Omega$  i  $\mathcal{Q}$ :

$$\Omega_{AB} = \{p_A, p_B, id_A, id_B\} \quad \mathcal{Q}_{AB} = \{q_A, q_B, id_A, id_B\}$$

Oto proponowany w pracy [6] protokół z identyfikatorem. Dla odmiany, zaprezentuję protokół pewny. W cytowanej pracy przytoczono protokół niepewny w sensie Definicji 4.

### Przykład 3

Użytkownik A inicjalizuje łączność:

$$a) A \rightarrow B \quad (A, e_{BP_A}(m), B) \quad \alpha_1 = w_1 = e_{BP_A}$$

Odbiorca B dekoduje słowem  $\beta_1$  wiadomość  $m$  i rozpoczyna procedurę uwierzytelniania, odsyłając wiadomość  $m$  zaopatrzoną w identyfikator  $id_B$ :

$$b) B \rightarrow A \quad (B, e_{AP_B id_B}(m), A) \quad \beta_1 = e_{AP_B id_B} q_A d_B$$

$$w_2 = \mathcal{F}[\mathcal{T}(\beta_1 \alpha_1)] = e_{AP_A id_B} q_A d_B e_{BP_A} = e_{AP_B id_B}$$

Użytkownik A odsyła do B pieczętowany i szyfrowany identyfikator  $id_B$ :

$$c) A \rightarrow B \quad (A, e_{BP_A id_A id_B}(m), B) \quad \alpha_2 = e_{BP_A id_A} q_B d_A$$

$$w_3 = \mathcal{F}[\mathcal{T}(\alpha_2 w_2)] = e_{BP_A id_A} q_B d_A p_B id_B = e_{BP_A id_A id_B}$$

Jeśli odbiorca B otrzyma, po zdekodowaniu słowem  $\beta_2$ :

$$\beta_2 = q_A d_B id_A id_B \text{ identyfikator } id_B,$$

wtedy uwierzytelnienie wiadomości oraz jej nadawcy zakończyło się sukcesem.

### 8. PROTOKOŁY Z RÓWNOUPRAWNIENIEM STRON

Obecność arbitra w protokołach z równouprawieniem stron eliminuje konieczność wzajemnej weryfikacji użytkowników metodą "handshake'u" oraz umożliwia wprowadzenie nowych przekształceń jawnych protokołu - znacznika czasowego<sup>1)</sup> i znacznika ważności<sup>2)</sup> (wyłączny przywilej arbitra).

DEFINICJA 9. Niech użytkownik S pełni w systemie rolę arbitra. Słowo  $t \in \Phi^*$  opisuje czas nadania wiadomości. Przekształcenie  $t_S$  jest operacją składania słów.

$$t_S : \Phi^* \rightarrow \Phi^*$$

$$(\forall m \in \Phi^*) (\exists t \in \Phi^*) : t_S(m) = tm = m_{time}$$

DEFINICJA 10. Przekształceniem  $r_B$  użytkownik B weryfikuje czas wysłania wiadomości:

$$r_B : \Phi^* \rightarrow \Phi^*$$

$$(\forall m_{time} \in \Phi)^* : r(m_{time}) = \begin{cases} m, & \text{jeśli } |clk_B - t| < \Delta t_1 + \Delta t_2 \\ \text{nieokreślone, w przeciwnym} \\ \text{przypadku} \end{cases}$$

oznaczenia:

$clk_B$  - lokalny zegar użytkownika,

$\Delta t_1$  - różnica fazy między zegarem głównym sieci a zegarem użytkownika B,

$\Delta t_2$  - opóźnienie propagacji wiadomości w sieci,

$\Delta t_1$  i  $\Delta t_2$  - są wartościami stałymi w sieci.

1) (Ang. time-stamp) - termin ten wprowadzono w pracy [5].

2) Arbiter dopisuje znacznik ważności jako dowód uwierzytelnienia wiadomości i nadawcy.

Przekształcenia  $t_S$  i  $r_B$  są publicznie znane. Ponieważ mieszczą się w klasie rozważanych języków, zatem stanowią symbole alfabetu  $\Sigma$  - formalnego alfabetu języka protokołów. Należy zauważyć, że przekształcenie znacznika czasowego może zastosować każdy inny użytkownik sieci (jeśli istnieje centralny zegar w sieci).

Następny parametr weryfikacyjny jest używany w protokole trójstronnym (stosowanym wyłącznie przez arbitra). Znacznik ważności jest wybranym przez arbitra, publicznie znanym słowem-identyfikatorem tworzonym na tej samej zasadzie co znacznik czasowy.

DEFINICJA 11. Przekształcenie  $id_S$  dopisuje prefiks  $ids$  do słowa wiadomości  $m$ .

$$id_S : \Phi^* \rightarrow \Phi^*$$

$$(\forall m \in \Phi^*) : id_S(m) = idsm = m_{valid}$$

Słowo  $m_{valid}$  trafia do użytkownika B, który dokonuje weryfikacji przez porównanie otrzymanego prefiksu ze wzorcem identyfikatora:

DEFINICJA 12. Przekształcenie  $id_B$  kasuje  $ids$  w słowie  $m_{valid}$ :

$$id_B : \Phi^* \rightarrow \Phi^*$$

$$(\forall m_{valid} \in \Phi^*) : id_B(m_{valid}) = \begin{cases} m, & \text{jeśli } m_{valid} = idsm \\ \text{niedefiniowane, w przeciwnym przypadku} \end{cases}$$

Poniżej zostanie przedstawiony przykład protokołu z udziałem strony trzeciej - arbitra. Protokół  $T_{AB}$  jest sumą języków  $T_{AS}$  i  $T_{SB}$  - protokołów dwustronnych opisanych Definicją 3.

Każdorazowo przesyłane jest jedno słowo, które odbiorca B akceptuje, jeśli posiada ono znacznik ważności arbitra. Zastosowanie przez nadawcę A publicznego klucza użytkownika B

gwarantuje tajemnicę przesyłanej wiadomości. A zatem, arbiter jest tzw. "ślepy arbitrem", wykonującym wszystkie funkcje uwierzytelniające bez dekodowania dochodzącej do niego wiadomości [1].

#### Przykład 4

Użytkownik A koduje wiadomość swoim kluczem prywatnym  $d_A$  oraz publicznym odbiorcy -  $e_B$ , co powoduje, że staje się ono niejawnie dla arbitra. Następnie, zakodowane słowo zaopatruje w odpowiednie parametry uwierzytelniające oraz koduje kluczem publicznym arbitra  $e_S$ . Wysyła zatem dość skomplikowane słowo protokołu:

$$a) A \rightarrow S \quad (A, e_S d_A p_A p_B^t e_B d_A(m), S)$$

$$\alpha_1 = w_1 = e_S d_A p_A p_B^t e_B d_A$$

Arbiter dokonuje uwierzytelnienia nadawcy i, pośrednio, wiadomości (stwierdza jej integralność i autorstwo nadawcy), następnie wysyła do B słowo  $w_2$ :

$$\mu_1 = e_B d_S p_A p_B^t e_S r_A q_B q_A e_A d_S$$

$$w_2 = f[\pi(\mu_1 \alpha_1)] = e_B d_S p_A p_B^t e_S e_B d_A$$

$$b) S \rightarrow B \quad (S, e_B d_S p_A p_B^t e_S e_B d_A, B)$$

Odbiorca B formuje słowo  $\beta_1$  i weryfikuje wiadomość: odczytuje znacznik ważności i znacznik czasowy, sygnatury A i B (czyli weryfikuje arbitra) i, uspokojony, przystępuje do odczytania wiadomości:

$$\beta_1 = e_A d_B r_S^t e_B q_B q_A e_S d_B$$

$$w_3 = f[\pi(e_A d_B r_S^t e_B q_B q_A e_S d_B e_B d_S p_A p_B^t e_S e_B d_A)] = \delta$$



Przedstawiony wyżej schemat rozwiązuje praktycznie wszystkie problemy związane z uwierzytelnieniem:

- spełnia wszystkie postulaty całkowitej weryfikacji;
- nie istnieje żadna informacja poufna, uzgodniona wcześniej między nadawcą, odbiorcą i arbitrem;
- żadna niewłaściwie datowana informacja nie zostanie zaakceptowana, nawet gdy klucze prywatne  $d_A$ , ( $d_B$ ) staną się publicznie znane;
- przesłana informacja jest niewidoczna dla arbitra.

## 9. WNIOSKI

Przedstawiona analiza bezpieczeństwa wykazała zależność między relacjami panującymi w sieci a stopniem zagrożenia protokołu kryptograficznego.

Zasada uprzywilejowania stron umożliwi przeciwnikowi aktywnemu próbę złamania obcego protokołu poprzez wykorzystanie słów innych protokołów.

Obecność arbitra w protokole z równouprawnieniem stron (niemożliwa do pogodzenia z zasadą uprzywilejowania w pozostałych dwóch grupach) eliminuje integrację użytkownika Z, zatem protokół taki jest, z punktu widzenia Definicji 4, całkowicie bezpieczny.

W artykule nie zostało poruszone w ogóle zagadnienie bezpieczeństwa ze strony samych użytkowników (stron) protokołu.

W pracy przedstawiono formalny opis i analizę bezpieczeństwa protokołu kryptograficznego oparte na teorii języków liniowo ograniczonych.

Proste kryterium bezpieczeństwa pozwala szybko i efektywnie ustalić, czy protokół nie jest narażony na złamanie na skutek błędnej struktury wewnętrznej. Stwierdzenie tego faktu jest dużym krokiem naprzód na drodze budowy powszechnego systemu ochrony danych w sieci teleinformatycznej.

## WYKAZ LITERATURY

1. Akl S.G.: Digital Signatures with Blindfolded Arbitrators Who Cannot Form Alliances. Proc. of the 1982 Symp. on Security & Privacy, V+1070P, pp. 129-135. NY, USA, IEEE 1982.
2. Andrukiewicz E.: Kodowanie wiadomości jako metoda ochrony danych w sieciach teleinformatycznych. Praca doktorska. Instytut Łączności, Warszawa 1987.
3. Andrukiewicz E.: Problemy ochrony informacji w publicznej sieci teleinformatycznej. Materiały KST'88, Bydgoszcz, 7 - 9 września 1988, s. 393-402.
4. Blikle A.: Automaty i gramatyki, PWN, Warszawa 1971.
5. Denning D.E., Sacco M.: Time Stamps in Key Distribution Protocols. Comm. ACM, vol. 24, No 8, August 1981, pp. 533-536.
6. Desmedt Y., Vandewalle J., Goevaerts R.: Fast Authentication Using Public-Key Schemes. 1984 International Zurich Seminar on Digital Communications, March 6-8, Proc. of IEEE, pp. 191-197.
7. Diffie W., Hellman M.: New Directions in Cryptography. IEEE Trans. Inf. Theory, November 1976, vol. IT-22, No 6, pp. 644-654.
8. Dolev D., Yao A.C.: On the Security of Public-Key Protocols. IEEE Trans. Inf. Theory, vol. IT-29, No 2, March 1983, pp. 193-207.
9. Simmons G.J.: Secure Communications in the Presence of Pervasive Deceit. Proc. of the Symp. on Security & Privacy, Oakland, CA, April 14-16 1980, pp. 84-92.

Эльжбета Андрукевич

## КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ В ТЕЛЕИНФОРМАТИЧЕСКИХ СЕТЯХ

### Резюме

Приводится формальное описание криптографического протокола основанного на теории линейно ограниченных языков и автоматов.

Предложено линейно ограниченный язык определяемый криптографическим протоколом. Два преобразования на языках - отображения /упорядочения и редукции/ позволяют формулировать простой критерий безопасности криптографического протокола /определение 4/.

Предложено классификацию основанную на типах связей существующих между потребителями сети. Использование критерия безопасности в протоколах разных групп иллюстрируется многими примерами.

Доказана тесная зависимость между связями существующими в сети и безопасностью криптографических протоколов.

Elzbieta Andrukiewicz

## THE CRYPTOGRAPHIC PROTOCOLS IN COMPUTER NETWORKS

### Summary

The formal description of the cryptographic protocol and an analysis of its security based on linear bounded automata and language theory is presented.

The symbolic language is created for formal definition of the protocol as a linear bounded language. Two transformations performed on languages - ordering and reducing transformations - help to define a simple criterion of the security of the protocol (definition 4).

The classification of protocols based on relations between any two networks users is proposed. Several examples of applying the criterion of the security are shown for each group of protocols.

A dependance of the security of protocols on network relations is proved.

Elżbieta Andrukiewicz

## PROTOCOLES CRYPTOGRAPHIQUES DANS LES RESEAUX TÉLÉINFORMATIQUES

### Résumé

On a présenté la description formelle d'un protocole cryptographique basé sur la théorie des langages et des automates à mémoire linéairement bornée.

On a créé un langage à mémoire linéairement bornée qui sert à définir le protocole cryptographique. Deux transformations faites sur les langages en question à savoir celles de l'ordre et de réduction ont permis de formuler un simple critère de sécurité du protocole cryptographique (définition 4).

On a proposé une classification basée sur les types de relations entre les utilisateurs du réseau. Application de ce critère de sécurité pour les protocoles de différents groupes est illustré à l'aide de plusieurs exemples.

On a montré qu'il y a une stricte dépendance entre les relations existant dans un réseau et la sécurité des protocoles cryptographiques.

Elżbieta Andrukiewicz

## KRYPTOGRAFISCHE PROTOKOLLE IN TELEINFORMATISCHEN NETZEN

### Zusammenfassung

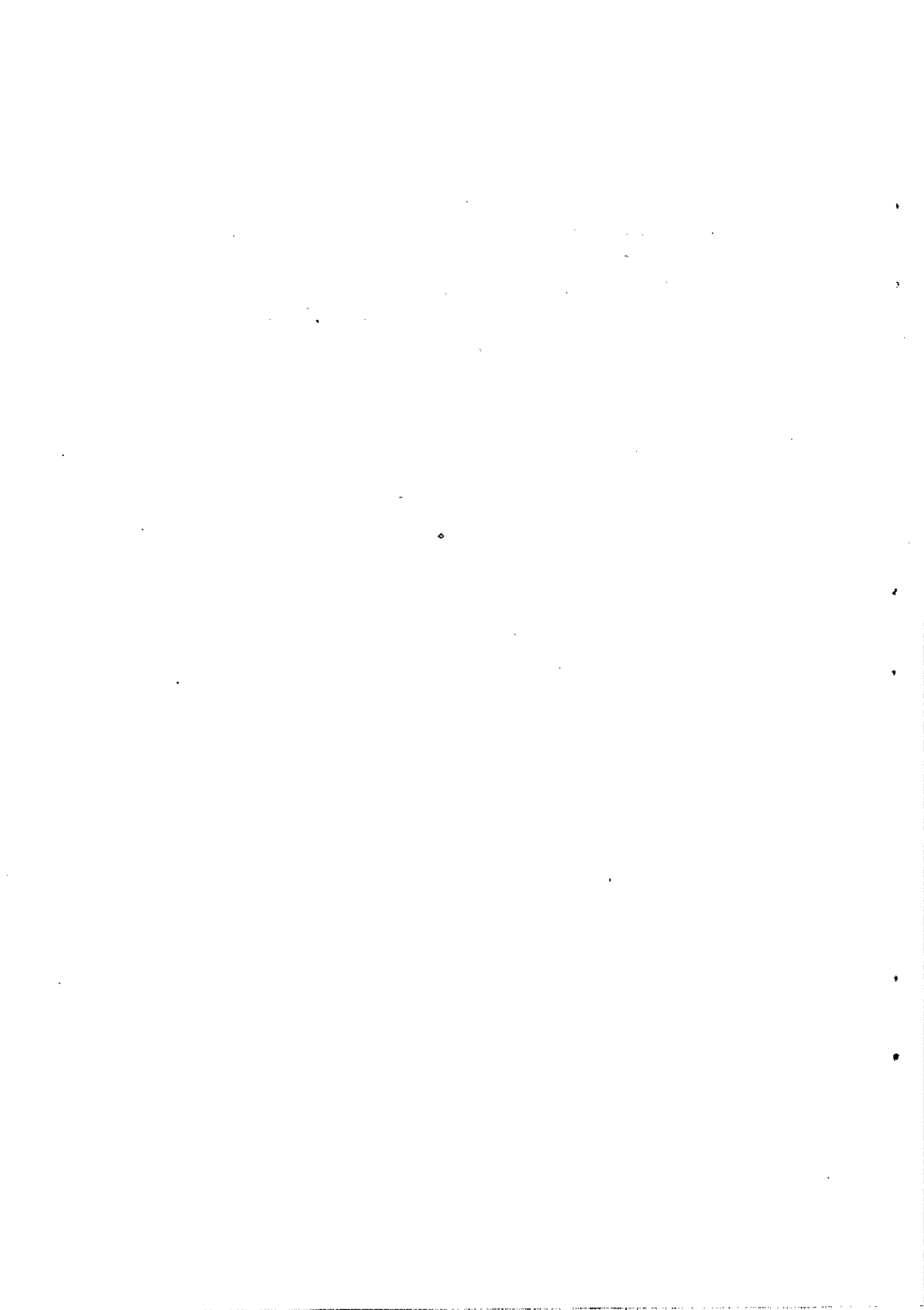
Es wurde die formale Beschreibung des auf Theorie der Sprachen und linear begrenzter Automaten basierenden Protokolls dargestellt.

Es wurde die linear begrenzte Sprache geschaffen, welche das kryptografische Protokoll definiert. Zwei Transformatio-

nen auf den Sprachen (richtende und reduzierende Abbildung) ermöglichen Formulierung eines einfachen Sicherheitskriteriums des kryptografischen Protokolls (Definition 4).

Es wurde die auf Relationstypen zwischen Netzbenutzer basierende Klassifikation proponiert. Anwendung des Sicherheitskriteriums für Protokolle der verschiedenen Gruppen wurde mit vielen Beispielen illustriert.

Es wurde die enge Zusammenhang zwischen den Relationen im Netz und der Sicherheit der kryptografischen Protokolle bewiesen.



Zbigniew Kowalski (Habdank)

621.395.74

## ANALIZA WŁAŚCIWOŚCI - ZMODYFIKOWANEJ TŁUMIENNOŚCI ODNIESIENIA

Rękopis dostarczony do Komitetu Redakcyjnego dn. 1989.05.03

W artykule przeprowadzono analizę właściwości zmodyfikowanej tłumienności odniesienia  $LR^1)$ , która została zalecona przez CCITT<sup>2)</sup> do oceny jakości łańcuchów telefonicznych i ich ogniw składowych. Wielkość  $LR$  obiektu (czwórnika dowolnego rodzaju: elektrycznego, elektroakustycznego, akustoelektrycznego, albo też akustycznego) została określona na podstawie ścisłej definicji matematycznej, wiążącej funkcyjnie tę skalarną wielkość z tłumiennością  $A$  badanego obiektu w zakresie częstotliwości akustycznych. Sprecyzowanie tej funkcyjnej zależności stworzyło możliwość dokonania analizy linearności i addytywności wielkości  $LR$ , a także określenia wpływu losowych błędów wyznaczania tłumienności punktowych  $A$  na błędy oceny wielkości  $LR$  badanych obiektów.

### 1. WPROWADZENIE

Podstawowym czynnikiem wpływającym na słyszalność rozmów telefonicznych jest tłumienie energii sygnałów, przesyłanych drogami połączeniowymi tworzonymi w sieci. Na podstawie międzynarodowych uzgodnień drogi te, zwane łańcuchami telefonicznymi, przyjęto charakteryzować tłumiennością odniesienia, skalarną wielkością, ustanowioną w roku 1928 przez CCIF<sup>3)</sup>.

1)  $LR$ : Loudness Rating (patrz [1]).

2) CCITT: Comité Consultatif International Telegraphique et Telephonique (powstały w roku 1956 z połączenia CCIF i CCIT).

3) CCIF: Comité Consultatif International Telephonique.

Przyjęto zasadę, że tłumienność odniesienia jest wyznaczana na podstawie subiektywnych wrażeń jednakowej głośności dźwięków mowy, transmitowanej na przemian przez badany obiekt (łańcuch telefoniczny albo jego ogniwo) oraz przez wzorzec odniesienia.

Przeprowadzone badania wykazały jednak, że ocena tłumienności odniesienia obiektu, uzyskana na podstawie jednorazowego porównania ze wzorcem jest obarczona bardzo dużą niepewnością. W celu zwiększenia dokładności oceny tłumienności badanego obiektu, jego porównanie ze wzorcem odniesienia jest przeprowadzane wielokrotnie, przy czym porównania te są dokonywane przez członków specjalnie dobranej (głównie ze względu na dobry słuch) i odpowiednio przeszkolonej ekipy telefonometrycznej. Podczas pomiarów każdy członek ekipy (występujący dwukrotnie: raz jako mówiący; drugi raz jako nasłuchujący) dokonuje oceny tłumienności badanego obiektu, współpracując kolejno ze wszystkimi pozostałymi jej członkami. Dlatego przy liczebności ekipy telefonometrycznej równej  $N$  (zazwyczaj 4+6) osób, liczba porównań  $P$  badanego obiektu ze wzorcem wynosi:

$$P = N(N-1) \quad (1)$$

Zakładając, że każde porównanie jest takiej samej dokładności, jako ocenę tłumienności badanego obiektu przyjmuje się wartość średnią z wyników poszczególnych porównań, tzn.:

$$A = \frac{1}{P} \sum_{\substack{j, i=1 \\ i \neq j}}^N A_{ji} \quad (2)$$

gdzie:  $A_{ji}$  oznacza wynik pomiaru tłumienności uzyskany w przypadku, gdy  $j$ -ty członek ekipy mówi, zaś  $i$ -ty słucha.

Ze względu na przyjętą zasadę subiektywnej metody oceny, mimo stosowania powtórzeń, uśrednione oceny tłumienności odniesienia nadal są mało dokładne, przy czym zależą one od składu osobowego ekipy telefonometrycznej i od aktualnego stanu samopoczucia jej operatorów. Z punktu widzenia zastoso-



wał praktycznych powtarzalność tych uśrednionych ocen tłumienności odniesienia okazała się zupełnie niezadowalająca, stwierdzono bowiem występowanie rozbieżności ocen rzędu kilku decybeli (w ostatnich latach wykazano nawet, że te rozbieżności mogą dochodzić do 8 dB). Dlatego wkrótce po ustanowieniu omawianej wielkości rozpoczęto prace nad obiektywizacją pomiarów tłumienności odniesienia, umożliwiającą uzyskanie zadowalającej powtarzalności wyników pomiarów przy znacznie mniejszej pracochłonności ich wykonania.

W roku 1940 opracowano metodę obiektywnych pomiarów tłumienności odniesienia, wykorzystującą jako sygnał pomiarowy ton woblujący<sup>1)</sup> (Braun [1+2]). Okazało się jednak, że za pomocą zbudowanego wówczas przyrządu można było uzyskać zadowalającą zgodność obiektywnych i subiektywnych wyników pomiarów tylko dla określonego typu obiektów (np. dla aparatów telefonicznych tylko jednego typu).

Na skutek tej istotnej wady, metoda Brauna nie została zalecona do powszechnego stosowania ani przez CCIF, ani też przez CCITT, mimo iż modyfikacja tej metody jest nadal wykorzystywana w przyrządach pomiarowych (firmy Bruel & Kjaer), dotychczas stosowanych w różnych krajach przez administracje łączności i wytwórnie aparatów telefonicznych.

Dopiero w roku 1980, na VII Zgromadzeniu Plenarnym CCITT [3], wprowadzając zamiast dotychczas stosowanej: klasycznej - zmodyfikowaną tłumienność odniesienia LR, zalecono stosowanie również obiektywnej metody pomiaru tej nowej wielkości, jako dającej generalnie (tzn. dla rozmaitych obiektów) zadowalającą zgodność ocen z ustaloną przez CCITT subiektywną metodą pomiaru tej wielkości. W końcu roku 1988, na IX Zgromadzeniu Plenarnym CCITT, postanowiono całkowicie odstąpić od stosowania subiektywnej metody wyznaczania tłumienności odniesienia i zalecono stosowanie wyłącznie obiektywnej metody pomiaru wielkości LR.

---

1) Sygnał sinusoidalny o częstotliwości okresowo zmienianej (np. 1/s) w zakresie akustycznym (np. od 200 do 4000 Hz).

Wyznaczaną na podstawie pomiarów obiektywnych zmodyfikowaną tłumienność odniesienia LR określono w zaleceniu P.79 CCITT [3, 4] jako różnicę:

$$LR = L - L_w \quad (3)$$

gdzie  $L$  oraz  $L_w$  są tłumieniami głośności sygnałów dźwiękowych (ściślej: sygnałów o częstotliwościach akustycznych), transmitowanych odpowiednio przez badany obiekt oraz przez wzorzec odniesienia IRS<sup>1)</sup>. Badanym obiektem może być czwórnik dowolnego rodzaju: akustyczny, elektryczny, akustoelektryczny albo też elektroakustyczny; wzorcem odniesienia jest w każdym przypadku czwórnik tego samego rodzaju co i badany obiekt. Tłumienie głośności sygnałów transmitowanych przez dany czwórnik jest pewną miarą tego czwórника i dlatego zostało nazwane jego tłumiennością głośności.

Tłumienność głośności  $L$  linearnego czwórника dowolnego rodzaju zdefiniowano jako funkcjonal tłumienności  $A(f)$  tego czwórника, określony w pasmie akustycznym o częstotliwościach granicznych  $[f_d, f_g]$  następującym wzorem (patrz Dodatek 1.1):

$$L = \frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-A(f) \frac{m}{10}} g(f) df \quad (4)$$

gdzie  $m$  jest współczynnikiem wzrostu głośności,  $A(f)$  jest częstotliwościową charakterystyką tłumienności tego czwórника, zaś  $g(f)$  jest funkcją gęstości wagi unormowaną w rozważanym pasmie częstotliwości, tzn. spełniającą warunek:

$$\int_{f_d}^{f_g} g(f) df = 1 \quad (5)$$

Należy zaznaczyć, że CCITT dopuszcza stosowanie kilku rodzajów pasm częstotliwości. W tym opracowaniu będziemy rozwa-

1) IRS: Intermediate Reference System; (patrz [11]).

zać tylko jeden rodzaj pasma: telefonii naturalnej (o częstotliwościach granicznych  $f_d = 300$  Hz i  $f_g = 3400$  Hz).

Wielkość  $L$  określonego czwórnik (o niezmiennych właściwościach transmisyjnych) jest zatem liczbą, której wartość zależy od funkcji  $A(f)$ ; należy zwrócić uwagę, że wielkość  $L_w$  charakteryzująca wzorzec jest z założenia (patrz Dodatek 1.2) stałą o wartości równej znamionowej tłumienności głośności wzorca odniesienia IRS (tab. 1).

Tablica 1

Wartości stałej  $L_w$  charakteryzującej wzorzec IRS  
(wg "Handbook on Telephonometry" [5, punkt 6.4.2])

Charakterystyka	Rodzaj czwórnik	$L_w$ [dB]
Część nadawcza IRS	akustoelektryczny	+3,0
Część odbiorcza IRS	elektroakustyczny	-12,0
Część łącząca IRS	elektryczny	0,0
Cały łańcuch IRS	akustyczny	-9,0

W praktyce pomiarowej badania właściwości czwórników są przeprowadzane przy ustalonych częstotliwościach  $f_k \in [f_d, f_g]$  (gdzie  $k = 1, \dots, p$ , przy czym  $p$  jest liczbą punktów pomiarowych), a wartość tłumienności głośności jest określana na podstawie przybliżonej równości<sup>1)</sup>:

$$L \approx -\frac{10}{m} \lg \sum_{k=1}^p G_k \cdot 10^{-A_k \frac{m}{10}} \equiv L \quad (6)$$

w której  $A_k = A(f_k)$ , natomiast  $G_k = g(f_k) \cdot \Delta f_k$  są unormowanymi współczynnikami wagowymi dla częstotliwości  $f_k$  znajdującymi się wewnątrz odpowiednich wstęp o szerokości  $\Delta f_k$ ; współczynniki te spełniają warunek:

$$\sum_{k=1}^p G_k = 1 \quad (7)$$

1) Uwaga: w tym opracowaniu punktowe aproksymaty wielkości pasmowych (zdefiniowanych z zastosowaniem całki określonej w pasmie częstotliwości) są oznaczone symbolem zawierającym kropkę ponad odpowiednim znakiem, a więc:  $L$ ,  $L_o$ ,  $R$ .

Ze wzoru (4) widać, że tłumienność głośności  $L$  czwórnika zależy od jego częstotliwościowej charakterystyki  $A(f)$  w paśmie przesyłowym. W artykule przedstawiono metodę i wyniki analizy tej zależności dla kanałów i łańcuchów telefonicznych, przeprowadzonej dla przypadku z reguły występującego przy projektowaniu sieci telefonicznej, gdy nie ma pełnych informacji o przebiegach funkcji  $A(f)$ , charakteryzujących poszczególne ogniwa projektowanej sieci. Analiza numeryczna została przeprowadzona przy wykorzystaniu wzoru (6) stosowanego w praktyce do obliczeń wielkości  $L$ , przyjmując podane w [5, p. 6.4.2] dla naturalnego pasma telefonicznego wartości częstotliwości  $f_k$  i współczynników wagowych  $G_k$  (tabl. 2).

Tablica 2

Wartości parametrów:  $m$ ,  $p$ ,  $f_k$ ,  $G_k$   
do wyznaczania tłumienności głośności  $L$  w paśmie telefonicznym  
(wg "Handbook on Telephonometry" [5, punkt 6.4.2])

Współczynnik wzrostu głośności:  $m = 0,2$ ;

Liczba punktów aproksymacji całki przez sumę:  $p = 11$ .

k	Częstotliwość $f_k$ [Hz] *)	Współczynnik $G_k$
1	315	0,05
2	400	0,1
3	500	0,1
4	630	0,1
5	800	0,1
6	1000	0,1
7	1250	0,1
8	1600	0,1
9	2000	0,1
10	2500	0,1
11	3150	0,05

\*) Wartości częstotliwości ustalone przez ISO (International Standard Organisation).

## 2. OCENA TŁUMIENNOŚCI GŁOŚNOŚCI KANAŁÓW TELEFONICZNYCH OCENA BŁĘDÓW LINEARNOŚCI MIARY

Rozważmy kanał telefoniczny (w sensie ogólnym: czwórnik o elektrycznym lub akustycznym wejściu oraz wyjściu), którego tłumienność<sup>1)</sup> wynosi:

$$A(f) = A_c + D(f) \quad (8)$$

gdzie  $A_c = A(f_c)$  jest tłumiennością rozważanego czwornika dla częstotliwości odniesienia (centralnej częstotliwości pasma):

$$f_c = \sqrt{f_d \cdot f_g}, \quad (9)$$

zaś  $D(f)$  są zniekształceniami tłumieniowymi tego czwornika, określonymi względem częstotliwości  $f_c$  (tzn.  $D(f_c) = 0$ ).

Uwzględniając (8) w (2) możemy wyrazić tłumienność głośności rozważanego kanału następującym wzorem:

$$L = A_c + \Delta L \quad (10)$$

gdzie:

$$\Delta L = -\frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-\frac{D(f)}{10} \frac{m}{10}} g(f) df \quad (11)$$

jest przyrostem tłumienności głośności rozważanego czwornika, wywołany jego zniekształceniami tłumieniowymi w pasmie  $[f_d, f_g]$ .

Należy zwrócić uwagę, że w przypadku, gdy wartość parametru  $m$  dąży do zera, zachodzą związki (patrz Dodatek 2):

$$\lim_{m \rightarrow 0} L = \int_{f_d}^{f_g} A(f) g(f) df \equiv L_0 \quad (12)$$

albo:

$$\lim_{m \rightarrow 0} L = A_c + \Delta L_0 \equiv L_0 \quad (13)$$

1) Dowolnego rodzaju - patrz ostatni akapit tego rozdziału.

gdzie:

$$\Delta L_0 = \int_{f_d}^{f_g} D(f) g(f) df \quad (14)$$

Różnica tych dwóch wielkości wynosi:

$$\begin{aligned} R &= L - L_0 = \Delta L - \Delta L_0 = \\ &= - \int_{f_d}^{f_g} D(f) g(f) df - \frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-D(f) \frac{m}{10}} g(f) df \quad (15) \end{aligned}$$

Jak widać ze wzorów (14) i (15), przy ustalonej funkcji wagi  $g(f)$  zarówno  $\Delta L_0$  jak i  $R$  zależą tylko od zniekształceń tłumieniowych  $D(f)$  rozważanego czwórnika. Ponieważ w zbiorze kanałów telefonicznych te zniekształcenia są funkcjami losowymi, spróbujmy określić górne ograniczenia tych wielkości.

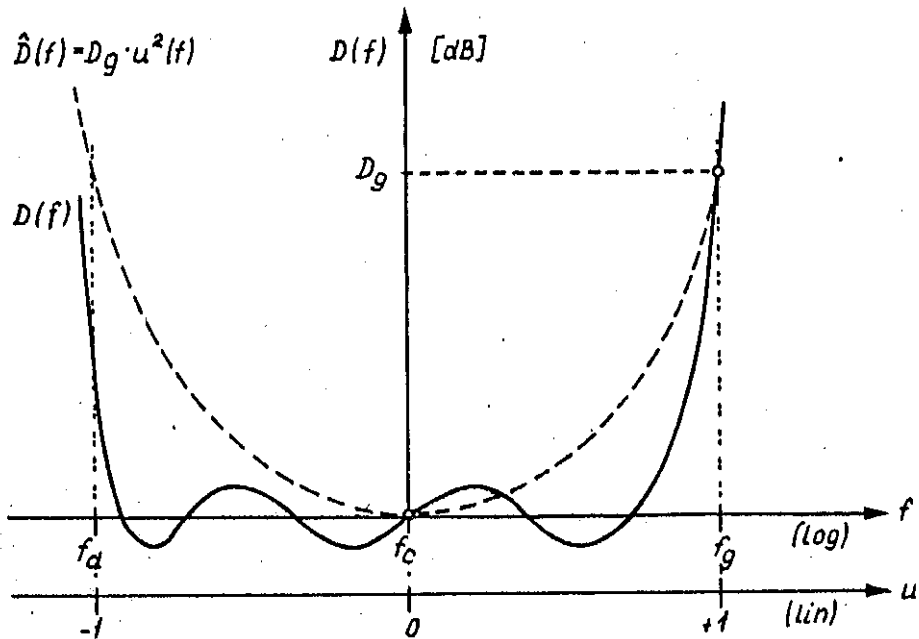
### 2.1. Górna granica wielkości $\Delta L_0$

Na rys. 1 przedstawiono przykładową charakterystykę zniekształceń tłumieniowych przypadkowego kanału telefonicznego, którą można scharakteryzować wartością zniekształceń  $D_g$ , występujących dla częstotliwości  $f_g$  górnej granicy pasma przesyłowego:

$$D_g = D(f_g) \quad (16)$$

Przyjmijmy, że w zbiorze kanałów telefonicznych wszystkie charakterystyki  $D(f)$  zniekształceń tłumieniowych, które przechodzą przez punkty:  $(f_c, 0)$  oraz  $(f_g, D_g)$  są prawie wszędzie ograniczone od góry parabolą określoną wzorem:

$$\hat{D}(f) = D_g \cdot u^2(f) \quad (17)$$



Rys. 1. Charakterystyka zniekształceń tłumieniowych kanału telefonicznego (objaśnienia w tekście punktu 2.1)

gdzie

$$u(f) = \frac{\lg\left(\frac{f}{f_c}\right)}{\lg\left(\frac{f_g}{f_c}\right)} \quad (18)$$

Wykres tej paraboli przedstawiono na rys. 1 linią przerywaną. Przyjęte ograniczenie oznacza, że w pasmie przesyłowym  $[f_d, f_g]$  mogą istnieć pewne zakresy częstotliwości  $f$  (z reguły występujące w otoczeniu częstotliwości  $f_c$ ), w których nie jest spełniony warunek:

$$D(f) < \hat{D}(f) \quad (19)$$

natomiast zawsze jest spełniony warunek:

$$\Delta L_o < \hat{\Delta} L_o \quad (20)$$

gdzie

$$\hat{\Delta}L_o = \int_{f_d}^{f_g} D(f) g(f) df = D_g \int_{f_d}^{f_g} u^2(f) g(f) df \quad (21)$$

Wprowadzając oznaczenie:

$$\int_{f_d}^{f_g} u^2(f) g(f) df = \hat{\delta} \quad (22)$$

otrzymujemy:

$$\hat{\Delta}L_o = \hat{\delta} D_g \quad (23)$$

W celu wyznaczenia wartości liczbowej współczynnika  $\hat{\delta}$  zastępujemy całkowanie sumowaniem, a więc przyjmujemy, że zachodzi przybliżona równość:

$$\hat{\delta} \approx \sum_{k=1}^p G_k u_k^2 \quad (24)$$

gdzie

$$u_k = u(f_k) = \frac{\lg\left(\frac{f_k}{f_c}\right)}{\lg\left(\frac{f_g}{f_c}\right)} \quad (25)$$

Przyjmując dla naturalnego pasma telefonicznego podane w tabelicy 2 wartości częstotliwości  $f_k$  i współczynników wagowych  $G_k$ , uzyskuje się wartość współczynnika

$$\hat{\delta} \approx 0,300 \quad (26)$$

## 2.2. Górna granica wielkości R

Górną granicę wielkości R można wyznaczyć, podstawiając (17) do (11):



$$\begin{aligned} \hat{\Delta L} &= -\frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-D(f) \frac{m}{10}} g(f) df = \\ &= -\frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-D_g u^2(f) \frac{m}{10}} g(f) df \end{aligned} \quad (27)$$

a wówczas:

$$\hat{R} = \hat{\Delta L} - \hat{\Delta L}_0 \quad (28)$$

gdzie  $\hat{\Delta L}_0$  jest określone wzorem (21).

W celu wyznaczenia zależności liczbowych wielkości  $\hat{R}$  od argumentu  $D_g$ , zastępujemy całkowanie sumowaniem, a więc przyjmujemy, że zachodzi przybliżona równość:

$$\begin{aligned} \hat{\Delta L} &\approx -\frac{10}{m} \lg \sum_{k=1}^p G_k 10^{-\hat{D}_k \frac{m}{10}} = \\ &= -\frac{10}{m} \lg \sum_{k=1}^p G_k 10^{-D_g u_k^2 \frac{m}{10}} \end{aligned} \quad (29)$$

Przyjmując dla naturalnego pasma telefonicznego podane w tabelicy 2 wartości częstotliwości  $f_k$  i współczynników wagowych  $G_k$ , uzyskuje się następujący związek aproksymacyjny (patrz Dodatek 3):

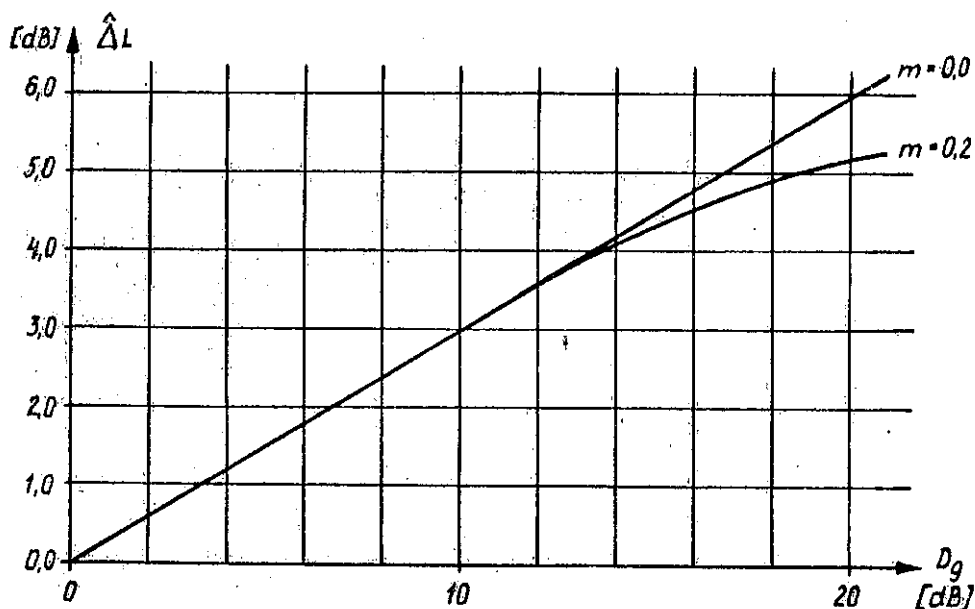
$$\hat{R} \approx -\tau m D_g^2 \quad (30)$$

gdzie

$$\tau = 8,5 \cdot 10^{-3} \text{ [dB}^{-1}\text{]}$$

Związki określone wzorami (23) oraz (30) umożliwiają stwierdzenie, że:

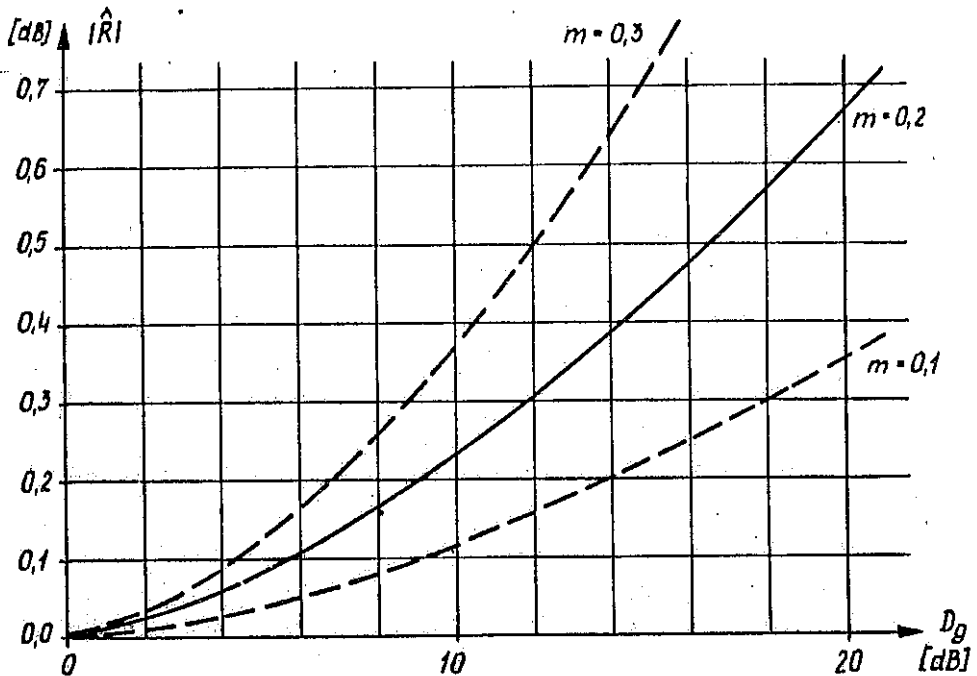
- zależność między wielkościami  $L_0$  a  $D_g$  jest linearna;
- zależność między wielkościami  $L$  a  $D_g$  jest nieliniarna;
- różnica  $R$  między wielkościami  $L$  a  $L_0$  jest błędem linearności wielkości  $L$ ; moduł tego błędu jest wprost proporcjonalny do wartości współczynnika  $m$  oraz do kwadratu wartości zniekształceń tłumieniowych  $D_g$  (patrz rys. 2 i 3).



Rys. 2. Zależność górnej granicy przyrostu tłumienności głośności  $\Delta L$  od zniekształceń tłumieniowych  $D_g$  kanału telefonicznego

Należy zwrócić uwagę, że wartość tego błędu jest nieistotna dla poszczególnych ogniw łańcuchów telefonicznych. Mianowicie dla łączy realizowanych w wielokrotnych systemach transmisyjnych o charakterystykach tłumieniowych, leżących w dopuszczalnym zakresie, tzn. dla  $D_g \leq 3$  dB przy  $m = 0,2$  zachodzi:  $|R| \leq 0,016$  dB. Natomiast dla aparatów telefonicz-

nych, których zniekształcenia tłumieniowe osiągają w praktyce wartość  $D_g \approx 10$  dB, moduł górnej granicy błędu linearności wynosi  $|R| \approx 0,17$  dB.



Rys. 3. Zależność modułu górnej granicy błędu linearności  $R$  wielkości  $L$  od zniekształceń tłumieniowych  $D_g$  kanału telefonicznego

Na zakończenie tego rozdziału trzeba podkreślić, że powyższe rozważania dotyczyły tłumienności dowolnego rodzaju, a więc: falowej, skrośnej oraz skutecznej (lub jej szczególnej postaci: wynikowej). W konkretnych zastosowaniach dotyczących projektowania oraz utrzymania sieci telefonicznej konieczne jest precyzowanie rodzaju tłumienności [14], [10].

### 3. OCENA BŁĘDÓW ADDYTYWNOŚCI TŁUMIENNOŚCI GŁOŚNOŚCI ŁAŃCUCHÓW TELEFONICZNYCH

W dokumentach CCITT [5÷6] postuluje się addytywność wielkości LR.

Jak wiadomo z klasycznej teorii czwórników [14], dla dowolnej częstotliwości  $f$  z definicji addytywną jest tylko tłumienność skrośna. Oznacza to, że tłumienność skrośna  $A_{\Sigma}$  łańcucha  $n$  czwórników jest równa sumie tłumienności skrośnych wszystkich czwórników składowych tego łańcucha<sup>1)</sup>:

$$A_{\Sigma}(f) = \sum_{i=1}^n A_i(f) \quad (31)$$

Uwzględniając zależność (8), skrośną tłumienność głośności  $i$ -tego czwórnika można wyrazić wzorem analogicznym do (10), a mianowicie:

$$L_i = A_{ic} - \frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-D_i(f) \frac{m}{10}} g(f) df \quad (32)$$

gdzie  $A_{ic}$  jest tłumiennością skrośną rozważanego czwórnika dla częstotliwości odniesienia  $f_c$ , zaś  $D_i(f)$  są zniekształceniami tłumieniowymi (skrośnymi) tego czwórnika.

Analogicznym wzorem wyraża się skrośna tłumienność głośności rozważanego łańcucha telefonicznego, a mianowicie:

$$L_{\Sigma} = A_{\Sigma c} - \frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-D_{\Sigma}(f) \frac{m}{10}} g(f) df \quad (33)$$

1) W przypadku tłumienności skrośnej zachodzi addytywność w szerokim sensie. Należy zwrócić uwagę, iż zazwyczaj operuje się pojęciem addytywności w wąskim sensie; zachodzi ona wówczas, gdy miara każdego obiektu jest wielkością jednoznacznie określoną przez właściwości samego obiektu, a więc nie zależy od jego otoczenia (tak jest np. w przypadku rezystancji). Warunek ten nie jest spełniony w przypadku tłumienności skrośnej - ta wielkość jest jednoznacznie określona przez właściwości nie tylko rozważanego czwórnika, lecz również aktualnie występującego obciążenia tego czwórnika; odpowiednie zależności podano w [10, roz.3]. W praktyce oznacza to, że tłumienność skrośna tego samego czwórnika włączanego w różne łańcuchy, jak to ma miejsce w sieci telefonicznej, wykazuje na ogół różne wartości; (w celu zmniejszenia tych różnic do dopuszczalnych granic, ustalono normy ograniczające niedopasowanie impedancyjne poszczególnych ogniw sieci).

gdzie  $A_{\Sigma c}$  jest określoną wzorem (31) tłumiennością skrośną łańcucha dla częstotliwości  $f_c$ , zaś  $D_{\Sigma}(f)$  są zniekształceniami tłumieniowymi (skrośnymi) tego łańcucha.

Uwzględniając addytywność zniekształceń tłumieniowych skrośnych, błąd addytywności  $B_n$  skrośnej tłumienności głośności  $n$ -ogniwowego łańcucha czwórników można wyrazić następująco:

$$\begin{aligned}
 B_n &= L_{\Sigma} - \sum_{i=1}^n L_i = \\
 &= \frac{10}{m} \sum_{i=1}^n \lg \int_{f_d}^{f_g} 10^{-D_i(f)} \frac{m}{10} g(f) df + \\
 &- \frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-\sum D_i(f)} \frac{m}{10} g(f) df \quad (34)
 \end{aligned}$$

Istnieją dwa alternatywne warunki dostateczne, przy spełnieniu których błąd ten staje się równy zeru, a mianowicie:

- I - gdy czwórniki wchodzące w skład rozważanego łańcucha nie wykazują zniekształceń tłumieniowych, tzn. gdy dla każdego  $i = 1, \dots, n$  zachodzi:  $D_i(f) \equiv 0$ , albo
- II - gdy wartość współczynnika  $m = 0$ .

W tym ostatnim przypadku skrośna tłumienność głośności zarówno rozważanego łańcucha, jak i jego czwórników składowych wyraża się wzorami analogicznymi do (13) i (14), a więc określony wzorem (34) błąd addytywności przyjmuje postać:

$$\begin{aligned}
 B_{no} &= L_{\Sigma o} - \sum_{i=1}^n L_{io} = \\
 &= \int_{f_d}^{f_g} \sum_{i=1}^n D_i(f) g(f) df - \sum_{i=1}^n \int_{f_d}^{f_g} D_i(f) g(f) df \equiv 0 \quad (35)
 \end{aligned}$$

W przypadku gdy współczynnik  $m > 0$ , można oszacować wartość błędu addytywności skrośnej tłumienności głośności w  $n$ -ogniwowym łańcuchu czwórników, przyjmując dla prostoty obliczeń, że zniekształcenia tłumieniowe (skrośne) każdego z czwórników składowych łańcucha są jednakowe i wynoszą:

$$D_i(f) = \frac{1}{n} D_{\Sigma}(f) \quad (36)$$

Uwzględniając (36) w (34) otrzymujemy:

$$\begin{aligned} B_n &= \frac{10n}{m} \lg \int_{f_d}^{f_g} 10^{-D_{\Sigma}(f)} \frac{m}{10n} g(f) df + \\ &- \frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-D_{\Sigma}(f)} \frac{m}{10} g(f) df \end{aligned} \quad (37)$$

Górną granicę  $\hat{B}_n$  tego błędu można obliczyć w sposób analogiczny do podanego w rozdziale 2 przyjmując, że dla rozważanego łańcucha zniekształcenia tłumieniowe (skrośne) są określone wzorem (17).

W celu wyznaczenia zależności liczbowych wielkości  $\hat{B}_n$  od argumentu  $D_g$  zastępujemy całkowanie sumowaniem, a więc przyjmujemy, że zachodzi przybliżona równość:

$$\begin{aligned} \hat{B}_n &\approx \frac{10n}{m} \lg \sum_{k=1}^p G_k 10^{-\hat{D}_k} \frac{m}{10n} + \\ &- \frac{10}{m} \lg \sum_{k=1}^p G_k 10^{-\hat{D}_k} \frac{m}{10} \end{aligned} \quad (38)$$

gdzie

$$\hat{D}_k = \hat{D}_{\Sigma}(f_k) = D_g u_k^2 \quad (39)$$

przy czym  $u_k$  jest określone wzorem (25).

Przyjmując podane w tabelicy 2 wartości częstotliwości  $f_k$  i współczynników wagowych  $G_k$ , uzyskuje się przy  $m = 0,2$  wyniki liczbowe przedstawione wykreślnie na rys. 4.

Analiza tych wyników obliczeń numerycznych umożliwia otrzymanie następującego związku aproksymacyjnego (patrz Dodatek 4):

$$\hat{B}_n \approx -\beta (m D_g^2)^c \frac{n}{n+2} \quad (40)$$

w którym:

$$\beta = 0,014 \text{ [dB}^{-(2c-1)}\text{]}; c = 0,9 \quad (41)$$

Ze wzoru (40) widać, że górna granica błędu addytywności rośnie prawie liniowo<sup>1)</sup> wraz z wartością współczynnika  $m$  i wraz z kwadratem wartości zniekształceń tłumieniowych  $D_g$ , występujących dla częstotliwości  $f_g$  górnej granicy pasma przesyłowego, a ponadto nieznacznie wzrasta wraz z liczbą  $n$  ogniw rozważanego łańcucha.

Jak widać z rys. 4, przy wartości współczynnika  $m = 0,2$ , górne granice błędu addytywności  $B_n$  skróśnej tłumienności głośności stają się istotne dla łańcuchów telefonicznych o dużych zniekształceniach tłumieniowych  $D_g$ .

Na zakończenie tego rozdziału warto zwrócić uwagę na związek między błędami: addytywności i linearności miary  $L$ . Miałowicie wyznaczając ze wzoru (30) wielkość:

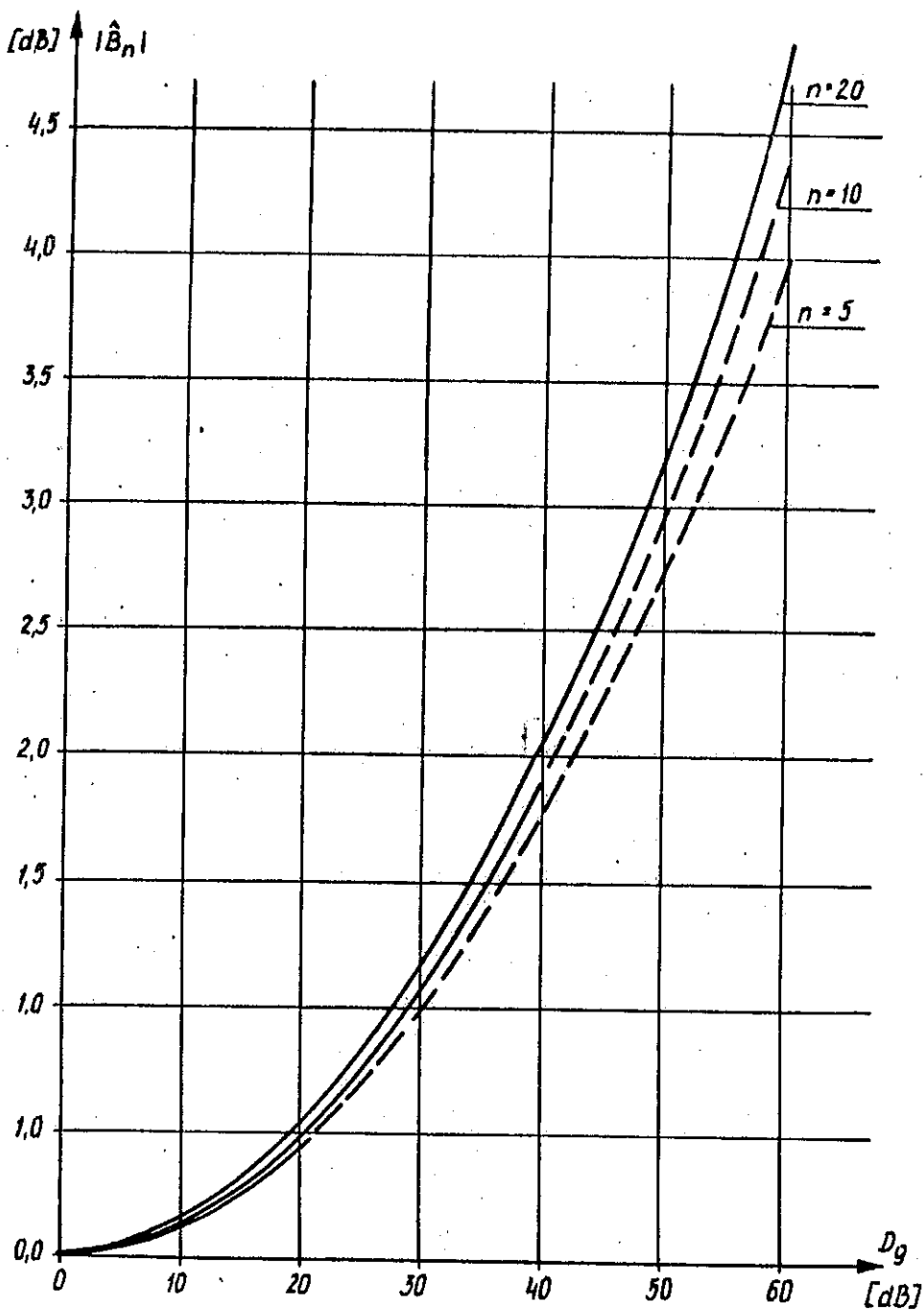
$$m D_g^2 \approx -\frac{\hat{R}}{\tau} \quad (42)$$

i podstawiając do wzoru (40), otrzymamy:

$$\begin{aligned} \hat{B}_n &\approx -\beta \left(-\frac{\hat{R}}{\tau}\right)^c \frac{n}{n+2} = \\ &= \frac{\beta}{\tau^c} \hat{R}^c \frac{n}{n+2} \end{aligned} \quad (43)$$

Ale ponieważ

$$\left(\frac{\beta}{\tau^c}\right) \approx 1 \quad (44)$$



Rys. 4. Zależność modułu górnej granicy błędu addytywności  $B_n$  wielkości  $L$  (przy  $m = 0,2$ ) od zniekształceń tłumieniowych  $D_g^n$   $n$ -ogniowego łańcucha telefonicznego



więc:

$$\hat{B}_n \approx \hat{R}^c \frac{n}{n+2} \quad (45)$$

oraz

$$\lim_{n \rightarrow \infty} \hat{B}_n \approx \hat{R}^c \quad (46)$$

Oznacza to, że błąd addytywności wielkości  $L$  wzrasta prawie liniowo<sup>1)</sup> wraz ze wzrostem błędu linearności tej wielkości.

#### 4. OCENA BŁĘDÓW WYZNACZANIA TŁUMIENNOŚCI GŁOŚNOŚCI W PRZYPADKU NIEPEWNYCH DANYCH POMIAROWYCH

Podane w rozdziale 2 zależności matematyczne umożliwiają wyznaczenie wartości tłumienności głośności  $L$  (lub  $L_0$ ) kanału (czwórnika) w przypadku, gdy tłumienności punktowe  $\{A_1, \dots, A_p\}$  (lub  $\{A_c, D_1, \dots, D_p\}$ ) tego kanału są dokładnie znane. W praktyce pomiarowej taki przypadek nigdy nie zachodzi - wyniki pomiarów zawsze są niedokładne.

Przyjmijmy, że wartości punktowych tłumienności czwórnika są wyznaczone niedokładnie, a mianowicie, że przy dowolnej częstotliwości  $f_k \in [f_d, f_g]$  wykazują taką samą wartość  $\sigma_1$  błędu standardowego niepewności, nie wykazując jednocześnie błędu poprawności. Przy takim założeniu punktowe oszacowanie  $A_k$  tłumienności rozważanego kanału (o ustalonej częstotliwościowej charakterystyce  $A(f)$  tłumienności) przy dowolnej, ale ustalonej częstotliwości  $f_k$  jest zmienną losową<sup>2)</sup> o wartości oczekiwanej równej:

$$E\{A_k\} = \bar{A}_k \quad (47)$$

i o wariancji równej:

$$V\{A_k\} = \sigma_1^2 \quad (48)$$

1) Zależność ściśle liniowa zachodzi w przypadku, gdy  $c = 1$ .

2) Uwaga: w tym opracowaniu symbole zmiennych losowych są oznaczone czcionką tłustą, a więc:  $A_k, L, L_0$ .

której wartość nie zależy od częstotliwości. W rozważanym przypadku oszacowanie  $L$  tłumienności głośności też jest zmienną losową:

$$\begin{aligned} L &= -\frac{10}{m} \lg \sum_{k=1}^p G_k 10^{-A_k \frac{m}{10}} = \\ &= -\frac{1}{\mu} \ln \sum_{k=1}^p G_k \exp(-\mu A_k) \end{aligned} \quad (49)$$

gdzie

$$\mu = \frac{m}{10} \ln 10 \quad (50)$$

Przy dodatkowym założeniu wzajemnej niezależności błędów niepewności ocen tłumienności punktowych, tzn.:

$$\text{Cov}(A_k, A_{k'}) = 0; \quad k, k' = 1, \dots, p; \quad k' \neq k \quad (51)$$

oraz wprowadzeniu oznaczenia:

$$\bar{L} = -\frac{1}{\mu} \ln \sum_{k=1}^p G_k \exp(-\mu \bar{A}_k) \quad (52)$$

otrzymujemy następujące przybliżone wyrażenia [15, §25], określające parametry rozkładu oszacowania tłumienności głośności:

- wartość oczekiwana:

$$E\{\bar{L}\} \approx \bar{L} + \frac{\sigma_1^2}{2} \sum_{k=1}^p \left[ \frac{\partial^2 \bar{L}}{\partial A_k^2} \Big|_{A_k = \bar{A}_k} \right] \quad (53)$$

- wariancja:

$$V\{\bar{L}\} \approx \sigma_1^2 \sum_{k=1}^p \left[ \frac{\partial \bar{L}}{\partial A_k} \Big|_{A_k = \bar{A}_k} \right]^2 \quad (54)$$

W przypadku gdy współczynnik  $m = 0$ , oszacowania tłumienności głośności są określone następującymi wzorami:

- zmienna losowa:

$$L_o = \sum_{k=1}^P G_k A_k \quad (55)$$

- wartość oczekiwana:

$$E\{L_o\} = \sum_{k=1}^P G_k \bar{A}_k = \bar{L}_o \quad (56)$$

- wariancja:

$$V\{L_o\} = \sigma_1^2 \sum_{k=1}^P G_k^2 \quad (57)$$

#### 4.1. Wrażliwość oszacowań tłumienności głośności

Wprowadźmy obecnie pojęcie wrażliwości wielkości  $L_o$  na błędy niepewności danych punktowych, określonej następująco:

$$W_{L_o} = \frac{1}{\sigma_1} \sqrt{V\{L_o\}} \quad (58)$$

Uwzględniając (57) otrzymamy:

$$W_{L_o} = \left[ \sum_{k=1}^P G_k^2 \right]^{\frac{1}{2}} \quad (59)$$

Analogicznie do (58), wrażliwość wielkości  $L$  na błędy niepewności danych punktowych zostaje określona jako:

$$W_L = \frac{1}{\sigma_1} \sqrt{V\{L\}} \quad (60)$$

Uwzględniając, że (patrz Dodatek 5.1):

$$\begin{aligned}
 v(\bar{L}) &\approx \sigma_1^2 \frac{\sum_{k=1}^p [G_k \exp(-\mu \bar{A}_k)]^2}{\left[ \sum_{k=1}^p G_k \exp(-\mu \bar{A}_k) \right]^2} = \\
 &= \sigma_1^2 \frac{\sum_{k=1}^p [G_k \exp(-\mu \bar{D}_k)]^2}{\left[ \sum_{k=1}^p G_k \exp(-\mu \bar{D}_k) \right]^2} \quad (61)
 \end{aligned}$$

gdzie

$$\bar{D}_k = \bar{A}_k - \bar{A}_c \quad (62)$$

otrzymamy:

$$W_L \approx \frac{\left[ \sum_{k=1}^p [G_k \exp(-\mu \bar{D}_k)]^2 \right]^{\frac{1}{2}}}{\sum_{k=1}^p G_k \exp(-\mu \bar{D}_k)} \quad (63)$$

Należy zwrócić uwagę, że określona wzorem (59) wrażliwość wielkości  $L_0$  zależy tylko od wartości współczynników wagowych  $G_k$ , osiągając minimum równe:

$$\min \{W_{L_0}\} = \frac{1}{\sqrt{p}} \quad (64)$$

w przypadku gdy wszystkie współczynniki wagowe są jednakowe, tzn. gdy dla każdego  $k=1, \dots, p$  zachodzi:

$$G_k = \frac{1}{p} \quad (65)$$

Natomiast wrażliwość wielkości  $L$  zależy również od wartości współczynnika  $m$ , a także od wartości zniekształceń tłumieniowych  $D_k$  rozważanego kanału, rosnąc wraz ze wzrostem tych zniekształceń. W przypadku gdy te zniekształcenia dążą do zera, występuje minimum wrażliwości równe:

$$\min \{W_L\} = W_{L0} \quad (66)$$

przy czym  $W_{L0}$  jest określone wzorem (59).

W celu określenia liczbowych zależności wrażliwości  $W_L$  od zniekształceń tłumieniowych kanału, przyjmijmy (identycznie jak w rozdziale 2), że górne ograniczenie zniekształceń wynosi:

$$\hat{D}_k = D_g u_k^2 \quad (67)$$

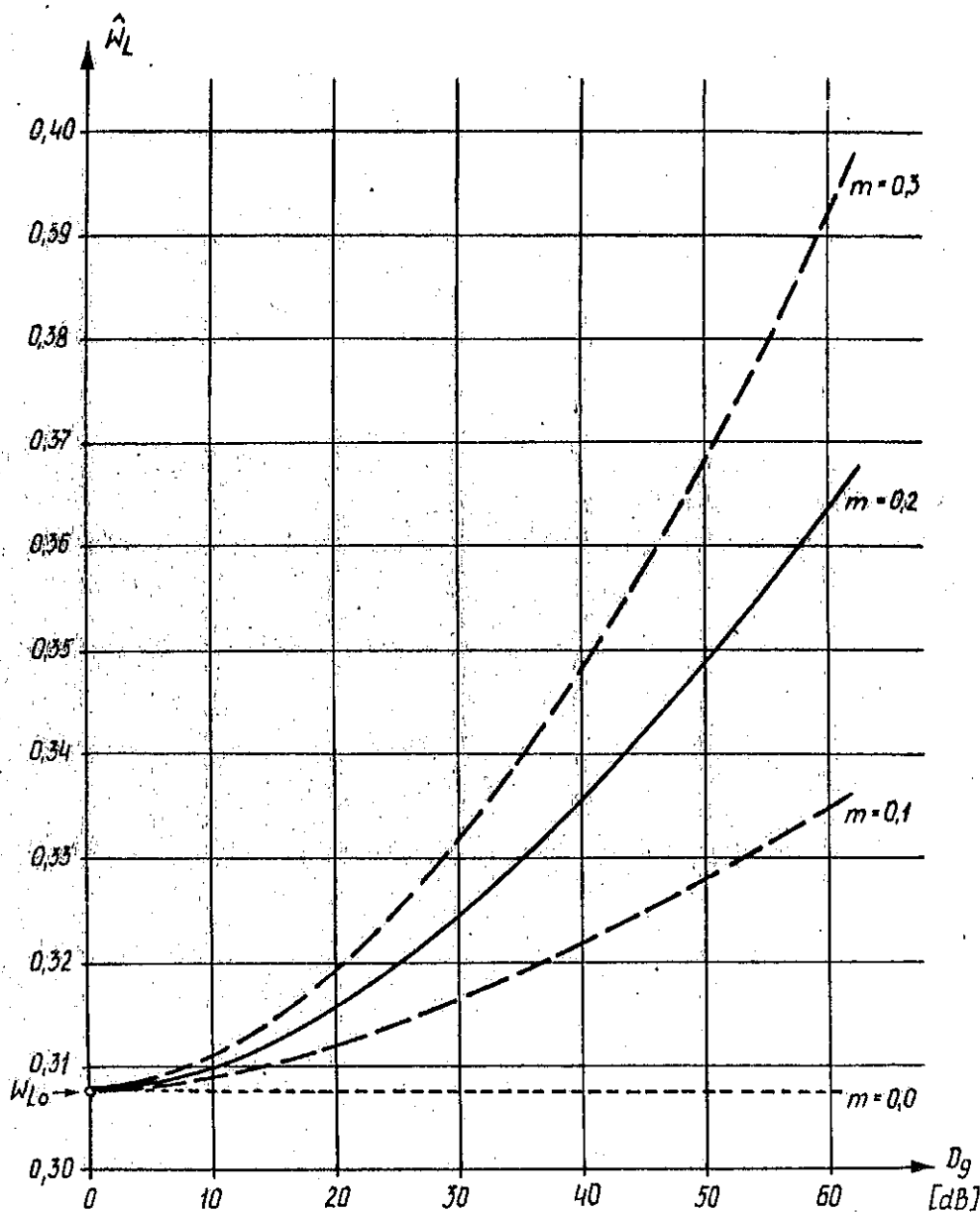
gdzie  $u_k$  jest określone wzorem (25).

Wprowadzając oznaczenie:  $c = \frac{1n}{10} \frac{10}{10}$  oraz podstawiając (50) i (67) do (63) otrzymujemy:

$$\hat{W}_L \approx \frac{\left[ \sum_{k=1}^p [G_k \exp(-c m D_g u_k^2)]^2 \right]^{\frac{1}{2}}}{\sum_{k=1}^p G_k \exp(-c m D_g u_k^2)} \quad (68)$$

Następnie przyjmując podane w tabl. 2 wartości częstotliwości  $f_k$  i współczynników wagowych  $G_k$ , otrzymujemy zależność  $\hat{W}_L(D_g; m)$  przedstawioną graficznie na rys. 5.

Przeprowadzona analiza numeryczna tej zależności umożliwiła wyznaczenie funkcji aproksymującej o postaci (patrz Dodatek 6):



Rys. 5. Zależność górnej granicy  $\hat{W}_L$  wrażliwości tłumienności głośności na błędy niepewności danych punktowych od zwiększających tłumieniowych  $D_g$  czwórników dla górnej częstotliwości  $f_g$  ( $= 3400$  Hz) pasma telefonicznego

$$\hat{W}_L \approx W_{L0} + m (k_0 + k_1 D_g + k_2 D_g^2) \quad (69)$$

przy czym występujące w tym wzorze współczynniki wynoszą:

$$\begin{aligned} W_{L0} &= 3,082 \cdot 10^{-1} \\ k_0 &= -4,02 \cdot 10^{-3} \\ k_1 &= 3,27 \cdot 10^{-3} \text{ [dB}^{-1}\text{]} \\ k_2 &= 2,42 \cdot 10^{-5} \text{ [dB}^{-2}\text{]} \end{aligned}$$

Możliwa jest również nieco mniej dokładna, ale za to prostsza postać liniowej funkcji aproksymującej, a mianowicie:

$$\hat{W}_L \approx W_{L0} + m (k'_0 + k_w D_g) \quad (70)$$

gdzie

$$\begin{aligned} k'_0 &= -1,7 \cdot 10^{-2} \\ k_w &= 4,7 \cdot 10^{-3} \text{ [dB}^{-1}\text{]} \end{aligned}$$

Warto zwrócić uwagę, że ze względu na wynikającą z (64) nierówność:

$$W_{L0} > \frac{1}{\sqrt{p}} \quad (71)$$

zachodzi związek:

$$\hat{W}_L \leq W_{L0} [1 + \sqrt{p} m (k_0 + k_w D_g)] \quad (72)$$

a ponieważ  $k'_0 < 0$ , więc:

$$\hat{W}_L < W_{L0} (1 + k_w \sqrt{p} m D_g) \quad (73)$$

#### 4.2. Obciążenie oszacowań tłumienności głośności

Z porównania wzorów (56) i (53) widać, że wielkość  $\bar{L}_0$  jest nieobciążonym estymatorem wielkości  $E\{L_0\}$ , natomiast wielkość  $\bar{L}$  jest obciążonym estymatorem wielkości  $E\{L\}$ , przy czym to

obciążenie jest wprost proporcjonalne do wariancji  $\sigma_1^2$  błędów niepewności punktowych ocen tłumienności  $A_k$  i wynosi (patrz Dodatek 5.2):

$$\begin{aligned}
 E\{\bar{L}\} - \bar{L} &\approx \frac{\sigma_1^2}{2} \left[ \sum_{k=1}^P \frac{\partial^2 L}{\partial A_k^2} \Big|_{A_k = \bar{A}_k} \right] = \\
 &= \frac{\sigma_1^2 \mu}{2} \frac{\sum_{k=1}^P \left\{ G_k \exp(-\mu \bar{A}_k) \left[ \sum_{\substack{j=1 \\ j \neq k}}^P G_j \exp(-\mu \bar{A}_j) \right] \right\}}{\left[ \sum_{k=1}^P G_k \exp(-\mu \bar{A}_k) \right]^2} = \\
 &= \frac{\sigma_1^2 \mu}{2} \frac{\sum_{k=1}^P \left\{ G_k \exp(-\mu \bar{D}_k) \left[ \sum_{\substack{j=1 \\ j \neq k}}^P G_j \exp(-\mu \bar{D}_j) \right] \right\}}{\left[ \sum_{k=1}^P G_k \exp(-\mu \bar{D}_k) \right]^2} \quad (74)
 \end{aligned}$$

Przeprowadzone w sposób analogiczny do podanego w pkt. 4.1 obliczenia numeryczne wg wzoru (74) umożliwiły też wyznaczenie wzoru aproksymacyjnego, który charakteryzuje obciążenie oceny tłumienności głośności:

$$E\{\bar{L}\} - \bar{L} \approx -k m \sigma_1^2 \quad (75)$$

gdzie współczynnik  $k \approx 0,1$  [dB<sup>-1</sup>].

Jak widać z powyższego wzoru, obciążenie oceny  $\bar{L}$  tłumienności głośności jest wprost proporcjonalne do kwadratu błędu standardowego  $\sigma_1$  niepewności ocen tłumienności  $A_k$ .

Ponieważ punktowe pomiary tłumienności wykazują bardzo mały błąd standardowy niepewności, tak że zawsze jest spełniony warunek:  $\sigma_1 < 0,3$  dB, wyznaczone ze wzoru (75) dla  $m = 0,2$



obciążenie nie przekracza wartości  $2 \cdot 10^{-3}$  dB, a więc jest zupełnie nieistotne. Dlatego w praktyce można zawsze przyjmować:

$$\epsilon\{L\} \approx \bar{L} \quad (76)$$

### 5. CHARAKTERYSTYKA ZMODYFIKOWANEJ TŁUMIENNOŚCI ODNIESIENIA I WYZNACZANIE JEJ WARTOŚCI

W rozdziałach 2 i 3 tego artykułu wykazano, że właściwości określonej wzorem (4) tłumienności głośności  $L$  są funkcją parametru  $m$ ; gdy  $m = 0$  rozważana wielkość przyjmuje postać określoną wzorem (12), a oznaczoną symbolem  $L_0$ . Ta szczególna postać rozważanej wielkości wykazuje linearność względem tłumienności  $A$  w pasmie przesyłowym czwórnikownika oraz addytywność miary przy łańcuchowym łączeniu czwórnikowników. Gdy parametr  $m > 0$ , wielkość  $L$  staje się nielinearna i nieaddytywna, przy czym błędy linearności i addytywności rosną wraz ze wzrostem wartości tego parametru.

Górną granicę błędu linearności tłumienności głośności

$$R = L - L_0 \quad (77)$$

można ocenić na podstawie wzoru (30), a górną granicę błędu addytywności

$$B_n = L_\Sigma - \sum_{i=1}^n L_i \quad (78)$$

- na podstawie wzoru (40).

Jak wynika ze wzoru (3), wielkość  $LR$  różni się od wielkości  $L$  o stałą  $L_w$ :

$$LR = L - L_w \quad (79)$$

Dlatego zmodyfikowana tłumienność odniesienia  $LR$  ma takie same właściwości jak tłumienność głośności  $L$ . Oznacza to, że jest ona tak samo nielinearna i nieaddytywna, a także wykazuje identyczną wrażliwość na losowe błędy wyznaczania jak wielkość  $L$ .

Górną granicę błędu linearności zmodyfikowanej tłumienności odniesienia

$$R = LR - LR_0 \quad (80)$$

gdzie

$$LR_0 = L_0 - L_w \quad (81)$$

można zatem ocenić na podstawie wzoru (30), tzn.:

$$\hat{R} \approx -\tau \cdot m \cdot D_g^2 \quad (82)$$

gdzie

$$\tau = 8,5 \cdot 10^{-3} \quad [\text{dB}^{-1}] \quad (83)$$

Z powyższego wzoru widać, że górna granica błędu linearności zmodyfikowanej tłumienności odniesienia jest w pierwszym przybliżeniu wprost proporcjonalna do kwadratu wartości zniekształceń tłumieniowych  $D_g$ , występujących dla częstotliwości  $f_g$  ( $\approx 3400$  Hz) górnej granicy pasma przesyłowego. Dlatego przy małych zniekształceniach tłumieniowych czwórników wartość liczbowa błędu linearności wielkości  $L$  jest do pominięcia. Obliczenia numeryczne przeprowadzone dla  $m = 0,2$  (patrz tabl. 2) wykazały, że przy  $D_g \leq 3$  dB wartość IRI jest rzędu setnej części dB, a przy  $D_g \leq 10$  dB - rzędu dziesiątej części dB. Oznacza to praktyczną zgodność ocen tłumienności według miar  $LR$  i  $LR_0$  dla poszczególnych ogniw sieci telefonicznej (wg norm: dla łączy międzycentralowych  $D_g \leq 3$  dB, a dla aparatów telefonicznych  $D_g \leq 10$  dB).

Błąd addytywności zmodyfikowanej tłumienności odniesienia, występujący przy łańcuchowym połączeniu  $n$  ogniw:

$$\beta_n = LR_\Sigma - \sum_{i=1}^n LR_i \quad (84)$$

można oszacować od góry na podstawie zależności (40), tzn.:

$$\hat{\beta}_n \approx -\beta (m D_g^2)^c \frac{n}{n+2} \quad (85)$$

w którym:

$$\beta = 0,014 \left[ \text{dB}^{-(2c-1)} \right]; c = 0,9 \quad (86)$$

Podobnie jak przy nielinearności, wartość błędu addytywności zależy głównie od zniekształceń tłumieniowych  $D_g$  rozważanego łańcucha (patrz rys. 4). Jednakże w tym przypadku, na skutek znacznej liczby  $n$  ogniw, które mogą występować w łańcuchach telefonicznych tworzonych w sieciach o przestrzennej komutacji łączy (do 20 w relacjach międzynarodowych), maksymalną wartość zniekształceń tłumieniowych  $D_g$  można ocenić na 60 dB. W takim przypadku obliczona na podstawie wzoru (85) górna granica błędu addytywności wielkości LR może osiągnąć dla  $m = 0,2$  wartość  $|\hat{\beta}_n| \approx 4,7$  dB, a więc nie jest do pominięcia w praktyce.

### 5.1. Szacowanie wartości LR

Dla celów planowania sieci telefonicznej, szacowanie zmodyfikowanej tłumienności odniesienia może być przeprowadzane na podstawie bardzo ogólnych danych, dotyczących poszczególnych rodzajów ogniw składowych tej sieci. Mianowicie, jeśli jest znana wartość znamionowa punktowej tłumienności  $A_c$  (dla częstotliwości  $f_c$  określonej wzorem (9)) ogniwa danego rodzaju oraz dopuszczalne dla tego ogniwa zniekształcenia tłumieniowe  $D_g$  (dla częstotliwości  $f_g$  górnej granicy pasma przesyłowego), to podstawiając (13) do (81) otrzymamy:

$$LR_0 = A_c - L_w + \Delta L_0 \quad (87)$$

Na podstawie wzorów (20) i (23) zachodzi związek:

$$\Delta L_0 < \delta D_g \quad (88)$$

gdzie

$$\delta \approx 0,3 \quad (89)$$

Należy przypomnieć, iż wartość tego współczynnika, podobnie jak i współczynników określonych wzorami (83) i (86) została wyznaczona przy założeniu, że charakterystyki zniekształceń tłumieniowych  $D(f)$  rozważanego obiektu są ograniczone od góry parabolą drugiego stopnia<sup>1)</sup>, określoną wzorami (17) i (18).

Na podstawie (80) mamy:

$$LR = LR_0 + R \quad (90)$$

przy czym górna granica wartości błędu linearności  $R$  jest określona wzorem (82).

Należy zwrócić uwagę, że  $R < 0$ , a więc zawsze zachodzi nierówność:

$$LR < LR_0 \quad (91)$$

Szacowanie zmodyfikowanej tłumienności odniesienia  $n$ -ogniwowych łańcuchów telefonicznych odbywa się na podstawie następujących zależności, charakteryzujących związki zachodzące między tłumiennościami skrośnymi rozważanego łańcucha i jego ogniw składowych:

$$LR_{0\Sigma} = \sum_{i=1}^n LR_{0i} \quad (92)$$

1) Warto zwrócić uwagę, że uśrednione charakterystyki zniekształceń tłumieniowych  $D(f)$  kanałów telefonicznych są z reguły bardziej spłaszczone niż parabola drugiego stopnia. Znajomość stopnia  $\theta$  spłaszczenia parabol równoważnych rzeczywistym charakterystykom zniekształceń tłumieniowych  $D(f)$  poszczególnych rodzajów czwórników tworzących kanały telefoniczne umożliwiłaby szacowanie wartości przyrostu  $\Delta L_0$  na podstawie zależności:

$$\Delta L_0 \approx \delta(\theta) D_0$$

gdzie  $\delta(\theta) < 0,3$  jest współczynnikiem zależnym od stopnia  $\theta$  spłaszczenia uśrednionych charakterystyk tłumieniowych.

oraz

$$LR_{\Sigma} = \sum_{i=1}^n LR_i + \theta_n \quad (93)$$

gdzie  $\theta_n$  jest błędem addytywności, którego górną granicę określa wzór (85).

Należy dodać, że dla każdego łańcucha zachodzi nierówność (91), tzn.:

$$LR_{\Sigma} < LR_{0\Sigma} \quad (94)$$

## 5.2. Wyznaczanie wartości LR na podstawie pomiarów

Przejdźmy obecnie do zagadnienia wyznaczania zmodyfikowanej tłumienności odniesienia czwórników na podstawie wyników pomiarów ich tłumienności punktowych, zakładając, że błąd standardowy niepewności tych pomiarów jest znany i wynosi  $\delta_1$ .

Najpierw rozważymy przypadek, gdy  $m = 0$ .

Ponieważ występująca we wzorze (81) wielkość  $L_w$  jest stałą, przy niepewnych danych pomiarowych zachodzą związki:

$$E\{LR_0\} = E\{L_0\} - L_w \approx E\{\hat{L}_0\} - L_w \quad (95)$$

oraz

$$V\{LR_0\} = V\{L_0\} \approx V\{\hat{L}_0\} \quad (96)$$

Dlatego, uwzględniając ponadto związek (56), można wyznaczać zmodyfikowaną tłumienność odniesienia mierzonego obiektu na podstawie wzoru:

$$LR_0^* = \sum_{k=1}^p G_k A_k^* - L_w \quad (97)$$

gdzie  $A_k^*$  jest wynikiem pomiaru punktowej tłumienności badanego czwórnika przy częstotliwości  $f_k$ ,  $G_k$  - współczynnikiem wagowym dla tej częstotliwości (wg tabl. 2), natomiast  $L_w$  jest stałą o wartości zależnej od rodzaju mierzonego czwórnika (wg tabl. 1).

Błąd standardowy takiego oszacowanie

$$\sigma_o = \sqrt{V\{LR\}} \approx \sqrt{V\{L_o\}} \quad (98)$$

na podstawie (58) wynosi:

$$\sigma_o = W_{L_o} \cdot \sigma_1 \quad (99)$$

gdzie współczynnik  $W_{L_o}$  jest określony wzorem (59), tzn.:

$$W_{L_o} = \left[ \sum_{k=1}^p G_k^2 \right]^{\frac{1}{2}} \quad (100)$$

Należy zwrócić uwagę, że określona wzorem (100) wrażliwość wielkości  $LR_o$  zależy tylko od wartości współczynników wagowych  $G_k$ , osiągając minimum równe:

$$\min \{W_{L_o}\} = \frac{1}{\sqrt{p}} \quad (101)$$

w przypadku gdy wszystkie współczynniki wagowe są jednakowe, tzn. gdy dla każdego  $k = 1, \dots, p$  zachodzi:

$$G_k = \frac{1}{p} \quad (102)$$

Warto zwrócić uwagę, że przy podanych w tabl. 2 wartościach współczynników  $G_k$  błąd standardowy  $\sigma_o$  wielkości  $LR_o$  jest bardzo nieznacznie większy od minimalnego, ponieważ w tym przypadku stosunek:

$$\frac{W_{L_o}}{\min \{W_{L_o}\}} = W_{L_o} \cdot \sqrt{p} \approx 1,022 \quad (103)$$

Oznacza to, że z punktu widzenia błędów niepewności ocen zmodyfikowanej tłumienności odniesienia, wyznaczanej na podstawie punktowych pomiarów tłumienności, w pkt. 4.6.3 podręcznika CCITT "Handbook on Telephonometry" [5] przyjęto korzystne wartości współczynników  $G_k$ .

Przejdźmy obecnie do przypadku, gdy  $m > 0$ .

Ponieważ występująca we wzorze (79) wielkość  $L_w$  jest stałą, przy niepewnych danych pomiarowych zachodzą związki:

$$E\{LR\} = E\{L\} - L_w \approx E\{\tilde{L}\} - L_w \quad (104)$$

oraz

$$V\{LR\} = V\{L\} \approx V\{\tilde{L}\} \quad (105)$$

Dlatego, uwzględniając ponadto związek (76), należy obliczać zmodyfikowaną tłumienność odniesienia LR mierzonego obiektu (czwórnika) na podstawie wzoru:

$$LR^* \approx -L_w - \frac{10}{m} \lg \sum_{k=1}^p G_k Q_k^* \quad (106)$$

gdzie

$$Q_k^* = 10^{-A_k^* \frac{m}{10}} \quad (107)$$

przy czym  $m$  jest współczynnikiem wzrostu głośności; znaczenia pozostałych symboli są identyczne jak we wzorze (97).

Błąd standardowy takiego oszacowania

$$\sigma = \sqrt{V\{LR\}} \approx \sqrt{V\{\tilde{L}\}} \quad (108)$$

na podstawie (60) wynosi:

$$\sigma = W_L \cdot \sigma_1 \quad (109)$$

przy czym wartość współczynnika  $W_L$ , charakteryzującego wrażliwość wielkości LR na błędy niepewności punktowych pomiarów tłumienności  $A_k$  ( $k=1, \dots, p$ ), można obliczyć na podstawie wzoru:

$$W_L^* \approx \frac{\left[ \sum_{k=1}^p [G_k Q_k^*]^2 \right]^{\frac{1}{2}}}{\sum_{k=1}^p G_k Q_k^*} \quad (110)$$

który wynika z podstawienia (107) do (63).

Należy zwrócić uwagę, że wrażliwość wielkości LR zależy nie tylko od wartości współczynników wagowych  $G_k$  ( $k=1, \dots, p$ ), lecz również od wartości współczynnika  $m$ , a także od wartości zniekształceń, tłumieniowych  $D_k$  ( $= A_k - A_G$ ) rozważanego kanału (patrz wzór (63), rosnąc wraz ze wzrostem tych zniekształceń (patrz rys. 5). W przypadku, gdy te zniekształcenia dążą do zera, występuje minimum wrażliwości równe:

$$\min \{W_L\} = W_{L0} \quad (111)$$

przy czym współczynnik  $W_{L0}$  jest określony wzorem (101).

Przy danej wartości zniekształceń tłumieniowych  $D_g$  dla częstotliwości  $f_g$  górnej granicy pasma telefonicznego, górną granicę wartości współczynnika  $W_L$  można wyznaczyć na podstawie wzoru (72), tzn.:

$$\hat{W}_L < W_{L0} (1 + k_w \sqrt{p} m D_g) \quad (112)$$

gdzie

$$k_w = 4,7 \cdot 10^{-3} \text{ [dB}^{-1}\text{]} \quad (113)$$

Na zakończenie artykułu warto zwrócić uwagę na opublikowane w [7] wyniki badań różnic

$$S = LR_g - LR$$

między subiektywnymi a obiektywnymi ocenami zmodyfikowanej tłumienności odniesienia aparatów telefonicznych, przy czym oceny obiektywne były oparte na zalecanym przez CCITT algorytmie obliczeniowym wg wzoru (106). Okazało się, że wartość skuteczna  $\phi^1$ ) tych różnic nie przekracza: 1,6 dB dla nadawczego kierunku transmisji oraz 1,4 dB dla kierunku odbiorczego.

Ponieważ górna granica modułu różnic  $R$  między wielkościami  $LR$  i  $LR_0$  dla aparatów telefonicznych została oszacowana

1) Zachodzi związek:  $\phi = \sqrt{(d^2 + s^2)}$ , gdzie  $d$  oznacza wartość średnią różnic, zaś  $s$  - ich odchylenie standardowe.



(patrz koniec rozdziału 2) na 0,17 dB, więc dla obu kierunków transmisji jest spełniony warunek:

$$|\hat{R}| \ll s \quad (115)$$

Oznacza to, że występujące w praktyce wartości różnic  $R$  określonych wzorem (80) leżą w centralnej strefie obszaru wartości różnic  $S$  określonych wzorem (114). Można zatem postawić hipotezę, że w przypadku wyznaczania wielkości  $LR_0$  wg wzoru (96), uzyskane doświadczalnie wartości skuteczne  $\$_0$  różnic  $S_0$  określonych wzorem:

$$S_0 = LR_s - LR_0 \quad (116)$$

będą tego samego rzędu wielkości, jak dotychczas zaobserwowane wartości  $\$$ .

## 6. PODSUMOWANIE I WNIOSKI

W artykule wykazano, że z metrologicznego punktu widzenia wielkość  $LR_0$  jest lepsza od wielkości  $LR$ , ponieważ jest addytywna oraz wykazuje minimalną wrażliwość na losowe błędy danych pomiarowych, występujące przy wyznaczaniu tłumienności punktowych.

Biorąc pod uwagę, że:

- projektowanie sieci telefonicznej na podstawie tłumienności zawsze odbywa się przy założeniu addytywności stosowanej miary;
- utrzymanie sieci telefonicznej w zakresie tłumienności z reguły przeprowadza się na podstawie wyników pomiarów poszczególnych ogniw sieci;
- wszystkie rodzaje ogniw sieci telefonicznej z reguły wykazują na tyle małe zniekształcenia tłumieniowe  $D_0$  dla górnej częstotliwości pasma przesyłowego, że różnice wartości miar  $LR$  i  $LR_0$ , charakteryzujących każde ogniwo dowolnego rodzaju są rzędu setnej lub co najwyżej dziesiątej części decybe-la - oznacza to pomiarową nieistotność tych różnic;

autor jest zdania, że w praktyce należy stosować obiektywną metodę wyznaczania zmodyfikowanej tłumienności odniesienia opartą na wielkości  $LR_0$ , a nie na wielkości LR.

#### PODZIĘKOWANIA

Autor wyraża wdzięczność Panu prof. dr inż. Jerzemu Dudziewiczowi oraz Panu dr n.mat.-fiz. Janowi Butkiewiczowi za bardzo wnikliwe uwagi dotyczące pierwotnej wersji tego opracowania, dzięki którym jego ostateczna postać zyskała na ścisłości i komunikatywności.

#### WYKAZ LITERATURY

1. Braun K.: Theoretische und Experimentelle Untersuchung der Bezugsdampfung und der Lautstärke. Telegraphen und Fernsprech-Technik, Nr 2, 1940.
2. Braun K.: Ein neuer Bezugsdampfungs-messer mit Objectiver Erregung und Anzeige. Telegraphen und Fernsprech-Technik, Nr 8, 1940.
3. CCITT: Yellow Book, Vol. V. ITU, 1981.
4. CCITT: Red Book, Vol. V. ITU, 1985.
5. CCITT: Handbook on Telephony. ITU, 1987.
6. CCITT: Report COM XII - R.5 (period 1985/88).
7. CCITT: Contribution COM XII - 92 (period 1985/88).
8. Dudziewicz J.: Pomiary teletransmisyjne. WKŁ, Warszawa 1975.
9. Jaworski J.: Matematyczne podstawy metrologii. WNT, Warszawa 1979.
10. Kowalski Z.: Pasmowe tłumienności czwórników i ortotelefoniczna tłumienność odniesienia. Rozprawy Elektrotechniczne, zeszyt 3/4, 1982.

11. Kowalski Z.: Ewolucja tłumienności odniesienia jako miary jakości łańcuchów telefonicznych. Referaty Problemowe Instytutu Łączności, zeszyt 88, 1988. (II wydanie - rozszerzone: Biuletyn Informatyczny Instytutu Łączności, zeszyt 11, 1988).
12. Kowalski Z.: Zmodyfikowana tłumienność odniesienia kanałów i łańcuchów telefonicznych. Referaty Problemowe Instytutu Łączności, zeszyt 90, 1988.
13. Kowalski Z.: Błędy wyznaczania zmodyfikowanej tłumienności odniesienia. Referaty Problemowe Instytutu Łączności, zeszyt 92, 1988.
14. Nowicki W.: Podstawy teletransmisji. Tom I. WKiŁ, Warszawa 1971.
15. Praca zbiorowa: Rachunek prawdopodobieństwa w problemach i zadaniach. PWN, Warszawa 1979.
16. Rumszycki L.: Matematyczne opracowanie wyników eksperymentu. WNT, Warszawa 1973.
17. Tatarkiewicz J., Witkowski A.: 2<sup>5</sup> numerycznych programów w języku BASIC. SIGMA, Warszawa 1987.
18. Żyszkowski Z.: Miernictwo akustyczne. WNT, Warszawa 1987.

## DODATKI

(Wyprowadzenia wzorów)

**Dodatek 1: Tłumienność głośności L**

Dodatek 1.1: Wyprowadzenie wzoru (6)

Wrażenie głośności dźwięków o widmie zawartym w zakresie częstotliwości  $[f_d, f_g]$  można wyrazić wzorem

$$W = \int_{f_d}^{f_g} W(f) df \quad (D1-1)$$

gdzie  $W(f)$  jest wrażeniem głośności składowego tonu o częstotliwości  $f$ .

W zakresie głośności występującym w telefonii, wrażenie głośności można aproksymować funkcją mocy  $P$  odbieranych sygnałów, o postaci

$$W(f) = P^m(f) g(f) \quad (D1-2)$$

oraz

$$W = \bar{P}^m \quad (D1-3)$$

gdzie  $P(f)$  jest mocą tonu o częstotliwości  $f$ ,  $\bar{P}$  - uśrednioną mocą dźwięków, zawartych w zakresie częstotliwości  $[f_d, f_g]$ ,  $g(f)$  - funkcją wagi unormowaną w tym zakresie, zaś  $m$  - stałym współczynnikiem.

Podstawiając (D1-3) i (D1-2) do (D1-1) otrzymujemy zależność

$$\bar{P}^m = \int_{f_d}^{f_g} P^m(f) g(f) df \quad (D1-4)$$

oraz

$$\bar{P} = \left[ \int_{f_d}^{f_g} P^m(f) g(f) df \right]^{\frac{1}{m}} \quad (D1-5)$$

Gdy sygnały są transmitowane kanałem o zależnej od częstotliwości tłumienności  $A(f)$  wyrażonej w dB, moc odbieranych sygnałów można określić następującymi funkcjami mocy  $P_0$  występującej na wejściu tego kanału; dla tonu o częstotliwości  $f$  mamy:

$$P(f) = P_0 \cdot 10^{-\frac{A(f)}{10}} \quad (D1-6)$$

oraz analogicznie dla dźwięku zawierającego całe widmo częstotliwości:

$$\bar{P} = P_0 \cdot 10^{-\frac{L}{10}} \quad (D1-7)$$

gdzie  $L$  jest tłumiennością uśrednioną w zakresie częstotliwości  $[f_d, f_g]$  mocy  $\bar{P}$  sygnałów na wyjściu rozważanego kanału.

Podstawiając (D1-6) i (D1-7) do (D1-3a) otrzymujemy

$$10^{-\frac{L_m}{10}} = \int_{f_d}^{f_g} 10^{-A(f)\frac{m}{10}} g(f) df \quad (D1-8)$$

skąd

$$-\frac{L_m}{10} = \lg \int_{f_d}^{f_g} 10^{-A(f)\frac{m}{10}} g(f) df \quad (D1-9)$$

i ostatecznie

$$L = -\frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-A(f)\frac{m}{10}} g(f) df \quad (D1-10)$$

#### Dodatek 1.2: Tłumienność głośności $L_w$ wzorca IRS

Są możliwe dwa punkty widzenia na wielkość  $L_w$  występującą przy wyznaczaniu zmodyfikowanej tłumienności odniesienia metodą obiektywną: I - wywodzący się z zasad obowiązujących przy pomiarach przeprowadzanych metodą subiektywną oraz II - - wynikający z postulatu uzyskania możliwie największej dokładności aktualnie przeprowadzanych pomiarów. W artykule przyjęto II punkt widzenia.

I: W przypadku wyznaczania tłumienności odniesienia metodą subiektywną badany obiekt jest porównywany ze wzorcem, którego właściwości transmisyjne są kontrolowane metodami obiektywnymi. Parametry transmisyjne realnie istniejącego wzorca odniesienia ulegają zmianom w czasie, przy czym kalibracja umożliwia sprowadzenie tych zmian do określonego przedziału niepewności. Takiemu realnemu wzorcowi można by zatem przypisać określone wartości parametrów rozkładu tłumienności głośności, a mianowicie: wartość średnią  $L_w$  oraz odchylenie standardowe  $\sigma_w$ .

II. W przypadku wyznaczania tłumienności odniesienia metodą obiektywną badany obiekt nie jest porównywany ze wzorcem, natomiast jest mierzona wartość  $L$  tłumienności głośności tego obiektu. Spełnienie postulatu zgodności obiektywnych i subiektywnych ocen zmodyfikowanej tłumienności odniesienia można uzyskać, wyznaczając różnice: wyników pomiarów  $L$  tłumienności głośności badanych obiektów (czwórników) oraz wartości znamionowych  $L_w$  tłumienności głośności wzorca IRS (czwórnika takiego samego rodzaju, jak badany obiekt). W tym przypadku zatem wielkość  $L_w$  charakteryzująca wzorec IRS jest stałą, a więc:  $\sigma_w \equiv 0$ .

#### Dodatek 2: Przejście graniczne $L - L_0$

##### Wprowadzenie wzorów (17) i (14)

Tłumienność głośności jest określona wzorem:

$$L = -\frac{10}{m} \lg \int_{f_d}^{f_g} 10^{-A(f) \frac{m}{10}} g(f) df \quad (D2-1)$$

W przypadku, gdy wartość parametru  $m = 0$ , wzór (D2-1) przybiera postać nieoznaczoną typu

"0/0"

i z tego względu, dla wyznaczenia granicy funkcji  $L(m)$  gdy parametr  $m \rightarrow 0$ , stosuje się regułę de l'Hospital'a.

Podstawiając:

$$10^{-A(f) \frac{m}{10}} = e^{-A(f) \frac{m}{10} \ln 10}$$

oraz

$$\frac{m}{10} \ln 10 = \mu$$

otrzymujemy:

$$L = -\frac{1}{\mu} \ln \int_{f_d}^{f_g} e^{-A(f) \mu} g(f) df \quad (D2-2)$$

W przypadku, gdy  $m \rightarrow 0$ , zachodzi:

$$\lim_{m \rightarrow 0} L = \lim_{\mu \rightarrow 0} L = \lim_{\mu \rightarrow 0} \frac{\frac{d}{d\mu} \left[ \ln \int_{f_d}^{f_g} e^{-A(f) \mu} g(f) df \right]}{-\frac{d}{d\mu} \mu} =$$

$$= \lim_{\mu \rightarrow 0} \frac{\int_{f_d}^{f_g} -A(f) e^{-A(f) \mu} g(f) df}{\int_{f_d}^{f_g} e^{-A(f) \mu} g(f) df} \quad (D2-3)$$

Ale ponieważ:

$$\lim_{\mu \rightarrow 0} e^{-A(f) \mu} = e^0 = 1 \quad (D2-4)$$

więc:

$$\lim_{\mu \rightarrow 0} L = \frac{- \int_{f_d}^{f_g} A(f) g(f) df}{- \int_{f_d}^{f_g} g(f) df} \quad (D2-5)$$

Ze względu na unormowanie funkcji gęstości wagi zachodzi:

$$\int_{f_d}^{f_g} g(f) df = 1 \quad (D2-6)$$

a więc:

$$\lim_{\mu \rightarrow 0} L = \lim_{m \rightarrow 0} L = \int_{f_d}^{f_g} A(f) g(f) df \quad (D2-7)$$

Podstawiając:

$$\hat{A}(f) = A_C + D(f) \quad (D2-8)$$

otrzymujemy również:

$$\lim_{m \rightarrow 0} L = A_C + \int_{f_d}^{f_g} D(f) g(f) df \quad (D2-9)$$

### Dodatek 3: Aproxymacja funkcji $\hat{R}(D_g, m)$

#### (Wyprowadzenie wzoru (30))

W Dodatkach 3 i 4 zastosowano symbolikę przyjętą w BASIC'u dla operacji potęgowania. Oznacza to, że zachodzi równoważność:

$$\{X^W\} = \{(X)^{\wedge}w\}$$

gdzie  $w$  oznacza wykładnik potęgi.

Wyznaczenie funkcji aproksymującej górną granicę błędu linearności:

$$\hat{R} = F(D_g, m)$$

wyrażoną wzorami: (28), (29), (23) i (24) jest możliwe w dwóch etapach:

- 1 - w którym zostaje określona funkcja  $F_1(D_g | m)$ ,
- 2 - w którym zostaje określona funkcja  $F_2(D_g, m)$ .

#### Etap 1:

Wyznaczenie zależności  $\hat{R} = F_1(D_g) \quad F_1(D_g | m=m_1)$

o postaci:  $F_1 = k_1(D_g)^{\wedge}w_1 \quad (D31-1)$

gdzie  $k_1$  i  $w_1$  są nie znanymi współczynnikami.



Dane:

przy  $D_g = D_1$  jest:  $F_1 = \hat{R}(D_1, m_1) = R_1$

przy  $D_g = D_2$  jest:  $F_1 = \hat{R}(D_2, m_1) = R_2$

ze wzoru (D31-1):

$$k_1 = \frac{F_1}{(D_g)^{w_1}} \quad (D31-2)$$

skąd:

$$\frac{R_1}{(D_1)^{w_1}} = \frac{R_2}{(D_2)^{w_1}} \quad (D31-3)$$

więc:

$$\left(\frac{D_2}{D_1}\right)^{w_1} = \frac{R_2}{R_1} \quad (D31-4)$$

i ostatecznie:

$$w_1 = \frac{\log \frac{R_2}{R_1}}{\log \frac{D_2}{D_1}} \quad (D31-5)$$

oraz:

$$k_1 = \frac{R_1}{(D_1)^{w_1}} \quad (D31-6)$$

Etap 2:

Wyznaczenie zależności  $\hat{R} \approx F_2(m) = F_2(D_g, m | D_g = D_1)$

o postaci:  $F_2 = k_2(m)^{w_2} (D_g)^{w_1} \quad (D32-1)$

gdzie  $k_2$  i  $w_2$  są nie znanymi współczynnikami.

Dane:

przy  $m = m_1$  jest:  $F_2 = \hat{R}(D_1, m_1) = R_1$ ,

przy  $m = m_2$  jest:  $F_2 = \hat{R}(D_1, m_2) = R_3$ .

ze wzoru (D32-1):

$$R_1 = k_2 (m_1)^{w_2} (D_1)^{w_1}$$

oraz

$$R_3 = k_2 (m_2)^{w_2} (D_1)^{w_1}$$

skąd:

$$\frac{R_1}{R_3} = \left( \frac{m_1}{m_2} \right)^{w_2} \quad (D32-2)$$

więc

$$w_2 = \frac{\log \frac{R_1}{R_3}}{\log \frac{m_1}{m_2}} \quad (D32-3)$$

ale porównując (D32-1) z (D31-1) mamy:

$$k_2 (m_1)^{w_2} = k_1$$

więc:

$$k_2 = \frac{k_1}{(m_1)^{w_2}} \quad (D32-4)$$

Uwzględniając (D31-6) w (D32-4) mamy ostatecznie:

$$k_2 = \frac{R_1}{(D_1)^{w_1} (m_1)^{w_2}} \quad (D32-5)$$

a wprowadzając zmianę oznaczeń:

$$w_1 = w, \quad w_2 = c \quad \text{oraz} \quad k_2 = \tau$$

otrzymujemy:

$$F_2(D_g, m) = \tau (m)^c (D_g)^w \quad (D32-6)$$

Obliczenia dokładne wg wzorów (28), (29), (23) i (24) przeprowadzono przy następujących danych liczbowych:

$$D_1 = 10 \text{ dB}; \quad D_2 = 20 \text{ dB}; \quad m_1 = 0,2; \quad m_2 = 0,3$$

i uzyskano następujące wyniki:

$$R_1 = -0,1690291; \quad R_2 = -0,6523953; \quad R_3 = -0,2491053.$$

Na podstawie tych danych obliczono wg wzorów: (D31-5), (D32-3), (D32-5) wartości współczynników wzoru aproksymacyjnego (D32-6):

$$\tau = -0,008872; \quad c = 0,9564; \quad w = 1,9485.$$

Należy zwrócić uwagę, że uzyskanie dokładnej aproksymacji funkcji określonej wzorami (28), (29), (23) i (24) w przypadku ustalonej wartości współczynnika  $m (=,02)$  jest możliwe przy założeniu dowolnej wartości wykładnika  $c$ . Natomiast krytyczne są wartości wykładnika  $w$  (ze względu na zależność  $R$  od  $D_g$ ). Jeżeli założyć  $c = 1$  oraz zaokrągloną wartość współczynnika  $w = 1,95$ , to na podstawie wzoru (D32-6) możemy otrzymać wartość współczynnika:

$$\tau = \frac{F_2}{m(D_g)^w} \quad (D32-7)$$

Następnie podstawiając:  $m = m_1$ ;  $D_g = D_1$ ;  $F_2 = \hat{R}(D_1, m_1) = R_1$  otrzymujemy:

$$\tau \approx -0,00948$$

Jeżeli założyć  $c = 1$  oraz przybliżoną wartość współczynnika  $w = 2$ , to na podstawie wzoru (D32-6) możemy otrzymać wartość współczynnika:

$$\tau = \frac{F_2}{m(D_g)^2} \quad (D32-8)$$

Następnie podstawiając:  $m = m_1$ ;  $D_g = D_1$ ;  $F_2 = \hat{R}(D_1, m_1) = R_1$  otrzymujemy:

$$\tau \approx -0,0085$$

Przeprowadzone porównanie wyników obliczeń błędu addytywności  $\hat{R}$  wg dokładnego wzoru (28) z jego oszacowaniem na podstawie wzoru (29) wykazało, że przy wartości współczynnika  $m = 0,2$  górną granicą modułu błędu oszacowania nie przekracza 0,001 dB w zakresie  $D_g \leq 10$  dB oraz 0,03 dB w zakresie  $D_g \leq 20$  dB.

#### Dodatek 4: Aproksymacja funkcji $\hat{B}_n(D_g, m, n)$

##### (Wyprowadzenie wzoru (40))

Wyznaczenie funkcji aproksymującej górną granicę błędu addytywności:

$$\hat{B}_n = F(D_g, m, n)$$

wyrażoną dokładnym wzorem (38), jest możliwe w trzech etapach:

- 1 - w którym zostaje określona funkcja  $F_1(D_g | m, n)$ ,
- 2 - w którym zostaje określona funkcja  $F_2(D_g, m | n)$ ,
- 3 - w którym zostaje określona funkcja  $F_3(D_g, m, n)$ .

##### Etap 1:

Wyznaczenie zależności  $\hat{B}_n \approx F_1(D_g) = F_1(D_g | m=m_1, n=n_1)$

o postaci:  $F_1 = k_1 (D_g)^{w_1}$  (D41-1)

gdzie  $k_1$  i  $w_1$  są nie znanymi współczynnikami.

Dane:

przy  $D_g = D_1$  jest:  $F_1 = \hat{B}_n(D_1, m_1, n_1) = B_1$

przy  $D_g = D_2$  jest:  $F_2 = B_n(D_2, m_1, n_1) = B_2$

ze wzoru (D41-1):

$$k_1 = \frac{F_1}{(D_g)^{w_1}} \quad (D41-2)$$

skąd:

$$\frac{B_1}{(D_1)^{w_1}} = \frac{B_2}{(D_2)^{w_1}} \quad (D41-3)$$

więc:

$$\left(\frac{D_2}{D_1}\right)^{w_1} = \frac{B_2}{B_1} \quad (D41-4)$$

i ostatecznie:

$$w_1 = \frac{\log \frac{B_2}{B_1}}{\log \frac{D_2}{D_1}} \quad (D41-5)$$

oraz:

$$k_1 = \frac{B_1}{(D_1)^{w_1}} \quad (D41-6)$$

Etap 2:

Wyznaczenie zależności  $\hat{\theta}_n \approx F_2(m) = F_2(D_g, m | D_g = D_1, n = n_1)$

o postaci:  $F_2 = k_2(m)^{w_2} (D_g)^{w_1} \quad (D42-1)$

gdzie  $k_2$  i  $w_2$  są nie znanymi współczynnikami.

Dane:

przy  $m = m_1$  jest:  $F_2 = \hat{\theta}_n(D_1, m_1, n_1) = B_1$

przy  $m = m_2$  jest:  $F_2 = \theta_n(D_1, m_2, n_1) = B_3$

ze wzoru (D42-1):

$$B_1 = k_2(m_1)^{w_2} (D_1)^{w_1}$$

oraz

$$B_3 = k_2(m_2)^{w_2} (D_1)^{w_1}$$

skąd:

$$\frac{B_1}{B_3} = \left( \frac{m_1}{m_2} \right)^{w_2} \quad (D42-2)$$

więc:

$$w_2 = \frac{\log \frac{B_1}{B_3}}{\log \frac{m_1}{m_2}} \quad (D42-3)$$

ale porównując (D42-1) z (D-41-1) mamy:

$$k_2 (m_1)^{w_2} = k_1$$

więc:

$$k_2 = \frac{k_1}{(m_1)^{w_2}} \quad (D42-4)$$

### Etap 3:

Wyznaczenie zależności  $\hat{B}_n \approx F_3(n) \equiv F_3(D_g, m, n | D_g = D_1, m = m_1)$

o postaci:

$$F_3 = k_3 \frac{1}{n + w_3} (m)^{w_2} (D_g)^{w_1} \quad (D43-1)$$

gdzie  $k_3$  i  $w_3$  są nie znanymi współczynnikami.

Dane:

przy  $n = n_1$  jest:  $F_3 = \hat{B}_n(D_1, m_1, n_1) = B_1$

przy  $n = n_2$  jest:  $F_3 = B_n(D_1, m_1, n_2) = B_4$

ze wzoru (D43-1) mamy:

$$B_1 = k_3 \frac{n_1}{n_1 + w_3} (m_1)^{w_2} (D_1)^{w_1}$$

oraz:

$$B_4 = k_3 \frac{n_2}{n_2 + w_3} (m_1)^{w_2} (D_1)^{w_1}$$

skąd:

$$\frac{B_1}{B_4} = \frac{n_1 (n_2 + w_3)}{n_2 (n_1 + w_3)}$$

a więc:

$$(n_1 + w_3) n_2 B_1 = (n_2 + w_3) n_1 B_4$$

$$w_3 (n_1 B_4 - n_2 B_1) = n_1 n_2 (B_1 - B_4)$$

i ostatecznie:

$$w_3 = \frac{n_1 n_2 (B_1 - B_4)}{n_1 B_4 - n_2 B_1} \quad (D43-2)$$

Porównując (D43-1) z (D42-1) mamy:

$$k_3 \frac{n_1}{n_1 + w_3} = k_2$$

więc:

$$k_3 = k_2 \left( 1 + \frac{w_3}{n_1} \right) \quad (D43-3)$$

Uwzględniając (D42-4) i (D41-6) w (D43-3) mamy:

$$k_3 = \frac{B_1 \left( 1 + \frac{w_3}{n_1} \right)}{(D_1)^{w_1} (m_1)^{w_2}} \quad (D43-4)$$

a wprowadzając zmianę oznaczeń:

$$w_1 = w, \quad w_2 = c, \quad w_3 = n_0 \quad \text{oraz} \quad k_3 = \beta$$

otrzymujemy:

$$F_3(D_g, m, n) = \beta \frac{n}{n+n_0} (m)^c (D_g)^w \quad (D43-5)$$

Ponadto oznaczając:

$$s = \frac{w}{c}$$

otrzymujemy ostatecznie:

$$F_3(D_g, m, n) = \beta \frac{n}{n+n_0} [m(D_g)^s]^c \quad (D43-6)$$

Obliczenia dokładne wg wzoru (38) przeprowadzono przy następujących danych liczbowych:

$$D_1=30 \text{ dB}; \quad D_2=60 \text{ dB}; \quad m_1=0,2; \quad m_2=0,3; \quad n_1=20; \quad n_2=4$$

i uzyskano następujące wyniki:

$$B_1 = 1,336238; \quad B_2 = 4,733270; \quad B_3 = 1,887049; \quad B_4 = 3,550261$$

Na podstawie tych danych obliczono wg wzorów: (D41-5), (D42-3), (D43-2) i (D43-4) wartości współczynników wzoru aproksymacyjnego (D43-5):

$$\beta = 0,01157; \quad c = 0,85126; \quad w = 1,82466; \quad n_0 = 1,81749$$

Należy zwrócić uwagę, że uzyskanie dokładnej aproksymacji funkcji określonej wzorem (38) w przypadku ustalonej wartości współczynnika wzrostu głośności  $m$  ( $=0,2$ ) jest możliwe przy założeniu dowolnej wartości wykładnika  $c$ . Natomiast krytyczne są wartości wykładnika  $w$  (ze względu na zależność  $B_n$  od  $D_g$ ) oraz współczynnika  $n_0$  (ze względu na zależność  $B_n$  od  $n$ ). Jeżeli założyć następujące przybliżone wartości współczynników:  $w = 1,8$  oraz  $n_0 = 2$ , a także przyjąć, że  $s = 2$ , to  $c = 0,9$  i na podstawie wzoru (D43-6) możemy otrzymać wartość współczynnika:

$$\beta = \frac{F_3}{(mD_g^2)^c} \frac{n + n_0}{n} \quad (D43-7)$$



Następnie podstawiając:  $m = m_1$ ;  $D_g = D_2$ ;  $n = n_1$ ;  $F_3 = \hat{B}_n(D_2, m_1, n_1) = B_2$  otrzymujemy:

$$\beta \approx 0,014$$

Przeprowadzone porównanie wyników obliczeń błędu addytywności  $B_n$  wg dokładnego wzoru (38) z jego oszacowaniem na podstawie wzoru (40) wykazało, że przy wartości współczynnika  $m = 0,2$  górną granicą modułu błędu oszacowania nie przekracza 0,1 dB w zakresie  $D_g \leq 60$  dB oraz  $n = 2 \div 20$ .

#### Dodatek 5: Pochodne funkcji $L(\{A_k\})$ ; $k=1, \dots, p$

Punktowe oszacowanie tłumienności głośności  $L$  jest funkcją  $p$  argumentów:  $A_1, \dots, A_p$ , określoną wzorem (49):

$$L = -\frac{1}{\mu} \ln \Sigma_p \quad (05-1)$$

gdzie

$$\mu = \frac{m}{10} \ln 10 \quad (05-2)$$

$$\Sigma_p = \sum_{k=1}^p S_k \quad (05-3)$$

$$S_k = G_k \exp(-\mu A_k) \quad (05-4)$$

#### Dodatek 5.1: wyprowadzenie wzoru (61)

Pierwsza pochodna cząstkowa:

$$\frac{\partial L}{\partial A_k} = -\frac{1}{\mu} \frac{1}{\Sigma_p} \frac{d}{dA_k} \Sigma_p \quad (05-5)$$

a ponieważ

$$\frac{d}{dA_k} \Sigma_p = \frac{d}{dA_k} \sum_{j=1}^p S_j = \frac{d}{dA_k} S_k = -\mu G_k \exp(-\mu A_k) \quad (D5-6)$$

więc:

$$\frac{\partial \dot{I}}{\partial A_k} = \frac{G_k \exp(-\mu A_k)}{\sum_{j=1}^p G_j \exp(-\mu A_j)} = \frac{S_k}{\Sigma_p} \quad (D5-7)$$

a zatem:

$$\sum_{k=1}^p \left[ \frac{\partial \dot{I}}{\partial A_k} \right]^2 = \frac{\sum_{k=1}^p S_k^2}{\left[ \Sigma_p \right]^2} = \frac{\sum_{k=1}^p \left[ G_k \exp(-\mu A_k) \right]^2}{\left[ \sum_{k=1}^p G_k \exp(-\mu A_k) \right]^2} \quad (D5-8)$$

#### Dodatek 5.2: wyprowadzenie wzoru (73)

Druga pochodna cząstkowa:

$$\begin{aligned} \frac{\partial}{\partial A_k} \left[ \frac{\partial \dot{I}}{\partial A_k} \right] &= \frac{\partial}{\partial A_k} \left[ \frac{S_k}{\Sigma_p} \right] = \frac{\Sigma_p (S_k)' - S_k (\Sigma_p)'}{(\Sigma_p)^2} = \\ &= \frac{\Sigma_p (-\mu S_k) - S_k (-\mu S_k)}{(\Sigma_p)^2} = \frac{-\mu S_k (\Sigma_p - S_k)}{(\Sigma_p)^2} = \\ &= \frac{-\mu G_k \exp(-\mu A_k) \left[ \sum_{j=1; j \neq k}^p G_j \exp(-\mu A_j) \right]}{\left[ \sum_{k=1}^p G_k \exp(-\mu A_k) \right]^2} \quad (D5-9) \end{aligned}$$

a zatem:

$$\sum_{k=1}^p \left[ \frac{\partial^2 L}{\partial A_k^2} \right] = \frac{-\mu \sum_{k=1}^p \left\{ G_k \exp(-\mu A_k) \left[ \sum_{j=1; j \neq k}^p G_j \exp(-\mu A_j) \right] \right\}}{\left[ \sum_{k=1}^p G_k \exp(-\mu A_k) \right]^2} \quad (05-10)$$

Dodatek 6: Aproksymacja funkcji  $\hat{W}_L(D_g; m)$

Zastosowano aproksymację określoną wzorem (68) funkcji  $\hat{W}_1 \cong \hat{W}_L(D_g; m)$  wielomianem n-tego stopnia o postaci:

$$W_n(D_g; m) = \sum_{k=0}^n a_k D_g^k \quad (06-1)$$

gdzie współczynniki

$$a_k \cong A_k(m) \quad (06-2)$$

zostały wyznaczone opisaną w [16, rozdz. 3] metodą minimalizacji średniokwadratowej różnic wartości funkcji  $\hat{W}_L$  i wielomianu  $W_n$  w  $N$  ( $> n$ ) punktach:

$$S_N^2 = \sum_{i=1}^N (\hat{W}_{Li} - W_{ni})^2 \quad (06-3)$$

gdzie

$$\hat{W}_{Li} \cong W_L(D_{gi}; m) \quad (06-4)$$

$$W_{ni} \cong \sum_{k=0}^n a_k D_{gi}^k \quad (06-5)$$

Obliczenia numeryczne przeprowadzono za pomocą opisaną w [17] procedurę NKWIEL, wyznaczającą nie tylko współczynniki  $a_k$ , lecz również miarę jakości aproksymacji w postaci współczynnika korelacji  $R$  między wartościami funkcji  $\hat{W}_{Li}$  a wartościami wielomianu  $W_{ni}$  w  $N$  wybranych punktach  $D_{gi}$  ( $i=1, \dots, N$ ).

Przyjmując wielomian stopnia  $n = 2$  oraz liczbę  $N = 13$  par danych liczbowych  $(D_{gi}, \hat{W}_{Li})$ , gdzie  $i = 1, \dots, N$ , uzyskano w zakresie  $D_g \in [0 \div 60]$  dB bardzo dobrą jakość dopasowania aproksymaty do funkcji (68): o współczynniku korelacji  $R = 0,9997$ .

W tym przypadku wartości współczynników  $k$  występujących we wzorze (69) obliczono następująco:

$$k_0 = \frac{1}{m} (a_0 - W_{L0}) \quad (D6-6)$$

$$k_1 = \frac{a_1}{m} \quad (D6-7)$$

$$k_2 = \frac{a_2}{m} \quad (D6-8)$$

Przyjmując wielomian stopnia  $n = 1$  oraz liczbę  $N = 13$  par danych liczbowych  $(D_{gi}, \hat{W}_{Li})$ , gdzie  $i = 1, \dots, N$ , uzyskano w zakresie  $D_g \in [0 \div 60]$  dB dobrą jakość dopasowania aproksymaty do funkcji (68): o współczynniku korelacji  $R = 0,996$ .

Збигнев Ковальски /Хабданк/

#### АНАЛИЗ СВОЙСТВ МОДИФИЦИРОВАННОГО ОТНОСИТЕЛЬНОГО ЭКВИВАЛЕНТА ЗАТУХАНИЯ

#### Резюме

В статье проводится анализ свойств модифицированного относительного эквивалента затухания LR, который рекомендуется МККТТ для оценки качества телефонных цепей и их составных звеньев. Величина LR объекта /четырёхполюсника любого типа: электрического, электроакустического и акусто-электрического или акустического/ была рассчитана на основании точного математического определения связывающего эту скалярную величину с затуханием A испытываемого объекта

в диапазоне акустических частот. Уточнение этой функциональной зависимости доло возможность проведения анализа линейности и аддитивности величин LR а также определения влияния случайных ошибок расчета точечного затухания  $A$  на ошибки оценки величин LR испытываемых объектов.

Zbigniew Kowalski (Habdank)

### ANALYSIS OF LOUDNESS RATING ATTRIBUTES

#### Summary

In the paper an analysis was carried out of attributes of loudness rating LR which was recommended by CCITT for quality evaluation of telephone chains and their component links. Loudness rating LR of an object (four-terminal network of any kind: electric, electroacoustic, acoustoelectric or acoustic) was defined on the base of a rigorous mathematic definition functionally relating their scalar magnitude to the attenuation  $A$  of the tested object in the range of acoustic frequencies. The specifying of this functional relation has enabled to accomplish an analysis of linearity and addivity of the LR magnitudes and to define the influence of random errors of a determination of a point attenuation  $A$  on evaluation errors of LR magnitudes of the tested objects.

Zbigniew Kowalski (Habdank)

### ANALYSE DES PROPRIÉTÉS DE L'AFFAIBLISSEMENT DE RÉFÉRENCE MODIFIÉ

#### Résumé

On a effectué l'analyse des propriétés de l'affaiblissement modifié de référence LR, recommandé par CCITT comme un

instrument d'évaluation de la qualité des chaînes téléphoniques de transmission et de leurs parties composantes. Valeur LR d'un objet (du quadripole de type quelconque: électrique, électroacoustique, acoustico-électrique ainsi que acoustique) est défini à partir de la définition stricte mathématique qui lie de façon fonctionnel cette valeur scalaire avec l'affaiblissement  $A$  de l'objet en question, dans la bande des fréquences acoustiques. Grâce à cette fonction on a eu la possibilité de faire l'analyse de la linéarité et de l'additivité de la LR ainsi que de déterminer l'influence des erreurs aléatoires qui se manifestent en cours de détermination de l'affaiblissement ponctuel  $A$  sur les erreurs de l'évaluation des valeurs LR des objets soumis à l'examen.

Zbigniew Kowalski (Habdank)

#### ANALYSE DER EIGENSCHAFTEN DER MODIFIZIERTEN BEZUGSDÄMPFUNG

##### Zusammenfassung

In dem Artikel wurde die Analyse der Eigenschaft der modifizierten Bezugsdämpfung LR durchgeführt, die für die Abschätzung der Qualität der Fernspreverbindungen und deren Teile von CCITT empfohlen wurde. Die Grösse der LR eines Objektes (elektrisches, elektroakustisches oder akustisches Vierpoles) wurde auf Grund der genauen mathematischen Definition bestimmt, die diese skalare Grösse mit Dämpfung  $A$  des geprüften Objektes im akustischen Frequenzbereich verbindet. Präzisierung der funktionalen Abhängigkeit ermöglichte die Vollendung der Analyse der Linearität und Additivität der LR-grösse, wie auch die Bestimmung des Einflusses der Zufallsfehler der Bestimmung der Punktdämpfungen  $A$  auf die Fehler der Schätzung der LR-grösse der geprüften Objekte.

Jan Bogucki

621.372.8

**NIEJEDNORODNE LINIE TRANSMISYJNE Z ROZKŁADEM WYKŁADNICZYM  
COSINUS-KWADRAT I PARABOLICZNYM**

Rękopis dostarczono do Komitetu Redakcyjnego dn. 1989.01.10

W artykule podano równania na wartość impedancji zespolonej transmitowanej przez odcinek bezstratnej, niejednorodnej linii transmisyjnej z rozkładem wykładniczym, cosinus-kwadrat i parabolicznym. Równania te użytko, rozwiązując równania różniczkowe drugiego rzędu (Riccati) w zależności od impedancji niejednorodnej linii i jej długości. Równania te są użyteczne przy rozwiązywaniu zagadnienia niedopasowania.

Falowód - w ogólnym przypadku - jest filtrem górnoprzepustowym. Poprzez zawężanie szerszego boku falowodu można uzyskać dowolną częstotliwość graniczną (dla rodzaju podstawowego). Dla częstotliwości mniejszych od częstotliwości granicznej fala jest silnie tłumiona, natomiast dla częstotliwości wyższych od tej częstotliwości występuje pasmo przepustowe falowodu. Bezpośrednie połączenie falowodu "normalnego", np. z falowodem zawężonym jest przyczyną powstania dość dużych strat wynikłych z niedopasowania impedancji w pasmie przepustowym. Dlatego też w układach mikrofalowych jedną z najbardziej istotnych spraw jest dopasowanie impedancji toru łączącego źródło z odbiornikiem. Przy dopasowaniu uzyskuje się maksymalną sprawność przenoszenia, optymalne warunki pracy generatora oraz minimalne straty w układzie wynikłe z niedopasowania. Zadanie łączenia przesyłowych linii o różnych standardach z możliwie małym współczynnikiem odbicia spełniają transformatory impedancji, wśród których najczęściej są stosowane przejścia płynne z rozkładem wykładniczym, cosinus-kwadrat czy parabolicznym.

Przy projektowaniu transformatora z reguły przyjmuje się, że przyczyną odbicia fali jest wyłącznie skok impedancji. W rzeczywistości w liniach przesyłowych w płaszczyznach połączenia dwóch linii o różnych impedancjach powstają wyższe rodzaje fal. Mimo że żaden z wyższych rodzajów nie może rozchodzić się w falowodzie, to te typy fal wchodzą do równań określających składowe pola w płaszczyźnie styku, co jest przyczyną zmiany modułu i argumentu współczynnika odbicia dla podstawowej fali w płaszczyźnie skoku impedancji. Wpływ wyższych typów fal ma indukcyjny charakter, inaczej mówiąc, w miejscu styku pojawia się tak jakby przewodność indukcyjna.

W wielu opracowaniach [2, 5, 8] omawia się analizę niejednorodnych linii transmisyjnych. Jednakże większość z nich sugeruje użycie wykresu Smith'a dla rozwiązania problemu dopasowania, który nie może być w rzeczywistości użyty, jeśli impedancja ma charakter zespolony a nie rzeczywisty. W niniejszym artykule podano równania na obliczenie impedancji wejściowej niejednorodnej linii transmisyjnej z rozkładem wykładniczym, cosinus-kwadrat i parabolicznym.

## 1. RÓWNANIA RÓŻNICZKOWE DLA IMPEDANCJI WEJŚCIOWEJ

W jednorodnej linii o charakterystycznej impedancji  $Z_0$  i impedancji obciążenia  $Z_a$ , która jest transmitowana na odległość " $l$ " (do generatora), oporność wejściowa  $Z_{in}$  wynosi:

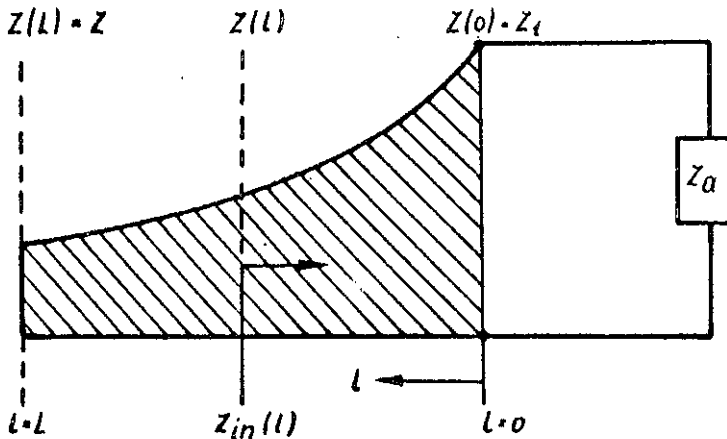
$$\frac{Z_{in}}{Z_0} = \frac{Z_a + jZ_0 \operatorname{tg} \beta l}{Z_0 + jZ_a \operatorname{tg} \beta l} \quad (1)$$

Impedancja niejednorodnej linii transmisyjnej  $Z_0$  jest funkcją odległości  $l$  i dlatego jej wartość należy zapisać  $Z(l)$ . Dla uproszczenia oznaczymy  $Z(l) = Z$ .

Definiując wyrażenie na impedancję wejściową (rys. 1), oznaczymy impedancję  $Z_{in}$  dla  $l$  oraz  $(Z_{in} + dZ_{in})$  dla  $(l + dl)$ . Jeżeli przyjąć, że linia będzie jednorodna o "impedancji charakterystycznej"  $Z$  poprzez przyrost długości  $dl$ , to:



$$\frac{Z_{in} + dZ_{in}}{Z} = \frac{Z_{in} + jZ \operatorname{tg}(\beta dl)}{Z + jZ_{in} \operatorname{tg}(\beta dl)} \quad (2)$$



Rys. 1. Niejednorodna linia transmisyjna

Dla małych wartości  $\beta dl$ , można przyjąć  $\operatorname{tg}(\beta dl) = (\beta dl)$ , wówczas:

$$\frac{dZ_{in}}{dl} = \frac{-j\beta Z_{in}^2}{Z} + j\beta Z \quad (3)$$

Równanie (3) jest zwane równaniem Riccati, które może być przetransformowane do jednorodnego liniowego równania różniczkowego drugiego rzędu.

Po transformacji [6] mamy:

$$Z_{in} = \frac{Z}{j\beta} \frac{1}{u} \frac{du}{dl} \quad (4)$$

Korzystając z (3) i (4) można napisać:

$$\frac{d^2u}{dl^2} + \left( \frac{1}{Z} \frac{dZ}{dl} \right) \frac{du}{dl} + \beta^2 u = 0 \quad (5)$$

## 2. LINIA Z ROZKŁADEM WYKŁADNICZYM

Wzdłuż wykładniczego transformatora  $\ln Z(l)$  zmienia się liniowo ze zmianą  $l$ :

$$\ln Z = \ln Z_1 + \frac{l}{L} \ln \left( \frac{Z_2}{Z_1} \right) \quad (6)$$

Różniczkując (6) względem  $l$  i korzystając z (5) mamy:

$$\frac{d^2 u}{dl^2} + \left[ \frac{1}{L} \ln \left( \frac{Z_2}{Z_1} \right) \right] \frac{du}{dl} + \beta^2 u = 0 \quad (7)$$

Rozwiązując (7) otrzymuje się:

$$\frac{Z_{in}}{Z(l)} = \frac{Z_a \left[ \frac{1}{\lambda_g} - \frac{1}{\lambda_c} \operatorname{tg} \left( \frac{2\pi l}{\lambda_g} \right) \right] + j \frac{Z_1}{\lambda} \operatorname{tg} \left( \frac{2\pi l}{\lambda_g} \right)}{Z_1 \left[ \frac{1}{\lambda_g} + \frac{1}{\lambda_c} \operatorname{tg} \left( \frac{2\pi l}{\lambda_g} \right) \right] + j \frac{Z_a}{\lambda} \operatorname{tg} \left( \frac{2\pi l}{\lambda_g} \right)} \quad (8)$$

gdzie:

$$\lambda_g = \frac{\lambda}{\sqrt{1 - \left( \frac{\lambda}{\lambda_c} \right)^2}}$$

$$\lambda_c = 4\pi L \ln \left( \frac{Z_1}{Z_2} \right)$$

## 3. LINIA Z ROZKŁADEM COSINUS-KWADRAT

Również w przypadku linii z rozkładem cosinus-kwadrat, impedancja linii transmisyjnej jest funkcją odległości i dla odległości  $l$  od obciążenia:

$$Z = a \cos^2 bl \quad (9)$$

gdy:

$$l = 0 \quad Z(0) = Z_1 = a$$

$$l = L \quad Z(L) = Z_2 = Z_1 \cos^2 bl$$

$$b = \frac{1}{L} \cos^{-1} \left( \frac{Z_2}{Z_1} \right)$$

Korzystając z (5) i (9) mamy:

$$\frac{d^2 u}{dl^2} + (-2b \operatorname{tg} bl) \frac{du}{dl} + \beta^2 u = 0 \quad (10)$$

Rozwiązując równanie (10) otrzymuje się:

$$\frac{Z_{in}}{Z(l)} = \sqrt{1 + \left(\frac{b}{\beta}\right)^2} \left\{ \frac{Z_a + j \left( \sqrt{1 + \left(\frac{b}{\beta}\right)^2} \right) Z_1 \operatorname{tg} \sqrt{\beta^2 + b^2} l}{Z_1 \sqrt{1 + \left(\frac{b}{\beta}\right)^2} + j Z_a \operatorname{tg} \sqrt{\beta^2 + b^2} l} \right\} - j \frac{b}{\beta} \operatorname{tg} \beta l \quad (11)$$

#### 4. PRZEJŚCIE PARABOLICZNE

Impedancja transmisyjnej linii zmienia się wraz z odlegością  $l$ :

$$Z = (a + bl)^2 \quad (12)$$

gdy:

$$l = 0 \quad Z(0) = Z_1 = a^2$$

$$l = L \quad Z(L) = Z_2 = (a + bL)^2$$

Dlatego:

$$b = \frac{\pm \sqrt{Z_2} - \pm \sqrt{Z_1}}{L}$$

Korzystając z (5) i (12) mamy:

$$\frac{d^2 u}{dt^2} + \left( \frac{2b}{a + \alpha l} \right) \frac{du}{dt} + \beta^2 u = 0 \quad (13)$$

Rozwiązując (13) otrzymuje się:

$$\frac{Z_{in}}{Z(l)} = \frac{Z_a - j Z_1 \left( \frac{b}{a\beta} + \operatorname{tg} \beta l \right)}{\left( \frac{b}{a\beta} \operatorname{tg} \beta l + 1 \right) Z_1 + j Z_a \operatorname{tg} \beta l} + j \frac{b}{\beta \sqrt{Z}} \quad (14)$$

## 5. WNIOSKI

Otrzymane równania (8), (11) i (14) pozwalają obliczyć wartość impedancji zespolonej transformowanej przez odcinek bezstratnej niejednorodnej linii transmisyjnej z rozkładem wykładniczym, cosinus-kwadrat i parabolicznym. Powinny być one użyteczne przy rozwiązywaniu problemów dopasowania impedancji w obwodach mikrofalowych.

## WYKAZ LITERATURY

1. Altman Ł.: Ustrojstwa swierchwysokich czastot. Moskwa 1968.
2. Berquist A.: Wave propagation on nonuniform transmission lines. IEEE Trans. Microwave Theory Techn., vol. MTT-20, 1972.
3. Bogucki J.: Falowodowy transformator impedancji w płaszczyźnie H pracujący w pobliżu częstotliwości krytycznej. Przegląd Telekomunikacyjny, nr 2, 1979.
4. Bogucki J.: Straty wywołane niedopasowaniem a wymiary falowodu. Wiadomości Telekomunikacyjne, nr 5, 1987.
5. Das D., Rustogi O.P.: Uniform transmission line equivalence of cascaded exponential lines. IEEE Trans. Microwave Theory Techn., vol. MTT-16, 1968.

6. Davis H.T.: Introduction to Nonlinear Differential and Integral Equations. Dover, New York 1962.
7. Feldsztajn A., Jawicz L., Smirnow W.: Sprawotchnik po elementam volnovodnoi techniki. Moskva. 1967.
8. Ghose R.N.: Exponential transmission lines as resonators and transformes. IRE Trans. Microwave Theory Techn., vol. MTT-5, 1957.
9. Jawicz L.: Ob odnom metodje sinteza stupentchätyh perehodov. Radio-technika, No 1, 1972.
10. Kamiński F.: Projektowanie torów dopasowywujących. Prace PIT, nr 49/50, 1965.
11. Litwin R.: Teoria pola elektromagnetycznego. WNT, Warszawa 1969.
12. Murray O.A.: Introductory course in Differential Equations. Longmans, London 1958.
13. Womack C.P.: The use of exponential transmission lines in microwave components. IRE Trans. Microwave Theory Techn., vol. MTT-10, 1962.

Ян Богуцки

### НЕОДНОРОДНЫЕ ПЕРЕДАЮЩИЕ ЛИНИИ С ЭКСПОНЕНТНОЙ КОСИНУС-КВАДРАТ И ПАРАБОЛИЧЕСКОЙ ХАРАКТЕРИСТИКОЙ

#### Резюме

В статье представлено уравнения определяющие комплексные сопротивление трансформирующие через отрезок неоднородной передающей без потери линии с характеристикой экспонентной, косинус-квадрат и параболической.

Эти уравнения получено из решений дифференцированных уравнений второго порядка /Гикати/ в зависимости от сопротивления неоднородной линии и её длины. Эти уравнения очень полезные для разрешения проблемы согласования.

Jan Bogucki

**NONUNIFORM TRANSMISSION LINES WITH EXPONENTIAL,  
COSINE-SQUARED AND PARABOLIC TAPERS**

Summary

The equations of complex impedance transformed a length of dissipationless, nonuniform transmission line with exponential, cosine-squared and parabolic tapers are presented here.

The equations are obtained by solving a second nonlinear, differential (Riccati) equation relating to impedance, the nonuniform line impedance and the line length. The results should be useful in solving impedance matching problems.

Jan Bogucki

**NON HOMOGENES LIGNES DE TRANSMISSION AVEC UNE DISTRIBUTION  
EXPONENTIELLE COSINUS CARRÉ ET PARABOLIQUE**

Résumé

On formule dans cet article les équations de l'impédance complexe transférée par un segment sans pertes d'une ligne de transmission non homogène avec une distribution exponentielle cosinus carré et parabolique.

On a obtenu ces équations par solution d'une équation différentielle de deuxième ordre (Riccati) en fonction de l'impédance de ligne non homogène et de sa longueur. Les équations en question sont utiles comme l'instrument à résoudre les problèmes d'incompatibilité.

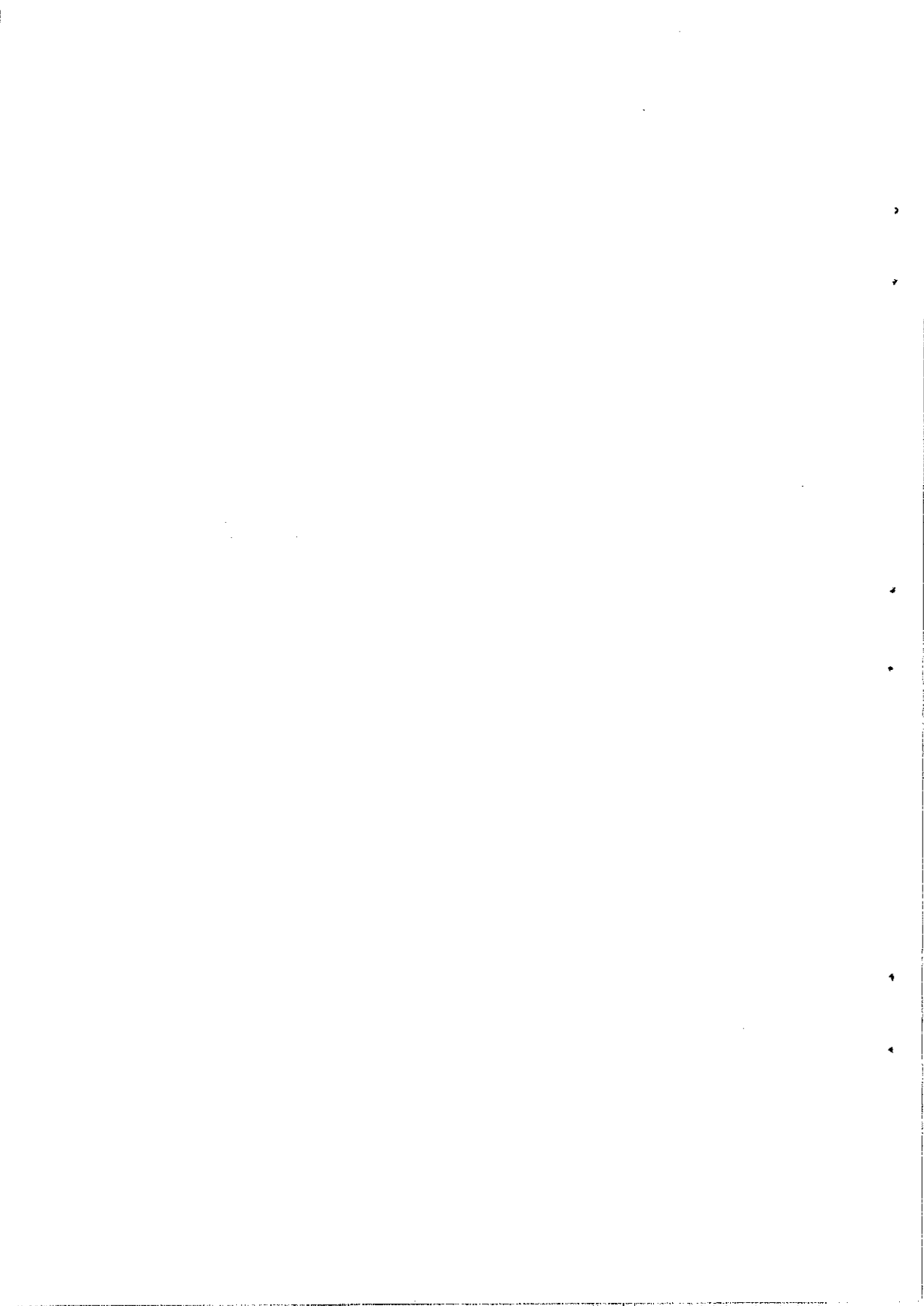
Jan Bogucki

**INHOMOGENE ÜBERTRAGUNGSLEITUNGEN MIT EXPONENTIAL-,  
COS<sup>2</sup>- UND PARABOLISCHER VERTEILUNG**

**Zusammenfassung**

In dem Artikel wurden Gleichungen für den Wert des durch Abschnitt der verlustfreien inhomogenen Übertragungsleitung mit Exponential-,  $\cos^2$ - und parabolischer Verteilung übertragenen Scheinwiderstandes gegeben.

Die Gleichungen wurden erreicht durch Lösung der Differentialgleichung zweiter Ordnung (Riccati) in Abhängigkeit von dem Scheinwiderstand und der Länge der inhomogenen Leitung. Die Gleichungen sind nutzbar bei Lösung des Problems der Fehlanpassung.





Ryszard Klimkiewicz  
Piotr Tyrawa

621.396.67

## BADANIA CHARAKTERYSTYK PROMIENIOWANIA ANTEN POMIAROWYCH ZAINSTALOWANYCH NA ŚMIGŁOWCU

Rękopis dostarczony do Komitetu Redakcyjnego dn. 1988.09.15

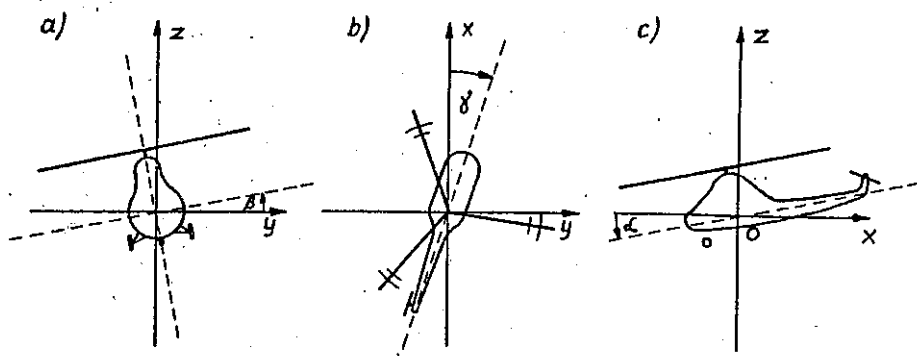
W artykule przedstawiono trzy metody, pozwalające na wykonanie pomiaru charakterystyki promieniowania anten pomiarowych zainstalowanych na śmigłowcu. Do realizacji praktycznej wybrano metodę lotu śmigłowca po okręgu. Wyniki pomiarów wykonanych dla wybranego szeregu częstotliwości, po odpowiednim przetworzeniu numerycznym, są wykorzystywane w praktyce metrologicznej laboratorium śmigłowcowego.

### 1. WPROWADZENIE

Do badań właściwości kierunkowych stacjonarnych anten nadawczych zakresu ultrakrótkofalowego stosuje się śmigłowiec wyposażony w odpowiednią aparaturę pomiarowo-rejestrującą. W locie pomiarowym śmigłowiec wraz ze związaną z nim anteną pomiarową zmienia cały czas swoją orientację względem anteny badanej. Zmienia się więc tym samym kierunek wiązki głównej anteny pomiarowej. W czasie pomiaru rejestruje się zarówno wartość natężenia pola elektromagnetycznego, jak i współrzędne położenia oraz orientacji śmigłowca w przestrzeni. W czasie końcowej obróbki wyników, możliwa jest korekta mierzonych napięć w.cz. pod warunkiem, że znana jest charakterystyka promieniowania umieszczonej na śmigłowcu anteny pomiarowej, która w sposób istotny różni się od charakterystyki zmierzonej dla wolnej przestrzeni.

W trakcie pomiaru, przy użyciu śmigłowca, przestrzennych charakterystyk promieniowania stacjonarnych anten nadawczych, np. telewizyjnych, lot śmigłowca pomiarowego powinien odbywać

się po obwodzie koła leżącego na płaszczyźnie poziomej, tak aby kierunek głównej wiązki promieniowania anteny pomiarowej zainstalowanej sztywno na śmigłowcu pokrywał się z kierunkiem na antenę badaną [4, 8]. W realizacji praktycznej lot taki jest niemożliwy; śmigłowiec zmienia cały czas swoje położenie i orientację w przestrzeni w różnych płaszczyznach. Między innymi ulega przechyleniu wokół własnej osi, np. pod wpływem oddziaływania siły odśrodkowej, doznaje skręcenia od stycznej do okręgu, np. pod wpływem nawet słabego wiatru, czy wreszcie pochyla się na skutek oddziaływania naturalnych sił fizycznych związanych ze sposobem poruszania się śmigłowca. Składowe zmiany położenia śmigłowca w czasie lotu pomiarowego przedstawiono na rys. 1a,b,c [9]. W wyniku tych oddziaływań zmienia się również kierunek anteny pomiarowej, która odchyła się od kierunku śmigłowca - antena badana. Można przyjąć, że przemieszcza się ona wewnątrz stożka eliptycznego o podstawie wydłużonej w poziomie (rys. 2). Z dotychczasowych doświadczeń pomiarowych wynika, że kąt bryłowy stożka nie przekracza wartości  $2\gamma \approx 70^\circ$  w płaszczyźnie poziomej i  $2\beta \approx 10^\circ$  w płaszczyźnie pionowej.

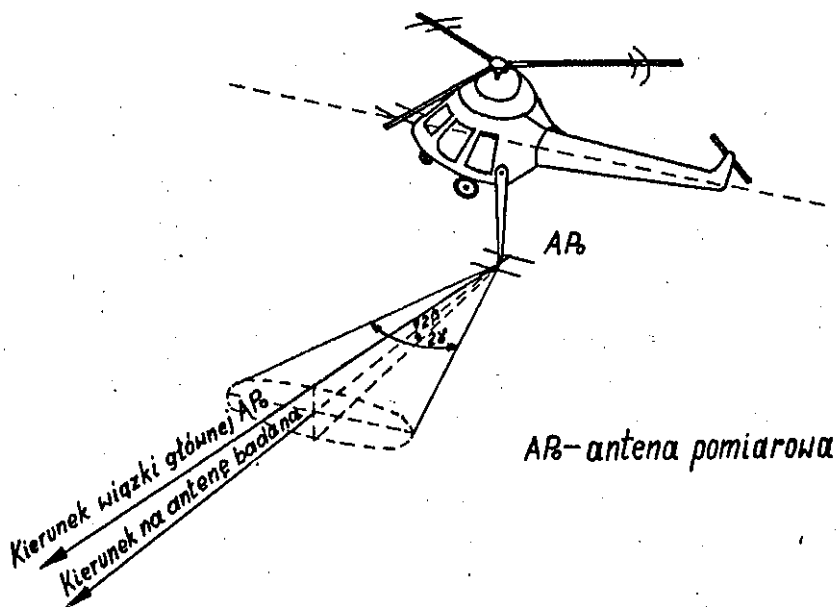


Rys. 1. Orientacja śmigłowca w przestrzeni

a) definicja kąta przechylenia śmigłowca; b) definicja kąta skręcenia śmigłowca; c) definicja kąta pochylenia śmigłowca

Łatwo zauważyć, że wahania śmigłowca można by zaniedbać, a zwłaszcza jego przechylenie i skręcenie (kąty  $\beta$  i  $\gamma$ ), gdyby charakterystyka promieniowania anteny pomiarowej w obszarze

kąta bryłowego stożka była izotropowa. Praktycznie wykonanie anteny o takich właściwościach nie jest możliwe.



Rys. 2. Odchylenia kierunku wiązki głównej promieniowania anteny pomiarowej  $AP_0$  podczas lotu pomiarowego śmigłowca

W śmigłowcowym laboratorium pomiarowym Instytutu Łączności O/Wrocław jako anteny pomiarowe wykorzystywane są aktualnie dwie anteny: antena 2-dipolowa i antena logarytmicznie-periodyczna, a więc anteny o właściwościach kierunkowych. Napięcie  $U$  na wyjściu anteny jest więc funkcją natężenia pola elektrycznego  $E$  w miejscu pomiaru i zysku energetycznego anteny  $G$ , ale również pośrednio - orientacji śmigłowca w przestrzeni  $(\alpha, \beta, \gamma)$ . Można to zapisać:

$$U = f [E, G, \alpha, E_A (\beta, \gamma)] \quad (1)$$

gdzie:

$E_A (\beta, \gamma)$  - wartość charakterystyki anteny pomiarowej na kierunku  $\beta, \gamma$ .

W związku z tym, w czasie pomiaru, rejestruje się zarówno napięcie na wyjściu anteny pomiarowej, jak i wielkości określające położenie oraz orientację śmigłowca i związanej z nim anteny pomiarowej w przestrzeni [4]. Znajomość położenia w przestrzeni, jak i znajomość aktualnej charakterystyki promieniowania anteny pomiarowej, pozwala w trakcie ostatecznej obróbki wyników korygować mierzone napięcie o współczynnik korekcyjny  $E_A(\beta, \gamma)$ .

Stwierdzono, że z powodu wpływu dużej powierzchni przewodzącej śmigłowca na rozkład pola elektromagnetycznego, charakterystyki promieniowania anteny pomiarowej zainstalowanej na śmigłowcu w istotny sposób różnią się od tych samych charakterystyk zmierzonych w wolnej przestrzeni, np. na poligonie pomiarowym. Charakterystyki promieniowania anten pomiarowych powinny zostać pomierzone po ich zamontowaniu w pozycji roboczej na śmigłowcu. Z uwagi na wiele czynników specyficznych dla tego układu, wymagane jest zastosowanie specjalnej techniki pomiarowej.

## 2. METODA POMIARU

### 2.1. Wybór metody pomiarowej

W technice antenowej, przy wykonywaniu pomiarów przestrzennej charakterystyki promieniowania dowolnych anten w warunkach poligonowych, przyjęto zasadę, że antena badana jest obracana w płaszczyźnie poziomej, w pełnym zakresie kąta azymutu ( $0^\circ - 360^\circ$ ), wokół stacjonarnej osi pionowej, w jednorodnym i stałym polu elektromagnetycznym wytworzonym przez antenę pomocniczą ustawioną w strefie pola dalekiego anteny badanej [1, 3, 6, 7]. Charakterystyka promieniowania anteny badanej  $E_A$  jest wyłącznie funkcją kąta azymutu :

$$E_A = f(\phi) \quad (2)$$

W przypadku gdy anteną badaną jest układ złożony z anteny pomiarowej i śmigłowca (układ A+S), zmierzenie jego charakte-

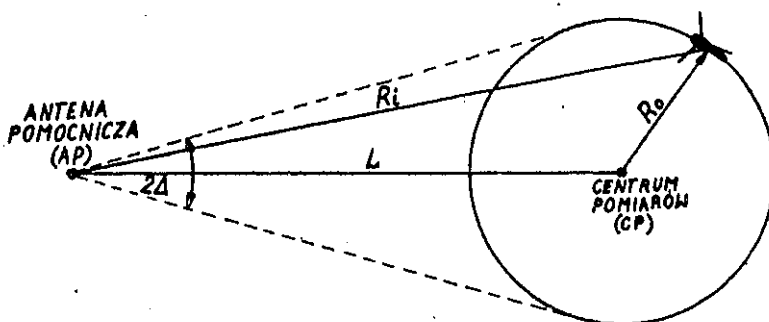
rystyki promieniowania w podany wyżej sposób nie jest możliwe. Ze względu na brak odpowiednio wytrzymałej obrotnicy, nie ma możliwości obracania śmigłowca wokół osi pionowej w warunkach poligonowych na ziemi. Nie jest również możliwe, aby śmigłowiec typu Mi-2, z pełnym wyposażeniem pomiarowym, wykonał w sposób kontrolowany wymagany obrót za pomocą silników, w tzw. zawisie - jest bowiem na to zbyt ciężki. Dlatego też było konieczne posłużenie się w tym przypadku inną metodą pomiaru charakterystyk promieniowania układu A+S, stosując normalne, możliwe do wykonania loty śmigłowca. Przy tym założeniu, pomiary charakterystyk promieniowania anteny pomiarowej na śmigłowcu można przeprowadzić trzema metodami różniącymi się sposobem poruszania się śmigłowca. W każdej z metod źródłem pola elektromagnetycznego jest antena pomocnicza (w skrócie AP) umieszczona w odległości  $L$  od tzw. centrum pomiarów (CP), nad którym wykonuje się loty pomiarowe. Antena pomocnicza powinna być umieszczona na przewyższeniu terenowym, tak aby śmigłowiec w locie znajdował się w przybliżeniu na wysokości jej środka elektrycznego.

Przedstawimy obecnie ogólne założenia poszczególnych metod pomiarowych oraz przeprowadzimy dyskusję ich zalet i wad.

### 2.1.1. Metoda lotu śmigłowca po okręgu (LPO)

Metoda ta polega na pomiarze napięcia na wyjściu anteny pomiarowej w czasie lotu śmigłowca w płaszczyźnie poziomej po okręgu o promieniu  $R_0$ , którego środek leży dokładnie nad centrum pomiarów CP [5]. Sposób przeprowadzenia pomiarów tą metodą przedstawiono na rys. 3. Promień toru lotu śmigłowca powinien być tak dobrany, aby przechylenie śmigłowca w wyniku działania siły odśrodkowej nie było zbyt duże. Opierając się na dotychczasowej praktyce pomiarowej można przyjąć dopuszczalny, minimalny promień okręgu równy 1 km. Wówczas, przy stosowanych prędkościach lotu, kąt przechylenia śmigłowca nie przekracza  $5^\circ$  [10]. Śmigłowiec, lecąc po tak dużym okręgu, porusza się w niejednorodnym polu elektromagnetycznym anteny pomocniczej ze względu na:

- zmianę odległości  $R_i$  śmigłowca od AP;
- wpływ właściwości kierunkowych anteny pomocniczej;
- interferencje fali bezpośredniej i odbitej od ziemi [2].



Rys. 3. Pomiar charakterystyki układu A+S metodą LPO

Względny zakres zmian natężenia pola przy odległościach granicznych (bez uwzględniania wpływu interferencji) można wyznaczyć z zależności:

$$\Delta E = 20 \cdot \log \frac{L + R_0}{L - R_0} \quad (3)$$

Dopuszczając odchyłki  $\Delta E$  nie większe niż 0,5 dB oraz przyjmując  $R_0 = 1000$  m z (3) można wyznaczyć, że odległość  $L$  powinna być większa niż 34 km - kąt  $\Delta$  nie przekracza wówczas wartości  $3,3^\circ$ . Przy takiej odległości, źródłem pola elektromagnetycznego może być jedynie stacja nadawcza dużej mocy (TV lub UKF). W przypadku spełnienia warunku na minimalną odległość  $L$  wpływ zmiany pierwszych dwóch czynników na mierzoną charakterystykę można pominąć, w każdym innym przypadku czynniki te muszą być uwzględnione.

Reasumując, można wymienić następujące zalety metody LPO:

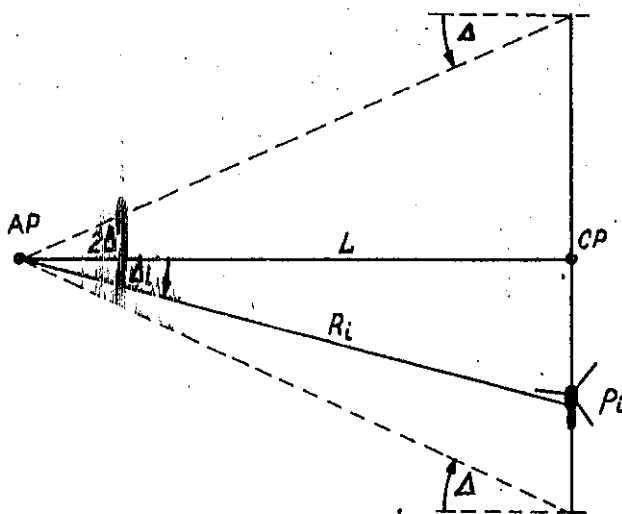
- pomiar charakterystyki w pełnym zakresie kąta azymutu;
- szybkość pomiaru.

Do wad metody można zaliczyć fakt, że:

- pomiar odbywa się w niejednorodnym polu elektromagnetycznym;
- na skutek przechyłu śmigłowca w locie po okręgu, pomiar charakterystyki nie odbywa się dokładnie w płaszczyźnie  $\theta = 90^\circ$ ;
- odległość  $L$  pomiędzy CP i AP oraz geometria toru lotu śmigłowca muszą być znane z zadowalającą dokładnością.

### 2.1.2. Metoda lotu śmigłowca po prostej (LPP)

Metoda ta polega na pomiarze napięcia na wyjściu anteny pomiarowej w czasie lotu śmigłowca po prostej (LPP) wytyczonej nad centrum pomiarowym CP i prostopadłej do kierunku CP-AP (rys. 4). Pozwala ona, w przeciwieństwie do metody LPO, na pomiar charakterystyki układu A+S tylko w ograniczonym zakresie kąta azymutu  $\pm \Delta$ , tzn. w zakresie kąta obejmującego, np. wiązkę główną. Na ogół, w przypadku rutynowych pomiarów śmigłowcowych, znajomość charakterystyki anteny pomiarowej w obszarze wiązki głównej jest wystarczająca. W metodzie tej



Rys. 4. Pomiar charakterystyki układu A+S metodą LPP

śmigłowiec porusza się również w niejednorodnym polu elektromagnetycznym anteny pomocniczej. Niejednorodność jest wywołana między innymi:

- zmianą odległości  $R_i$  śmigłowca od AP;
- wpływem właściwości kierunkowych anteny pomocniczej;
- interferencją fali bezpośredniej i odbitej od ziemi.

W związku z tym, napięcie  $U_i$  opisujące charakterystykę promieniowania anteny pomiarowej musi być przeliczone wg następującej zależności:

$$U_i = U_{oi} \cdot \frac{R_i}{L} \cdot E_{AP}(\Delta_i) \cdot K(\alpha, \beta, \gamma) \quad (4)$$

gdzie:

- $U_{oi}$  - napięcie na wyjściu anteny pomiarowej zarejestrowane w punkcie  $p_i$ ,
- $R_i$  - odległość śmigłowca od AP w punkcie  $p_i$ ,
- $E_{AP}(\Delta_i)$  - wartość charakterystyki anteny pomocniczej w kierunku  $\Delta_i$ ,
- $K(\alpha, \beta, \gamma)$  - współczynnik korekcyjny wynikający ze zmiany orientacji śmigłowca w przestrzeni.

Przy ustabilizowanym locie po prostej, przechyły boczne śmigłowca względem osi poziomej można zaniedbać ( $\beta = 0$ ), a przy stałej prędkości kąt pochylenia  $\alpha$  ma w przybliżeniu wartość stałą. Praktycznie, współczynnik korekcyjny jest wyłącznie zależny od kąta skręcenia  $\gamma$ .

Zaletą metody LPP jest:

- możliwość wykonania pomiarów charakterystyki układu A+S w zasadzie dokładnie w płaszczyźnie  $\theta = 90^\circ$ ;
- krótki czas wykonywania pomiarów;

natomiast wadą:

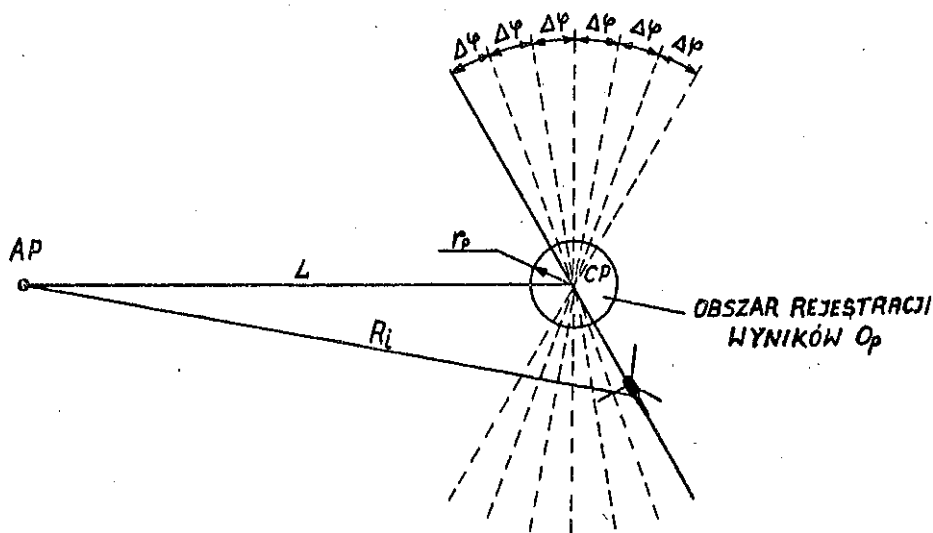
- pomiar charakterystyki w ograniczonym zakresie kąta azymutu;



- pomiar w niejednorodnym polu elektromagnetycznym;
- konieczność znajomości geometrii toru lotu śmigłowca i charakterystyki promieniowania anteny pomocniczej.

### 2.1.3. Metoda lotu śmigłowca nad punktem pomiarowym (LNPP)

Metodą najbardziej zbliżoną do sposobu wykonywania pomiarów charakterystyk promieniowania anten na poligonie jest metoda lotu śmigłowca nad punktem pomiarowym (LNPP). Sposób wykonywania pomiarów pokazano na rys. 5. W metodzie tej charakterystyka promieniowania układu A+S mierzona jest ze skokiem kąta azymutu równym  $\Delta\phi$ . Śmigłowiec, lecąc po liniach prostych o kierunkach różniących się o  $\Delta\phi$ , w założeniu przelatuje stale nad tym samym punktem przecięcia się prostych, w tym przypadku nad centrum pomiarowym CP. Istotne dla wyników pomiarów są wartości napięcia na wyjściu anteny pomiarowej, zarejestrowane na obszarze objętym okręgiem  $O_p$  na rys. 5.



Rys. 5. Pomiar charakterystyki układu A+S metodą LNPP

Jeśli przyjąć, że promień obszaru rejestracji jest dużo mniejszy od odległości L, a taki warunek można łatwo spełnić, natężenie pola od anteny pomocniczej AP w obszarze rejestracji

jest prawie jednorodny. W takim przypadku, dla kierunku  $\phi_i$  średnia wartość napięcia na wyjściu anteny z obszaru rejestracji wyników będzie wynosić:

$$U_{sr}(\phi_i) = \frac{\sum_{n=1}^{N_i} U_n(\phi_i)}{N_i} \cdot K(\alpha_n, \beta_n, \gamma_n) \quad (5)$$

gdzie:

- $U_n(\phi_i)$  - chwilowa wartość napięcia w punkcie  $n$ , w obszarze rejestracji wyników na kierunku  $\phi_i$ ,
- $K(\alpha_n, \beta_n, \gamma_n)$  - współczynnik korekcyjny wynikający z aktualnej orientacji śmigłowca w punkcie  $n$ ,
- $N_i$  - liczba zarejestrowanych wartości napięcia dla kierunku  $\phi_i$ .

Charakterystyka układu A+S jest w tym przypadku opisana wyrażeniem:

$$E_{AS} = \frac{U_{sr}(\phi_i)}{U_{sr \max}} \quad (6)$$

gdzie:

- $U_{sr \max}$  - wartość maksymalna spośród napięć uśrednionych.

Zalety metody LNPP są następujące:

- pomiar odbywa się w niemal jednorodnym polu elektromagnetycznym;
- nie jest potrzebna znajomość odległości  $L$ ;
- wyeliminowany jest wpływ charakterystyki anteny pomocniczej;
- charakterystyka jest mierzona w płaszczyźnie  $\phi = 90^\circ$ .

Podstawowymi wadami metody są:

- czasochłonność i związane z tym koszty;
- dyskretny pomiar charakterystyki z krokiem kątowym  $\Delta\phi$ .

Z krótkiej analizy przedstawionych wyżej metod pomiarowych charakterystyk układu A+S można wnioskować, że najmniejszą możliwością popełnienia błędów stwarza metoda LNPP. Wynika to ze stosunkowo najmniejszej liczby współczynników, które należy uwzględnić oraz warunków, jakie należy spełnić. Niemniej jednak, ze względu na dużą pracochłonność oraz wysoki koszt związany z koniecznością wielokrotnych lotów śmigłowca, wybrano sposób pomiaru przedstawiony w metodzie LPD zwłaszcza, że do tej metody można było wykorzystać standardowe wyposażenie i oprogramowanie metrologiczne cyfrowego systemu pomiarowego na śmigłowcu.

## 2.2. Ustalenie warunków pomiaru

Jak już wiadomo z omówienia metody LPD (pkt. 2.1.1), to czy pomiar będzie odbywał się w jednorodnym polu elektromagnetycznym, uzależnione jest bezpośrednio od odległości  $L$  anteny pomocniczej AP od centrum pomiaru CP (rys. 3). Z przeprowadzonej dyskusji wynikało, że odległość  $L$  powinna być co najmniej równa 34 km. Przy tak dużej odległości źródłem zasilania anteny pomocniczej może być wyłącznie nadajnik nadawczej stacji telewizyjnej lub radiofonicznej UKF/FM. Pomiar z wykorzystaniem nadajników radiowo-telewizyjnych są jednak możliwe tylko na częstotliwościach ich pracy, a więc powinny być wykonywane w różnych miejscach kraju, co jest bardzo uciążliwe i kosztowne. Nie pozwoliłoby również na pomiar charakterystyk anteny pomiarowej w całym wymaganym zakresie częstotliwości. Pozostaje więc jedynie skorzystanie z generatora laboratoryjnego jako źródła mocy dla anteny pomocniczej. Jako źródło zasilania anteny pomocniczej wykorzystano generator laboratoryjny o mocy wyjściowej 2 W. Zastosowanie generatora o tak małej mocy wyjściowej powoduje, że odległość  $L$  pomiędzy AP i CP nie może być zbyt duża. Przyjmując jako wystarczający i bezpieczny poziom napięcia na wyjściu anteny pomiarowej równy 40 dB $\mu$ V, ustalono na podstawie wstępnych pomiarów [10], że odległość  $L$  powinna być bliska 3 km. Promień toru lotu  $R_0$  określono również doświadczalnie zakładając, że kąt przechyłu śmigłowca nie może prze-

kraczać  $5^\circ$  - warunek ten udało się spełnić przy promieniu równym 1200 m i prędkości liniowej śmigłowca nie przekraczającej 100 km/godz. Jest oczywiste, że dla przyjętych odległości  $L$  i promienia  $R_0$ , śmigłowiec będzie się poruszał w niejednorodnym polu elektromagnetycznym anteny pomocniczej z powodów wymienionych w pkt. 2.1.2. W związku z tym chwilowa wartość napięcia  $U_i$  na wyjściu anteny pomiarowej jest określona funkcją:

$$U_i = f [R_i, E_{AP}(\Delta_i), F(\Delta R_i), \Phi_L] \quad (7)$$

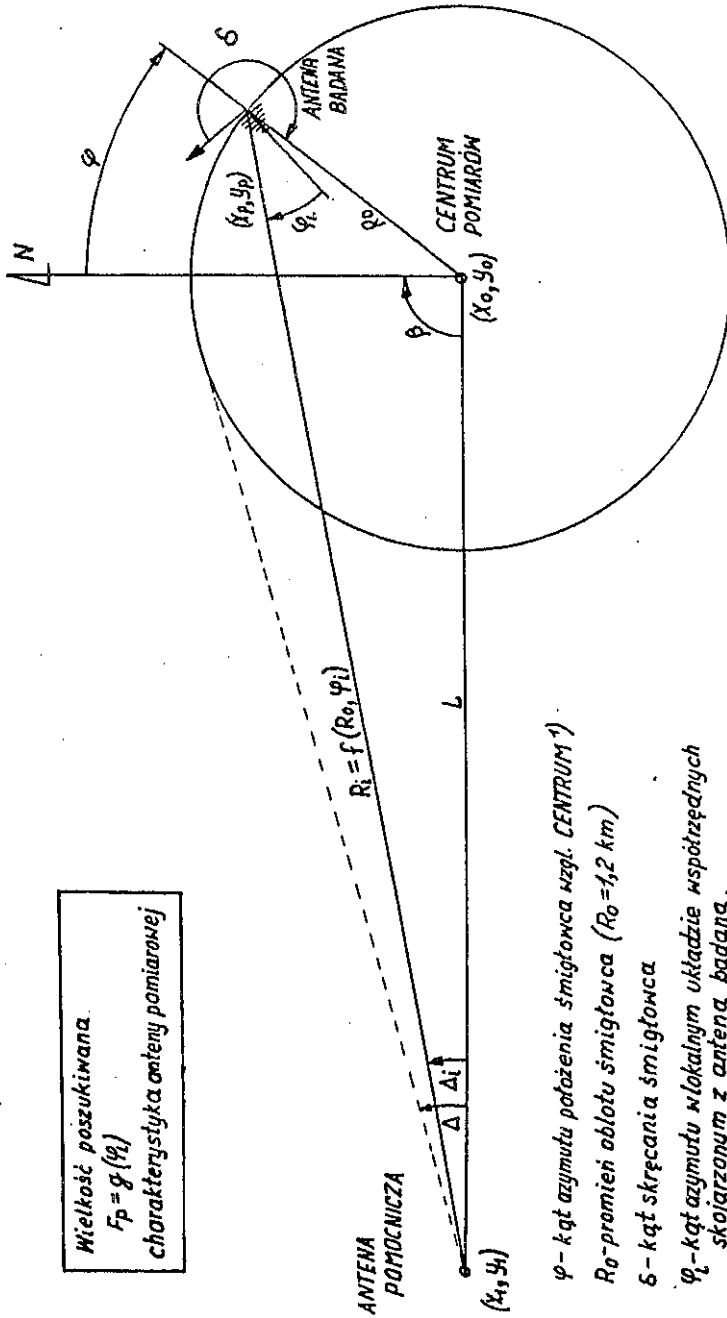
w której:

- $R_i$  - chwilowa odległość śmigłowca od AP,
- $E_{AP}(\Delta_i)$  - wartość charakterystyki AP na kierunku  $\Delta_i$ ,
- $F(\Delta R_i)$  - współczynnik związany z interferencją fali padającej i odbitej od ziemi,
- $\Phi_L$  - kąt azymutu w układzie skojarzonym z anteną pomiarową na śmigłowcu (rys. 6).

Wpływ odległości na poziom napięcia rejestrowanego na wyjściu anteny pomiarowej jest eliminowany w procesie końcowej obróbki wyników. Chwilowe wartości napięć  $U_i$  z poszczególnych punktów okręgu są transformowane do jednego wspólnego punktu, w tym przypadku do środka okręgu CP, według następującej zależności:

$$U_{iCP} = \frac{R_i}{L} U_i \quad (8)$$

Wpływ charakterystyki promieniowania anteny pomocniczej na napięcie  $U_i$  został wyeliminowany poprzez "śledzenie" śmigłowca w czasie lotu przez wiązkę główną jej charakterystyki promieniowania. Dzięki takiemu rozwiązaniu, można było zastosować jako anteny pomocnicze, anteny kierunkowe o stosunkowo dużym zysku. Wykorzystano tu zestaw anten typu Yagi o zysku  $6 \div 8$  dB, pokrywających zakres częstotliwości  $50 \div 790$  MHz.



Wielkość poszukiwana.  
 $F_p = g(\varphi_i)$   
 charakterystyka anteny pomiarowej

$\varphi$  - kąt azymutu położenia śmigłowca wzgl. CENTRUM<sup>1)</sup>

$R_0$  - promień oblotu śmigłowca ( $R_0 = 1,2 \text{ km}$ )

$\delta$  - kąt skręcania śmigłowca

$\varphi_i$  - kąt azymutu lokalnym układzie współrzędnych skojarzonym z anteną badaną.

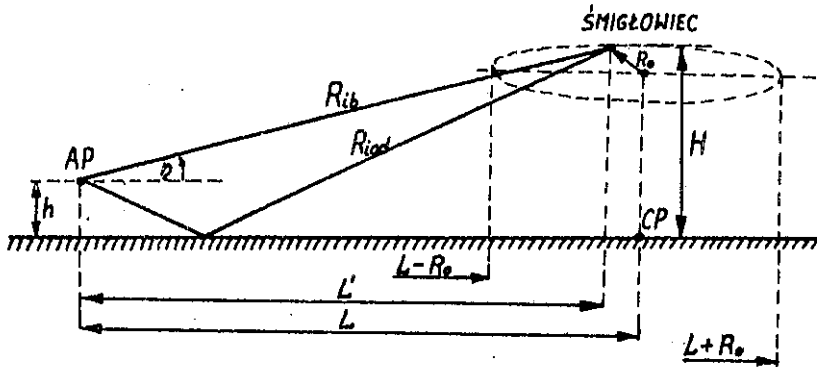
$L$  - wg rysunku

1)  $\varphi = \delta + \Omega - 180$

$\Omega$  - kurs magnetyczny

Rys. 6. Geometria lotu pomiarowego

Czynnik związany z wpływem interferencji fali padającej i odbitej na napięcie  $U_i$  jest dość trudny do uwzględnienia, niemniej jednak jego wpływ można częściowo ograniczyć [2,11]. Natężenie pola w miejscu chwilowego położenia anteny pomiarowej wraz ze śmigłowcem, dla fali bezpośredniej można zapisać następująco (rys. 7):



Rys. 7. Interferencja fal bezpośredniej i odbitej od ziemi

$$E_b = A_1 e^{j\beta R_{ib}}$$

a dla fali odbitej od ziemi:

$$E_{od} = A_2 e^{j\beta R_{iod}}$$

gdzie:

$A_1, A_2$  - amplitudy składowej elektrycznej (dla małych kątów współczynnik odbicia od ziemi jest bliski 1 i można przyjąć  $A_1 = A_2 = A$ ),

$R_{ib}$  - chwilowa długość drogi promieniowania bezpośredniego,

$R_{iod}$  - chwilowa długość drogi promieniowania odbitego,

$\beta$  - stała fazowa ( $2\pi/\lambda$ ).

$R_{ib}$  i  $R_{iod}$  są równe:

$$R_{ib} = \sqrt{(H-h)^2 + (L')^2} ; \quad R_{iod} = \sqrt{(H+h)^2 + (L')^2}$$

(oznaczenia wg rys. 7)

Całkowite natężenie pola w miejscu pomiaru jest równe sumie geometrycznej obu wektorów składowych. Po prostych przekształceniach, moduł natężenia wypadkowego jest równy:

$$E = 2A \cdot \cos\beta \frac{\sqrt{(H+h)^2 + (L')^2} - \sqrt{(H-h)^2 + (L')^2}}{2} \quad (9)$$

Jeśli teoretycznie założyć  $h=0$  (antena pomocnicza znajduje się tuż przy powierzchni ziemi), to wówczas długości dróg obu promieni są jednakowe, a natężenie pola nie podlega fluktuacjom interferencyjnym. Praktycznie jednak antena pomocnicza nie może leżeć wprost na ziemi, zresztą nie ma takiej konieczności. Zmianę natężenia pola wynikającą z interferencji fali bezpośredniej i odbitej od ziemi dla granicznych położzeń śmigłowca można policzyć z zależności:

$$E_{[dB]} = 20 \cdot \log \frac{\cos\beta \left[ \sqrt{(H+h)^2 + (L-R_0)^2} - \sqrt{(H-h)^2 + (L-R_0)^2} \right]}{\cos\beta \left[ \sqrt{(H+h)^2 + (L+R_0)^2} - \sqrt{(H-h)^2 + (L+R_0)^2} \right]} \quad (10)$$

Jeżeli przyjąć, że zmiana natężenia pola  $\Delta E$  nie może przekroczyć 0,5 dB, to przy założeniu, że  $L = 3000$  m,  $H = 150$  m,  $R_0 = 1200$  m oraz dla fali o długości 0,5 m (warunek mało korzystny), wzór (10) będzie spełniony dla wysokości  $h$  anteny pomocniczej nad ziemią równej 0,36 m. Dla mniejszych częstotliwości pomiarowych wysokość ta może być oczywiście większa.

Płaszczyzna lotu śmigłowca na ogół przewyższa wysokość umieszczenia anteny pomocniczej. Powoduje to, że charakterystyka układu A+S nie jest mierzona dokładnie dla  $\theta = 90^\circ$

(rys. 7). Średnią odchyłkę z tego tytułu można wyznaczyć z zależności:

$$\eta = \arctg \frac{H - h}{L} \quad (11)$$

Dla podanych wyżej warunków wartość  $\eta = 2,8^\circ$ , jest więc do pominięcia. Jeżeli antena pomocnicza zostanie ustawiona na wzniesieniu terenowym, kąt ten będzie jeszcze mniejszy.

### 3. POMIARY I OBRÓBKA WYNIKÓW

#### 3.1. Pomiary

Stanowisko pomiarowe zostało zlokalizowane w sąsiedztwie góry Ślęza. Antenę pomocniczą umieszczono na stoku góry, na wysokości około 120 m nad otaczającym terenem. Teren, nad którym wykonywane były loty, wybrano w miarę płaski, nie zabudowany i nie zalesiony. Środek okręgu (centrum pomiarów) był oddalony ( $L$ ) od anteny pomocniczej o około 2,5 km, a promień okręgu ( $R_0$ ) wynosił 1200 m. Śmigłowiec wykonywał loty na wysokości anteny pomocniczej, tj. na wysokości około 120 m nad poziomem terenu. W centrum pomiarów (CP) zlokalizowano naziemną część aparatury służącej do pomiaru odległości  $R_0$  i kąta skreślenia śmigłowca (rys. 6) [10]. Ze względu na przeważającą w kraju polaryzację poziomą nadawczych anten telewizyjnych i radiofonicznych UKF, pomiary charakterystyk anteny pomiarowej ograniczono do tej polaryzacji. Wykonywano pomiary poziomych charakterystyk w płaszczyźnie  $\theta \approx 90^\circ$ . Aby zwiększyć dokładność pomiarów, dla każdej z ustalonych częstotliwości, wykonywano po dwa pełne okręgi (z nadmiarem).

W czasie lotów pomiarowych rejestrowano następujące wielkości:

- napięcie w.c.z. mierzone mikrowoltomierzem selektywnym;
- odległość  $R_0$  śmigłowca od CP;
- kąt skreślenia śmigłowca  $\sigma$ ;



- kurs magnetyczny  $\Omega$  ;
- kąt przechyłu śmigłowca  $\beta$  i kąt nachylenia  $\alpha$  .

Utrzymywanie stałej wysokości lotu było kontrolowane przez barometryczny korektor wysokości. Wymienione wyżej wielkości rejestrowano na dysku elastycznym synchronicznie, w stałych odstępach czasu  $T_r$ , nazywanych czasem repetycji. Kontrolę nad procesem pomiaru i rejestracji pełnił komputer pokładowy. Okres repetycji tak dobrano, aby w czasie jednego oblotu zostało zarejestrowanych około 200 synchronicznych grup wyników.

### 3.2. Metoda obróbki wyników

Wielkością poszukiwaną jest charakterystyka promieniowania  $F_p(\phi_L)$  układu A+S, czyli anteny pomiarowej wraz ze śmigłowcem. Kąt  $\phi_L$  jest kątem azymutu w lokalnym układzie współrzędnych biegunowych skojarzonych z anteną badaną w taki sposób, że kierunek  $\phi_L = 0$  jest zgodny z jej osią wzdłużną i skierowany na zewnątrz śmigłowca. Kąt  $\phi_L$  nie należy do wielkości mierzonych i musi być wyznaczony analitycznie z pozostałych wielkości. Analogicznie, wskutek porównywalnych ze sobą odległości  $L$  i promienia okręgu pomiarowego  $R_0$ , napięcie w.cz. zarejestrowane na wyjściu anteny pomiarowej (badanej) nie jest wprost proporcjonalne do jej charakterystyki promieniowania. Musi być uprzednio przetransformowane do stałej, umownej odległości, np. odległości  $L$ . Na wstępie obróbki numerycznej, cały materiał pomiarowy poddawany jest weryfikacji formalnej. Ewentualne błędy grube są eliminowane z dalszej obróbki.

Do wyznaczenia z zarejestrowanych wyników szukanej charakterystyki  $F_p(\phi_L)$  zastosowano metodę histogramu. W dużym skrócie, algorytm obróbki wyników przedstawia się następująco:

- a) dla każdej synchronicznej grupy wyników, z kursu magnetycznego  $\Omega_1$  i kąta skreńcenia  $\sigma_1$  wyznacza się kąt azymutu (rys. 6):

$$\phi_i = \sigma_i + \Omega_i - 180 \quad (12)$$

- b) z trójkąta o wierzchołkach  $(x_0, y_0)$ ,  $(x_1, y_1)$  i  $(x_p, y_p)$  wyznacza się chwilową odległość  $R_i$ ;
- c) zmierzoną wartość napięcia  $U_i$  transformuje się do stałej odległości  $L$ ; jeżeli w aktualnie obrabianej grupie synchronicznej kąt przechyłu  $\beta_i$  przekracza granice  $\pm 5^\circ$  od położenia poziomego, wynik pomiaru napięcia wyłącza się z dalszej obróbki;
- d) pełny zakres kąta azymutu  $\phi_L$  w układzie współrzędnych związanych z badaną anteną dzielimy na 72 przedziały (klasy) o szerokości  $\pm 2,5^\circ$ , rozmieszczone na obwodzie wg reguły:

$$\phi_L = n \times 5^\circ \quad (0 \leq n \leq 71);$$

dla każdej zmierzonej i zarejestrowanej wartości napięcia  $U_i$  wyznacza się na podstawie zależności geometrycznych wynikających z rys. 6, odpowiadający mu kąt azymutu  $\phi_{Li}$  i bada jego przynależność do jednej ze zdefiniowanych wyżej klas - wszystkie napięcia przypadające do wspólnej klasy są sukcesywnie sumowane;

- e) po przetworzeniu wszystkich synchronicznych grup wyników, wyznacza się wartości średnie w klasach;
- f) zbiór wartości poddaje się tzw. filtracji numerycznej, przez aproksymację zależności napięcia  $U(\phi_L)$  szeregiem trygonometrycznym 12 stopnia.

Wyniki końcowe wyprowadza się na drukarkę w postaci tablicy wartości względnych i wykresu we współrzędnych biegunowych.

### 3.3. Przykładowe wyniki pomiarów

W charakterze ilustracji, na rys. 8 został zamieszczony wykres charakterystyki promieniowania jednej z anten zmierzonej dla częstotliwości 73,2 MHz [10]. Kierunek  $\phi_L = 0$  przy-



#### 4. ZAKOŃCZENIE

W zakładzie Anten IT O/Wrocław, w ramach prac nad rozwojem śmigłowcowego laboratorium do pomiaru właściwości kierunkowych anten, opracowano metodykę oraz przeprowadzono pomiary poziomych charakterystyk promieniowania anten pomiarowych. Pomiary wykonano dla anten zainstalowanych na śmigłowcu-laboratorium w warunkach normalnej eksploatacji. Jak dotąd, pomiary ograniczono do polaryzacji poziomej dla dziesięciu dyskretnych częstotliwości leżących w zakresie fal metrowych i decymetrowych. Uzyskane rezultaty pomiarów wskazują na istotny wpływ śmigłowca na właściwości kierunkowe anten pomiarowych, mimo stosowania dodatkowego, 5-metrowego masztu pomiarowego odsuwającego anteny pod śmigłowiec.

W czasie obróbki wyników z rutynowych pomiarów właściwości kierunkowych nadawczych anten telewizyjnych i radiofonicznych UKF/FM, wprowadzając poprawki uwzględniające chwilową pozycję i orientację śmigłowca - a tym samym i anteny pomiarowej - w stosunku do anteny badanej, należy brać pod uwagę charakterystyki anten pomiarowych zmierzone w pozycji roboczej na śmigłowcu, w miejsce charakterystyk zmierzonych na poligonie.

Wykonane pomiary traktowane jako rozpoznawcze wykazały, że istnieje potrzeba kontynuowania tych badań, między innymi dla dodatkowych częstotliwości oraz dla anten przewidzianych do pomiarów dla pionowej polaryzacji fali elektromagnetycznej. Odrębnym zagadnieniem badawczym, wymagającym opracowania nowej metody, jest pomiar pionowych charakterystyk promieniowania anten pomiarowych zainstalowanych na śmigłowcu.

#### WYKAZ LITERATURY

1. Bem D.J., Więckowski T.W.: Metody badań parametrów elektrycznych układów i urządzeń antenowych. Raport ITA, Politechnika Wrocławska, Wrocław 1980.

2. Fitzgerald R.G.: The gain of a horizontal half-wave dipole over ground. Transaction on AP, vol AP-15, July 1967.
3. Fradin A.Z., Rizkow E.W.: Izmerenija parametrov antenno-fidernych ustrojstw. Izd. SWJAZ, Moskwa 1982.
4. Grochocki W., Kałuski M., Klimkiewicz R.: Cyfrowy system pomiarowy CSP do pomiaru charakterystyk promieniowania anten z użyciem śmigłowca. Publikacja wewnętrzna nr Z-15/ /3/LALKOP/08/6/85, IŁ O/Wrocław 1985.
5. IEC Publication 489-8: Methods of measurement for antennas in the mobile servis.
6. Kolár J., Csernoch J.: Measurement of Antenna Gain and Radiation Pattern. Budavox Telecommunication Review, No 4, 1975.
7. Kummer W.H.: Antenna Measurement. Proceedings of the IEEE, vol. 66, No 4, April 1978.
8. Massucci M.: Relevé de diagrammes de rayonnement d'antennes d'emission à l'aide d'un hélicoptère. Revue de radio-diffusion-television, No 43, 1976.
9. Smereka A.: Doskonalenie metod pomiarowych przestrzennych charakterystyk anten nadawczych przy pomocy śmigłowca. Publikacja wewnętrzna nr LALKOP 9/83, IŁ O/Wrocław 1983.
10. Tyrawa P.: Analiza wpływu śmigłowca na właściwości kierunkowe anten pomiarowych. Publikacja wewnętrzna nr Z15/ /5/15-14/16/87, IŁ O/Wrocław 1987.
11. Wołpert A.R.: Ob izmerenji diagram antenn w usłowiach wlijanja otrazennych ot ziemnoj powlerchnosti wołn (metod "priziemnoj" wspomagatelnoj anteny). Radiotekhnika, t. 33, nr 6, 1978.

Рышард Климкевич  
Петр Тырава

ИЗМЕРЕНИЕ ХАРАКТЕРИСТИК НАПРАВЛЕННОСТИ  
ИЗМЕРИТЕЛЬНЫХ АНТЕНН УСТАНОВЛЕННЫХ НА  
ВЕРТОЛЕТЕ

Резюме

Рассматриваются три метода измерения характеристик направленности измерительных антенн установленных на борту вертолета.

Для практической реализации выбрано траекторию полета по кругу. Результаты измерений выполненные для выбранного ряда частот, после цифрового преобразования используются в метрологической практике измерительной лаборатории на вертолете.

Ryszard Klimkiewicz  
Piotr Tyrawa

TESTING OF RADIATION PATTERNS OF MEASURING ANTENNAS  
INSTALLED ON A HELICOPTER

Summary

In the paper three methods were presented enabling to carry out measurements of radiations patterns of measuring antennas installed on a helicopter. For the practical realization a method of a helicopter flying in a circle was chosen. The results of the measurements performed for the selected range of frequencies, after an appropriate numerical transformation, are utilized in metrologic practice of helicopter laboratory.

Ryszard Klimkiewicz  
Piotr Tyrawa

## ÉTUDES DES DIAGRAMMES DE RAYONNEMENT DES ANTENNES EMBARQUÉES SUR L'HELICOPTERE

### Résumé

Article présente trois méthodes permettant l'exécution de mesurage des diagrammes de rayonnement des antennes d'essais embarquées en hélicoptère. Pour la réalisation pratique on a choisi la méthode de vol de l'hélicoptère en cercle.

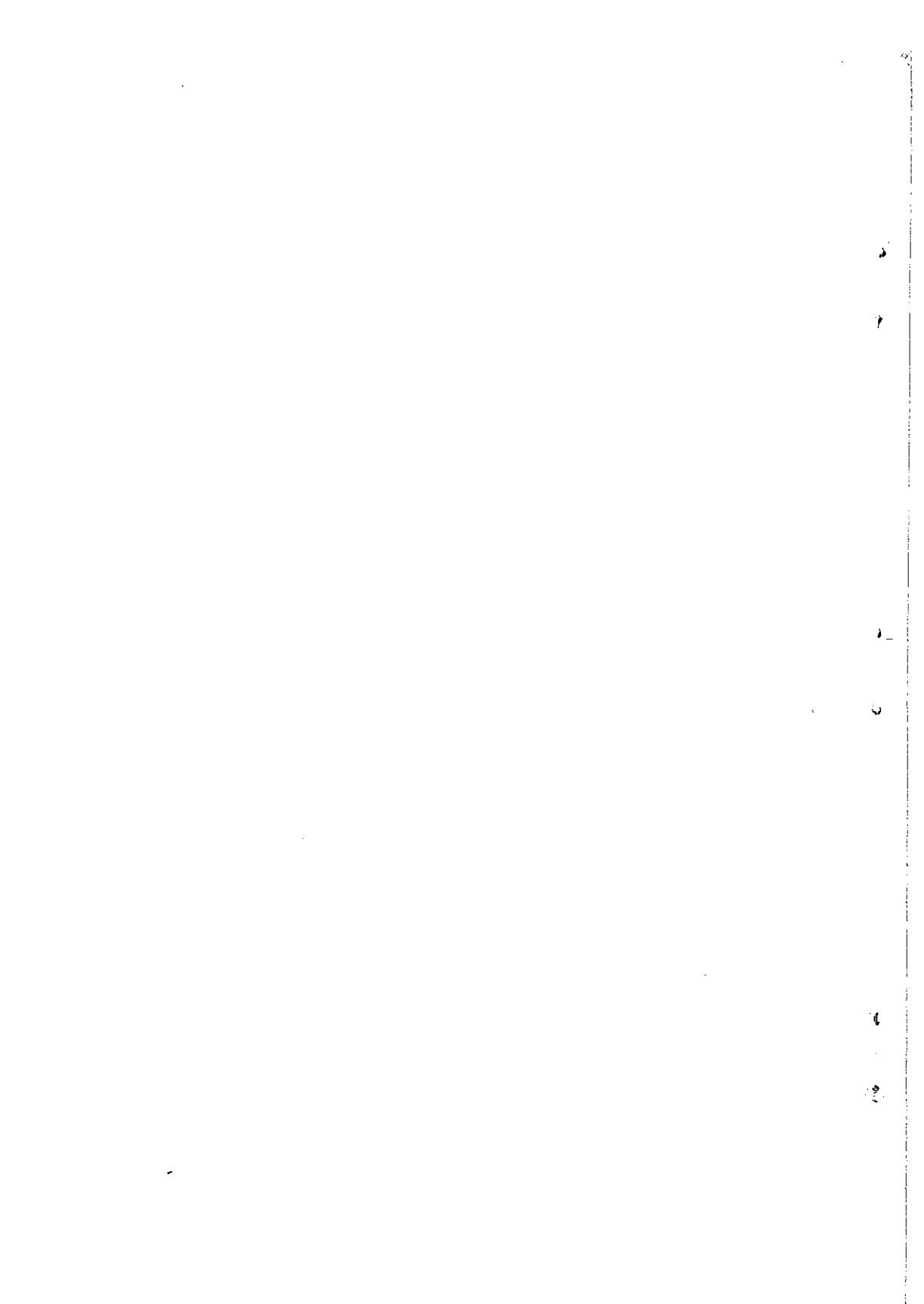
Les résultats des mesures exécutées pour une série de fréquences après une conversion numérique sont utilisés dans un laboratoire métrologique installé au bord d'un hélicoptère.

Ryszard Klimkiewicz  
Piotr Tyrawa

## PRÜFUNGEN DER STRAHLUNGSDIAGRAMMES DER AM HUBSCHRAUBER INSTALLIERTEN MESSANTENNEN

### Zusammenfassung

In dem Artikel wurden drei Methoden dargestellt, die die Ausführung der Messung der Strahlungsdiagrammes der am Hubschrauber installierten Messantennen ermöglichen. Für praktische Realisierung wurde die Methode des Kreisfluges des Hubschraubers gewählt. Die Resultate der für ausgewählte Frequenzreihe gefürten Messungen werden nach numerischer Verarbeitung in metrologischer Praxis des Hubschrauber-Laboratoriums ausgenutzt.





## AUTORZY



Mgr inż. Ryszard Klimkiewicz urodził się w 1934 r. Studia na Wydziale łączności Politechniki Wrocławskiej ukończył w 1957 r. W latach 1956-1959 pracował w Instytucie łączności we Wrocławiu. Od 1960 r. do 1966 r. był głównym konstruktorem Zakładów Radiowych i Telewizyjnych "ZARAT" (Zakład Produkcji Anten) we Wrocławiu. W 1968 r. ponownie zatrudnił się w Instytucie łączności. Specjalizuje się w dziedzinie radiotechniki nadawczej, ze szczególnym uwzględnieniem nadawczych systemów antenowych. Zgodnie ze swoją specjalnością, zdecydowaną większość swojego życia zawodowego przeznaczą na działalność w dziedzinie anten, zajmując się ich konstrukcją, budową, metrologią i normalizacją. W ciągu ostatnich kilku lat z powodzeniem prowadzi całość zagadnień merytorycznych związanych z rozwojem i wykorzystaniem śmigłowcowego laboratorium do pomiarów właściwości kierunkowych anten.



Dr inż. Zbigniew Kowalski urodził się w 1923 r. Uczęszczał do Szkół im. J. Zamoyckiego w Warszawie do r. 1939. W r. 1946, po ukończeniu Szkoły Inżynierskiej im. Wawelberga i Rotwanda, uzyskał tytuł inżyniera elektryka. W latach 1947-1951 był asystentem w Zakładzie Radiotechniki tej Uczelni. W latach 1951-1955 pełnił obowiązki kierownika Zespołu, a potem Pracowni łączności w Biurze Projektowym "Prozamet". Od 1955 r. jest zatrudniony w Instytucie łączności: od r. 1962 na stanowisku adiunkta, od r. 1990 - docenta

kontraktowego w Zakładzie Podstawowych Problemów Telekomunikacji. Specjalizuje się w zagadnieniach jakości transmisji w sieci telefonicznej. Z tej dziedziny napisał rozprawę doktorską, uzyskując w r. 1979 stopień doktora nauk technicznych. Opublikował łącznie około 100 artykułów, w tym kilka m.in. w "Archiwum Elektrotechniki", "Rozprawach Elektrotechnicznych" i w "Pracach Instytutu Łączności".



Mgr inż. Piotr Tyrawa urodził się w 1940 r. w Nakle. W 1966 r. ukończył studia na Wydziale Elektroniki Politechniki Wrocławskiej (specjalność radiotechnika). W tym samym roku rozpoczął pracę w Oddziale Wrocławskim Instytutu Łączności. Aktualnie jest adiunktem - kierownikiem Pracowni Anten Telewizyjnych. Zajmuje się głównie zagadnieniami projektowania anten, m.in. anten okrętowych, telewizyjnych, radiotelefonicznych sieci ruchomych, a także urządzeń antenowych. Jest rzeczoznawcą SEP w dziale elektroniki.

Dr inż. Elżbieta Andrukiewicz - notkę biograficzną wydrukowano w Pracach Instytutu Łączności, nr 94, 1987.

Inż. Jan Bogucki - notkę biograficzną wydrukowano w Pracach Instytutu Łączności, nr 1(77), 1975.

Ryszard Klimkiewicz, Piotr Tyrawa - Testing of radiation patterns of measuring antennas installed on a he-

Stanisław Miszczak, Andrzej Zieliński - Wspomnienie o Profesorze Stanisławie Dymowskim .....  
Elżbieta Andrukiewicz - Protocoles cryptographiques dans les reseaux téléinformatiques .....  
Zbigniew Kowalski (Habdank) - Analyse des propriétés de l'affaiblissement de référence modifié .....  
Jan Bogucki - Non homogenes lignes de transmission avec une distribution exponentielle cosinus carré et parabolique .....  
Ryszard Klimkiewicz, Piotr Tyrawa - Études des diagrammes de rayonnement des antennes embarquées sur

Stanisław Miszczak, Andrzej Zieliński - Wspomnienie o Profesorze Stanisławie Dymowskim .....  
Elżbieta Andrukiewicz - Kryptografische Protokolle in teleinformatischen Netzen .....  
Zbigniew Kowalski (Habdank) - Analyse der Eigenschaften der modifizierten Bezugsdämpfung .....  
Jan Bogucki - Inhomogene Übertragungsleitungen mit Exponential-,  $\cos^2$ - und parabolischer Verteilung .....  
Ryszard Klimkiewicz, Piotr Tyrawa - Prüfungen der Strahlungsdiagrammes der am Hubschrauber installierten

