PRACE INSTYTUTU ŁĄCZNOŚCI

1999
112

PRACE INSTYTUTU ŁĄCZNOŚCI

INSTYTUT ŁĄCZNOŚCI NR 112

WARSZAWA 1999

ISSN 0020-451X

Redaktor: mgr Krystyna Juszkiewicz

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

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

SPIS TREŚCI

СОДЕРЖАНИЕ

CONTENS

SOMMAIRE

INHALTSVERZEICHNIS

Elżbieta Andrukiewicz

004.056.5

NOWE SPOJRZENIE NA BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH

Przedstawiono ewolucję pojęcia bezpieczeństwa systemów informatycznych, jaką można zaobserwować w ostatnich latach. Wykazano, że bezpieczeństwo systemu oznacza więcej niż bezpieczeństwo informacji i należy rozszerzyć je o pojęcie bezpieczeństwa świadczenia usług. Powoduje to konieczność sformułowania nowych i zmodyfikowania istniejących kryteriów bezpieczeństwa. Spełnienie tych kryteriów może zapewnić polityka bezpieczeństwa definiowana na poziomie celów, strategii i działań. Zasadniczą tematyką tego artykułu jest realizacja polityki na poziomie działań. W tym celu wymagania bezpieczeństwa zostały sklasyfikowane w jedenastu obszarach bezpieczeństwa. W każdym z tych obszarów omówiono organizacyjny i techniczny aspekt bezpieczeństwa systemu informatycznego.

1. WSTĘP

Jednym z fundamentów rozwoju cywilizacji jest informacja. Efektywność tworzenia, rozpowszechniania i rozszerzania wiedzy, a co się z tym wiąże, postęp cywilizacyjny, opiera się na wymianie informacji. Drugim elementem tego rozwoju jest jednak konkurencja. Szanse przetrwania ma ten, kto okaże się lepszy od innych. Te dwa punkty widzenia są wzajemnie sprzeczne. Prymat konkurencji nad innymi zachowaniami powoduje narzucenie zasadniczych ograniczeń na nieskrępowane i bezwarunkowe rozpowszechnianie informacji. Potrzeba ochrony informacji w taki sposób, aby przedwcześnie nie została ona ujawniona komuś spoza kręgu osób wtajemniczonych, przybierała zawsze postać zbioru reguł i zakazów definiujących

bezpieczeństwo informacji. Zbiory te, w swej zasadniczej zawartości, odnoszą się do sposobu użytkowania środków przetwarzania informacji. Współcześnie środki te przybrały postać systemów i sieci teleinformatycznych. Postęp techniczny wpływa na ewolucję pojęcia bezpieczeństwa informacji oraz środków, za pomocą których jest ona przechowywana, przetwarzana i przesyłana. W ostatnich latach można zaobserwować istotną zmianę kierunku, w jakim podążają systemy teleinformatyczne. Okazuje się bowiem, że rozwój nowoczesnych technik informacyjnych staje się wartością cywilizacyjną samą w sobie. Innymi słowy, systemy teleinformatyczne przestały służyć jedynie jako środki wymiany informacji, a stały się źródłem tworzenia nowych usług. W ten sposób i bezpieczeństwo tych systemów stało się odrębną kategorią, do której należy włączyć nie tylko bezpieczeństwo informacji, jaka znajduje się w tych systemach, ale także bezpieczeństwo usług, które są realizowane za ich pomocą. W niniejszym artykule podjęto próbę odpowiedzi na pytanie, w jaki sposób sformułować definicję bezpieczeństwa systemów informacyjnych, która byłaby odpowiednia do roli, jaką systemy te pełnią obecnie.

2. EWOLUCJA POJĘCIA BEZPIECZEŃSTWA INFORMACJI I SYSTEMÓW INFORMATYCZNYCH

2.1. Tradycyjne kryteria bezpieczeństwa

Bezpieczeństwo informacji było tradycyjnie pojmowane jako spełnienie trzech kryteriów: poufności, integralności i dostępności. Informacja była bezpieczna, gdy:

- nie została przedwcześnie ujawniona,
- nie została w żaden sposób zniekształcona lub zmieniona,
- była dostępna w wyznaczonym czasie.

Wczesne chronione systemy komputerowe przetwarzające informacje przypominały fortecę. Fizyczne zabezpieczenia centralnego

ośrodka przetwarzania danych, wykwalifikowany i starannie selekcjonowany personel, zamknięte zastosowania stwarzały realną trudność dostępu do systemu. To poczucie pewności zabezpieczeń powodowało dodatkowe uproszczenie kryteriów bezpieczeństwa. Wykształciło się bowiem przekonanie, że zagrożenie dla bezpieczeństwa informacji pojawiało się w momencie, gdy opuszczała ona system. Analizowano zatem jedynie pasywne (podsłuch) lub aktywne metody przechwycenia informacji (kryptoanaliza szyfrów). Dość często jeszcze w dzisiejszych czasach można spotkać opinie, że bezpieczeństwo informacji to zapewnienie jej tajności. Nic bardziej mylącego. W artykule [7] opisano wiele praktycznych przykładów, w których bezpieczeństwo informacji polega w głównej mierze na zapewnieniu jej integralności i dostępności, a w znacznie mniejszym stopniu - poufności. Oto jeden z podanych przykładów, który w dalszej części artykułu będzie kilkakrotnie przytaczany i rozwijany dla poparcia prezentowanych tez.

Analizie poddano bezpieczeństwo systemu informatycznego banku. System informatyczny współczesnego banku jest podstawowym narzędziem realizacji celów jego działalności, pojmowanych jako świadczenie usług bankowych i czerpanie z tego zysków.

Co dla banku oznacza utrata poufności informacji o transakcjach klientów? Informacja o stanie kont zostanie opublikowana (np. w Internecie). Może to narazić bank na znaczne nieprzyjemności, utratę części klientów oraz straty finansowe z tytułu odpowiedzialności cywilnej.

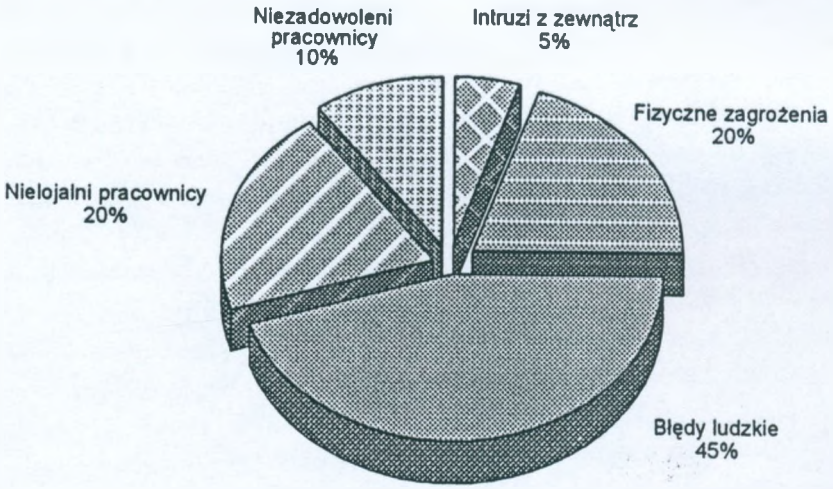
Co oznacza utrata dostępności informacji w systemie bankowym, np. przez miesiąc? Dla banku może to oznaczać katastrofę.

Wreszcie, co oznacza utrata integralności informacji w systemie? Stany kont klientów są liczbami przypadkowymi i nie ma możliwości ustalenia prawidłowych wartości!

Realną groźbą dla przedstawionej w przykładzie instytucji w przypadku utraty integralności i dostępności danych może być zatem jej

upadek. Warto zauważyć, że utratę dostępności zwykle można wykryć znacznie wcześniej niż utratę integralności.

Pozorne poczucie bezpieczeństwa systemu informatycznego pojmowanego jako forteca, poza zubożeniem kryteriów, powodowało, że stosowane mechanizmy były nieefektywne. Często się zdarzało, że jakkolwiek wejście do systemu było bardzo utrudnione, to wewnątrz nie było praktycznie żadnych zabezpieczeń. Szyfrowanie, fizyczne odseparowanie oraz kontrola dostępu były nieskuteczne wobec naruszeń bezpieczeństwa powodowanych przez własny personel. Wiele niezależnie przeprowadzonych badań [4, 5] od lat wskazywało, że największym zagrożeniem dla bezpieczeństwa systemu są błędy i rozmyślne działania pracowników! (rys. 1).



Rys. 1. Rozkład źródeł naruszeń bezpieczeństwa systemu informatycznego[1)]

[1)] Źródło: Hewlett Packard, 1999.

1.2. Rozszerzenie definicji bezpieczeństwa

Upowszechnienie sieci komputerowych zmieniło charakterystykę przechowywania, przetwarzania i przesyłania informacji. Użytkownicy, zasoby oraz funkcje, które do tej pory były ulokowane w jednym miejscu, teraz uległy rozproszeniu. I tak:

- przetwarzanie informacji jest realizowane za pomocą wielu procesorów rozdzielonych od siebie geograficznie;
- moc przetwarzania jest ulokowana znacznie bliżej użytkownika, w jego własnym komputerze lub na odległym - ale dedykowanym do realizacji określonej funkcji - serwerze;
- procesory mogą wykonywać zadanie równolegle oraz korzystać z wyników pracy innych procesorów, co powoduje konieczność właściwej komunikacji między procesorami;
- rozwój telekomunikacji umożliwia rzeczywiste **współdzielenie zasobów**, co oznacza:
  - rozproszone składowanie danych,
  - dostęp do rozproszonych baz danych,
  - zdalne przetwarzanie danych,
  - przesyłanie wiadomości.

W ostatnich latach gwałtowny rozwój Internetu spowodował, że współdzielenie zasobów może mieć charakter globalny.

Współdzielenie zasobów jest zatem pojęciem - kluczem do zrozumienia zmieniającej się roli systemów informacyjnych. Współczesny system informacyjny służy już nie tylko do transferu informacji. Jest narzędziem świadczenia różnego typu usług, w których wymiana informacji nie jest celem, ale jednym ze środków realizacji danej usługi. Dla tych systemów pojęcie bezpieczeństwa informacji jest zbyt wąskie. Bezpieczeństwo informacji oraz zabezpieczenie świadczenia usług tworzy szerszą kategorię, którą jest **bezpieczeństwo systemów informatycznych.** W tym nowym ujęciu bezpieczeństwa należy zmodyfikować istniejące kryteria oraz dołożyć kilka nowych.

Warto rozpatrzyć przykład użytkownika zdalnego dołączonego do systemu informatycznego. W skrajnym przypadku może to być klient, który chce korzystać z nowych możliwości oferowanych przez jego bank, tzw. "banku internetowego".

Jak należy zmodyfikować dotychczasowe kryteria bezpieczeństwa informacji? Z analizy przeprowadzonej w poprzednim przykładzie wynikało, że kryterium integralności informacji w wielu przypadkach może być najważniejszym kryterium jej bezpieczeństwa. Jednakże, w systemach rozproszonych pojęcie integralności obejmuje nie tylko poprawność przetwarzania informacji - zachowanie nienaruszonej zawartości danych i ich etykiet - w poszczególnych elementach systemu (np. w komputerze klienta i na serwerze banku), ale także ochronę przed nieuprawnionym zniekształceniem lub modyfikacją w trakcie transferu danych między tymi elementami. Integralność komunikacji można rozpatrywać w aspekcie poprawności transmisji, autentyczności źródła i ujścia danych (kryterium wspomniane wcześniej), poprawności protokołów itp. Tak samo poufność informacji musi obejmować wymagania poufności transmisji realizowanej za pośrednictwem publicznie dostępnych systemów i sieci teletransmisyjnych. Rozproszony charakter systemu powoduje konieczność uwzględnienia nowych aspektów dostępności informacji. Na spełnienie tego kryterium ma wpływ nie tylko zdolność przetwarzania poszczególnych elementów systemu, ale także zależności między nimi (w jakim zakresie jeden element musi czekać na wyniki przetwarzania w drugim elemencie) oraz sprawność systemu telekomunikacyjnego. Dlatego dostępność informacji należy rozpatrywać w kategoriach kryteriów czasowych.

Jakie nowe problemy bezpieczeństwa mogą powstać w rozproszonym, bankowym systemie informacyjnym, w którego skład dodatkowo wchodzi pewna, wirtualna część sieci globalnej?

Podstawowym elementem bezpieczeństwa jest uwierzytelnienie zarówno użytkownika, jak i odległego serwera. Zwykła procedura ban-

kowa stwierdzenia tożsamości oraz weryfikacji prawa do żądania wykonania polecenia musi zostać zrealizowana środkami elektronicznymi. Bank i jego klient znajdujący się na drugim końcu łącza muszą mieć pewność, że nawiązały komunikację z tym podmiotem, za którego druga strona się podaje. Ponadto, że przesyłana wiadomość (np. polecenie przeprowadzenia transakcji oraz potwierdzenie przyjęcia polecenia) będzie autentyczna (tzn. nie zostanie podstawiona gdzieś w pośrednim węźle komunikacyjnym inna, fałszywa wiadomość). Te dwa aspekty bezpieczeństwa informacji są określane jako **autentyczność systemu oraz danych**. Należy zatem dodać do definicji bezpieczeństwa informacji kolejne dwa kryteria autentyczności (systemu i danych).

Podstawowym aspektem bezpieczeństwa takiego systemu musi stać się jednoznaczne i niezaprzeczalne przypisanie poszczególnych transakcji poprawnie zidentyfikowanym użytkownikom. Prowadzi to do zdefiniowania kolejnego kryterium bezpieczeństwa: pełnej **rozliczalności** użytkowników oraz działań przez nich realizowanych.

Należy założyć jednakże, że w obrębie swych usług bank oferuje swoim klientom szeroki wachlarz produktów: np. zakup akcji, obligacji, zawarcie transakcji terminowych. W niektórych sytuacjach najważniejszym kryterium jest dostępność tych usług. Jakie straty poniesie klient, który w najodpowiedniejszym dla niego momencie nie będzie mógł zrealizować zakupu lub sprzedaży akcji?

Bezpieczeństwo świadczenia usług, tzn. pewność, że w wyznaczonym czasie usługa będzie dostępna, a jej jakość - gwarantowana, wymaga sformułowania kolejnych kryteriów. Do nich należą: **niezawodność, integralność i dostępność** tego systemu.

Odmowa świadczenia usługi (*denial of service)* w systemach informatycznych nie była dotąd wiązana z problematyką bezpieczeństwa. Było to zagadnienie inżynieryjne w dziedzinie niezawodności, utrzymania i dostępności *(RMA – reliability, maintenance, availability*). Wymagania w tym zakresie spełniały systemy wyposażone w funkcje

i urządzenia nadmiarowe, zaawansowane systemy diagnostyczne oraz elementy pracujące w trybie „gorącej rezerwy".

Interakcja między elementami systemu rozproszonego oraz konieczność zapewnienia komunikacji między tymi elementami stawiają nowe wymagania w zakresie niezawodności. W systemie rozproszonym o wiele łatwiej jest znaleźć punkt, z którego można uprawnionym użytkownikom zablokować dostęp do jego zasobów. W ostatnim czasie nastąpił gwałtowny wzrost liczby ataków na serwery internetowe, w wyniku których dostęp do tych serwerów był albo całkowicie blokowany, albo znacznie utrudniony [6]. Dlatego właśnie niezawodność, integralność i dostępność zasobów stają się nowymi kryteriami bezpieczeństwa we współczesnych systemach rozproszonych.

Bezpieczeństwo nie jest kategorią absolutną. Niełatwo jest je zmierzyć i sklasyfikować. Nie ma międzynarodowych standardów traktujących całościowo zabezpieczenie systemów informatycznych. W wielu krajach są publikowane poradniki, wytyczne i podręczniki. Jak do tej pory, tylko w jednym kraju (Wielka Brytania) obowiązuje norma krajowa [3], zawierająca wytyczne do zarządzania bezpieczeństwem w systemach informatycznych. Została ona wdrożona w wielu przedsiębiorstwach i organizacjach, nie tylko brytyjskich. Jest podstawowym dokumentem, na podstawie którego brytyjskie instytucje certyfikujące udzielają akredytacji politykom bezpieczeństwa. Norma brytyjska, podobnie jak znakomita większość publikacji z zakresu bezpieczeństwa systemów informatycznych, utożsamia bezpieczeństwo tych systemów z bezpieczeństwem informacji. Zgodnie z definicją tam podaną, bezpieczeństwo informacji to:

"Ochrona informacji dla zapewnienia:

a) poufności, co oznacza ochronę wrażliwej informacji przed ujawnieniem lub przechwyceniem przez nieuprawnione osoby;

b) integralności, co oznacza nienaruszalność informacji i oprogramowania komputerowego;

c) *dostępność, co oznacza pewność, że informacja oraz usługi o znaczeniu krytycznym są w żądanym czasie dostępne dla użytkowników".*

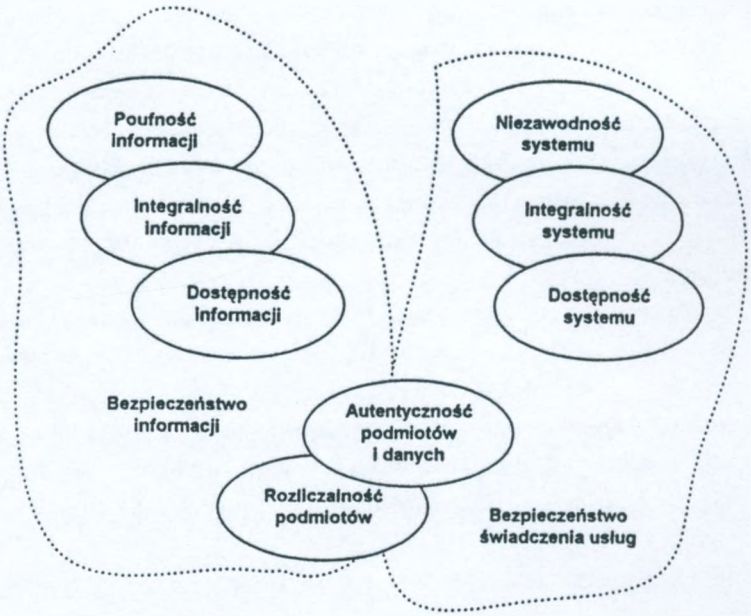
Z analizy przeprowadzonej w tym artykule wynika, że dla współczesnych systemów informatycznych definicja ta jest niewystarczająca z dwóch powodów:

a) istnieją dodatkowe kryteria bezpieczeństwa informacji takie, jak autentyczność danych i użytkowników oraz rozliczalność użytkowników, a istniejące (poufność, integralność i dostępność) muszą uwzględniać rozproszony charakter zasobów systemu; spełnienie zatem powyższych kryteriów oznacza konieczność ochrony zasobów, których przynależność nie jest jednoznacznie określona (np. wirtualny charakter połączeń internetowych sprawia, że w skrajnym przypadku każda cząstka informacji (pakiet) może być transmitowana inną drogą);

b) rozproszone systemy informatyczne oferują usługi, w których wymiana informacji jest tylko jednym ze środków ich realizacji; bezpieczeństwo świadczenia usług, obok bezpieczeństwa informacji, obejmuje także bezpieczeństwo samej infrastruktury, a więc integralność, dostępność i niezawodność systemu, a także autentyczność i rozliczalność jego użytkowników; prowadzi to do sformułowania nowych kryteriów bezpieczeństwa:
   - **rozliczalności,** co oznacza określenie i weryfikowanie odpowiedzialności za działania, usługi i funkcje realizowane za pośrednictwem systemu informatycznego;
   - **autentyczności,** co oznacza pewność, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy takich podmiotów, jak: użytkownicy, procesy, systemy i informacja;
   - **integralności** (zasobów systemu), co oznacza, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej;

- **dostępności** (zasobów systemu), co oznacza zdolność bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez upoważniony podmiot;
- **niezawodności,** co oznacza gwarancję odpowiedniego zachowania się systemu informacyjnego i spójności otrzymanych wyników, które powinny uzupełnić dotychczasowe kryteria poufności, integralności i dostępności informacji.

Zabezpieczanie systemów informatycznych obejmuje wszelkie działania związane ze zdefiniowaniem, osiągnięciem i utrzymaniem stanu spełnienia kryteriów, czyli osiągnięcia stanu bezpieczeństwa tego systemu. Na rys. 2 przedstawiono kryteria bezpieczeństwa z uwzględnieniem podziału na bezpieczeństwo informacji oraz bezpieczeństwo świadczenia usług.



Rys. 2. Kryteria bezpieczeństwa systemu informatycznego

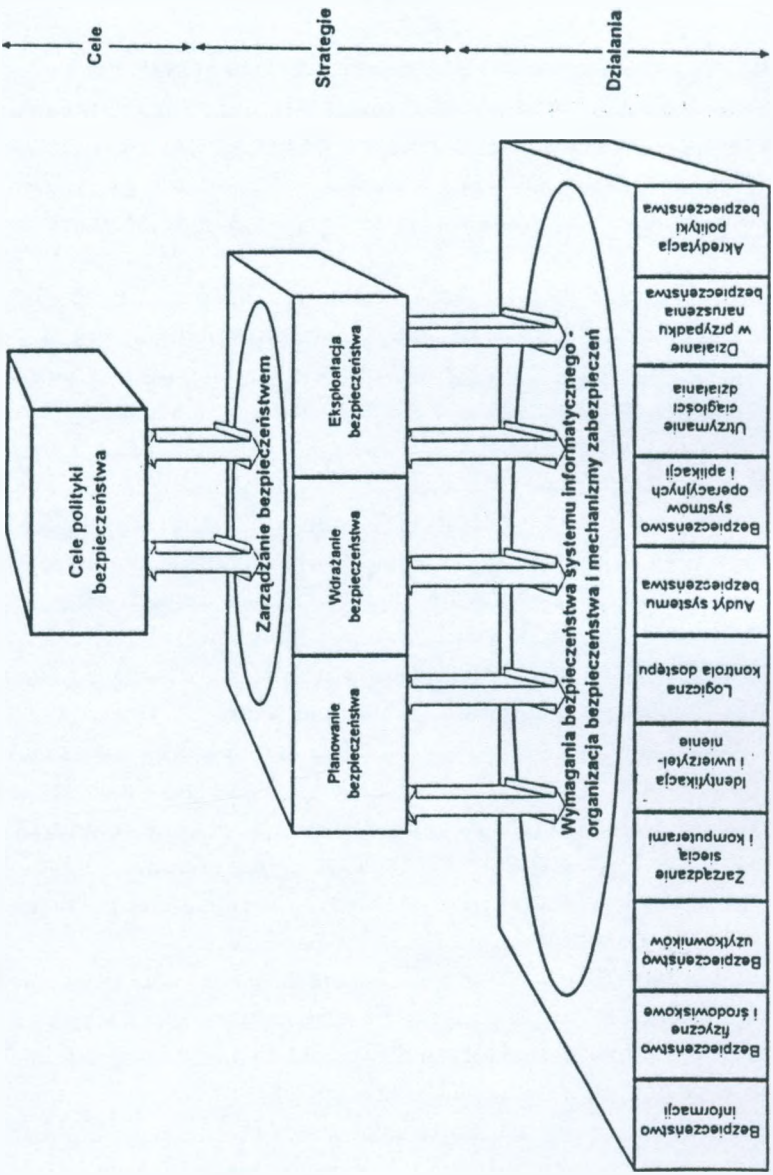
3. STRUKTURA POLITYKI BEZPIECZEŃSTWA

Osiągnięcie i utrzymanie stanu bezpieczeństwa systemu informatycznego wymaga zdefiniowania, wdrożenia i utrzymania polityki bezpieczeństwa. Zgodnie z [9], polityka bezpieczeństwa to udokumentowany zbiór zasad, praktyk i procedur, w którym dana organizacja określa, w jaki sposób chroni aktywa swego systemu informatycznego.

Politykę bezpieczeństwa można definiować na poziomie celów, strategii i działań (rys. 3). W modelu zaprezentowanym w tym artykule polityka bezpieczeństwa ma budowę wielopoziomową, w której cele przekładają się na strategie, a strategie na działania. Za zdefiniowanie celów jest odpowiedzialne kierownictwo organizacji. Zarządzanie bezpieczeństwem jest realizacją celów polityki bezpieczeństwa. W procesach zarządzania bezpieczeństwem dokonuje się wyboru strategii, np. strategii analizy ryzyka. Procesy zarządzania bezpieczeństwem umożliwiają poprawne planowanie, wdrożenie i eksploatację bezpieczeństwa. Odpowiedzialność za prawidłowe zarządzanie bezpieczeństwem ponoszą menadżerowie bezpieczeństwa (kierownictwo służb zabezpieczenia lub działu informatycznego). Wreszcie, na poziomie działań cele i strategie przekładają się na konkretne działania: sformułowanie wymagań na organizacyjne, prawne i techniczne środki zabezpieczenia, opracowanie i wdrożenie planów, regulaminów, procedur, mechanizmów zabezpieczeń. Tu odpowiedzialność rozkłada się na inspektorów bezpieczeństwa, administratorów systemów i aplikacji programowych oraz użytkowników.

Zdefiniowanie zbioru kryteriów bezpieczeństwa ma znaczenie podstawowe dla realizacji polityki bezpieczeństwa na wszystkich szczeblach. Pominięcie niektórych kryteriów znajdzie swe odbicie zarówno w celach, strategiach, jak i działaniach.

Warto przeanalizować na przykładzie naszego banku pominięcie kryterium autentyczności podmiotów. W celach polityki bezpieczeń-



Rys. 3. Wielopoziomowa struktura polityki bezpieczeństwa

stwa może zabraknąć zapisu dotyczącego autentyczności użytkowników korzystających z usług banku oraz autentyczność przedstawianych danych identyfikujących.

W analizie ryzyka, będącej jednym z procesów planowania bezpieczeństwa, może zostać pominięte zagrożenie w postaci podszycia się pod uprawnionego użytkownika oraz konsekwencja - nieautoryzowana transakcja na jego koncie. W rezultacie nie zostanie stwierdzona potrzeba użycia silnych mechanizmów uwierzytelniających i bank pozostanie przy tradycyjnej technice hasła (ewentualnie, innych prostych informacji, które uprawniony użytkownik powinien znać).

W wymaganiach pominięto opis procedur silnego uwierzytelniania oraz mechanizmów programowych i sprzętowych, zapewniających takie uwierzytelnienie. Bezpieczeństwo tego systemu będzie miało wbudowaną od początku "dziurę".

Pominięcie niektórych kryteriów bezpieczeństwa w systemie informatycznym rzutuje na postać wymagań na najniższym poziomie obszarów bezpieczeństwa. Na rys. 4 przedstawiono porównanie obszarów bezpieczeństwa zdefiniowanych w normie brytyjskiej (po lewej stronie) z najniższym poziomem strukturalnej polityki bezpieczeństwa prezentowanej w tym artykule. Obszary, które nie występują w ogóle w normie brytyjskiej są zakreskowane.

Dodatkową zaletą warstwowego podejścia jest, mniejsze niż w jednowymiarowym modelu prezentowanym w normie brytyjskiej, uzależnienie polityki od szybko zmieniającego się środowiska, w którym działa system informatyczny. Przykładowo, jeśli na samym dole "piramidy" zajdzie potrzeba modyfikacji zabezpieczenia (organizacyjnego lub technicznego), to impuls ten znajdzie odbicie na poziomie wyższym, w warstwie zarządzania bezpieczeństwem. W procesie monitorowania bezpieczeństwa zostanie rozpoznany zakres procesu planowania bezpieczeństwa, tzn. proces analizy ryzyka zostanie uruchomiony dla wskazanego obszaru systemu informatycznego, a w jej wyniku powstanie zmodyfikowany plan bezpieczeństwa. W ten spo-

Rys. 4. Obszary bezpieczeństwa zdefiniowane przez Autorkę (po prawej) oraz w normie [3] (po lewej)

sób konieczność modyfikacji zabezpieczenia będzie miała ograniczony wpływ na politykę bezpieczeństwa. Z punku widzenia samego dokumentu polityki zmiana ta może polegać na modyfikacji lub wymianie jednego z załączników. Strukturalne podejście do polityki bezpieczeństwa charakteryzuje się zatem efektywnością i niezmiennością.

Jednowymiarowość modelu bezpieczeństwa prezentowanego w normie [3] powoduje, że identyfikacja zależności między celami polityki a wymaganiami w określonych obszarach bezpieczeństwa jest utrudniona. Dlatego trudno określić, w jaki sposób może być efektywnie realizowana modyfikacja tej polityki.

Należy zaznaczyć, że w przypadku systemów informacyjnych, dla których podstawowymi kryteriami bezpieczeństwa są: poufność, dostępność i integralność informacji przetwarzanej na potrzeby wewnętrzne, norma [3] może być najzupełniej wystarczająca.

W systemach otwartych, w których autentyczność danych i użytkowników oraz rozliczalność użytkowników muszą być brane pod uwagę jako kryterium bezpieczeństwa informacji i/lub charakter działalności powoduje, że za pośrednictwem systemu informatycznego dana instytucja świadczy usługi, warto budować politykę opartą na modelu strukturalnym proponowany w tym artykule.

Zagadnienia związane z dwoma pierwszymi poziomami polityki bezpieczeństwa, tzn. określeniem celów polityki oraz zarządzaniem bezpieczeństwem zostały szczegółowo omówione w [2]. W tym opracowaniu zostanie opisana polityka bezpieczeństwa na poziomie działań. Polityka ta przybiera postać wymagań bezpieczeństwa.

4. OBSZARY BEZPIECZEŃSTWA - ORGANIZACJA BEZPIECZEŃSTWA I MECHANIZMY ZABEZPIECZEŃ

Na poziomie działań politykę bezpieczeństwa można realizować w poszczególnych obszarach bezpieczeństwa (rys. 3 i 4). Celem skla-

syfikowania obszarów bezpieczeństwa jest logiczne rozdzielenie zadań organizacyjnych oraz mechanizmów zabezpieczenia.

Złożoność problematyki bezpieczeństwa powoduje, że nie zawsze obszary te można całkowicie rozdzielić. W pewnych przypadkach wymagania związane z jednym zagadnieniem dotyczą także sfery problemów definiowanych w innym obszarze bezpieczeństwa.

Bezpieczeństwo na poziomie wymagań ma dwa aspekty: techniczny i organizacyjny. Organizacja i mechanizmy zabezpieczeń są wzajemnie ze sobą powiązane. Każdy techniczny środek zabezpieczenia wymaga określenia zasad jego użytkowania. Z kolei, dla każdego regulaminu organizacyjnego są niezbędne techniczne środki realizacji. Z tego względu obszar bezpieczeństwa jest zdefiniowany na podstawie mechanizmów zabezpieczenia oraz organizacji bezpieczeństwa.

4.1. Bezpieczeństwo informacji

Celem zdefiniowania tego obszaru bezpieczeństwa jest spełnienie kryterium poufności, integralności, dostępności i autentyczności aktywów informacyjnych instytucji oraz rozliczalności jej użytkowników. Kluczowe znaczenie dla bezpieczeństwa informacji ma jego organizacja.

4.1.1. Organizacyjny aspekt bezpieczeństwa informacji

Klasyfikacja informacji jest jednym z podstawowych działań przy określaniu potrzeb w zakresie bezpieczeństwa, czyli ogólnej analizy ryzyka. Określenie stopnia wrażliwości informacji, tzn. przyjęcie skali wartościowania ochrony informacji, stanowi przesłankę do przyjęcia odpowiedniej dla systemu informacyjnego oraz potrzeb danej instytucji strategii analizy ryzyka. Opis procesu wyboru analizy ryzyka znajduje się w [1]. W niniejszym artykule zakłada się, że informacja w systemie jest sklasyfikowana; zdefiniowano obszary jej występowa-

nia (aktywa, za pomocą których informacja ta jest przechowywana, przetwarzana i przesyłana), a odpowiednie środki jej ochrony zostaną uwzględnione w wymaganiach bezpieczeństwa.

4.1.1.1. Zasady postępowania z informacją podlegającą ochronie

Powinny być określone następujące reguły:
- dystrybucji informacji, w tym etykietowanie informacji i nośników oraz dystrybucja informacji w postaci elektronicznej;
- szkolenia w zakresie postępowania z informacją podlegającą ochronie (patrz także 4.3.1.3);
- cyklu życia informacji (tzn. czas, po którym informacja może zostać ujawniona).

Reguły postępowania z informacją podlegającą ochronie są wdrażane za pomocą mechanizmów zabezpieczenia.

4.1.2. Mechanizmy zabezpieczenia informacji

Techniczne środki zabezpieczenia informacji występują w wielu obszarach bezpieczeństwa. Do takich mechanizmów należą:
- fizyczne środki zabezpieczenia w postaci stref bezpieczeństwa (patrz także 4.2.2.3);
- mechanizmy logicznej kontroli dostępu - (patrz także 4.6.2);
- kryptograficzne mechanizmy ochrony informacji - jej poufności oraz integralności i dostępności (patrz także 4.8.2.1);
- nieodtwarzalne kasowanie danych na nośnikach.

4.2. Bezpieczeństwo fizyczne i środowiskowe

Celem zdefiniowania tego obszaru zabezpieczenia jest potrzeba fizycznej ochrony oraz separacji tych aktywów systemu informacyjnego, których działanie jest krytyczne z punktu widzenia celów działania całej instytucji.

Zabezpieczenie fizyczne aktywów systemu informacyjnego jest jednym z elementów ogólnego procesu zabezpieczenia infrastruktury instytucji. Zabezpieczenie podstawowej infrastruktury budynku powinno być uwzględnione już na etapie jego budowy. Środki zabezpieczenia fizycznego powinny spełniać ogólne normy i wymagania, np. budowlane, przeciwpożarowe itp.

4.2.1. Organizacyjny aspekt bezpieczeństwa fizycznego i środowiskowego

Organizacyjny aspekt w tym obszarze bezpieczeństwa przejawia się w postaci:
- ogólnych zasad organizacji procesów budowlanych i montażowych;
- zasad organizacji fizycznego dostępu do stref bezpieczeństwa;
- zasad fizycznego zabezpieczenia nośników danych.

4.2.2. Mechanizmy zabezpieczenia fizycznego i środowiskowego

4.2.2.1. Bezpieczeństwo budynku

Bezpieczeństwo fizyczne systemu informacyjnego zależy od cech budynku, w którym działa. Należy brać pod uwagę następujące uwarunkowania:
- wybór odpowiedniej lokalizacji;
- zabezpieczanie podstawowych instalacji budynku;
- zabezpieczenia antywłamaniowe.

4.2.2.2. Bezpieczeństwo infrastruktury i urządzeń systemu informacyjnego

Problemy związane z infrastrukturą systemu informacyjnego można rozpatrywać w następujących kategoriach:
- rozmieszczanie urządzeń systemu informacyjnego;

- zasilanie, w tym rezerwowe systemy zasilania;
- bezpieczeństwo okablowania;
- bezpieczeństwo urządzeń znajdujących się poza siedzibą instytucji.

4.2.2.3. Strefy zabezpieczeń

Fizyczne zabezpieczenie powinno opierać się na zdefiniowaniu stref kontrolnych i wprowadzeniu barier (perymetrów) między tymi strefami. Stworzenie bariery dla danej strefy powinno uwzględniać wartość chronionych aktywów i usług, a także ryzyko naruszenia zabezpieczeń oraz istniejące mechanizmy ograniczające to ryzyko. Każdy poziom fizycznego zabezpieczenia (jeśli zostały wyodrębnione) powinien mieć jednoznacznie przypisany zbiór mechanizmów kontrolujących wejście do strefy.

Chronione strefy powinny być wyposażone w mechanizmy (sprzętowe i/lub programowe) gwarantujące upoważnionym osobom autoryzowany dostęp. Należy rozpatrzyć zasadność stosowania dodatkowych ograniczeń, np. kontrolę dostępu gości i personelu pomocniczego oraz zapewnić niezwłoczne pozbawienie praw dostępu osób, które utraciły upoważnienie do wejścia do strefy (zwolnienie, przejście do innego działu itp.).

4.2.2.4. Emisja ujawniająca i impuls elektromagnetyczny

Każde urządzenie w systemie informatycznym jest źródłem promieniowania elektromagnetycznego. Promieniowanie to może przybrać jedną z trzech form propagacji:

- pola elektrycznego i pola magnetycznego oraz fal elektromagnetycznych;
- fal elektromagnetycznych emitowanych z zewnętrznych powłok metalicznych kabli koncentrycznych (tzw. fal powierzchniowych);

- prądów i napięć interferencyjnych indukowanych w liniach zasilania.

Skorelowanie informacji z niekontrolowaną emisją promieniowania nosi nazwę emisji ujawniającej. Informacja taka jest łatwa do przechwycenia. Zwykły odbiornik telewizyjny może stać się odbiornikiem sygnału niekontrolowanej emisji z odległości sięgającej do 100 m od źródła emisji. W przypadku zastosowania odbiorników o większej czułości jest możliwe przechwycenie informacji nawet z odległości kilku kilometrów. W przypadku fal powierzchniowych oraz pól indukowanych w kablach zasilających odległości te wynoszą ok. 100 ÷ 150 m [10]. Cechą charakterystyczną emisji niekontrolowanej jest zdolność przechodzenia sygnału z jednej formy propagacji w drugą. Przykładowo, fala elektromagnetyczna natrafiając na przewodnik, może być propagowana dalej w postaci fali powierzchniowej. Dlatego ochrona przed emisją ujawniającą musi uwzględniać wszystkie typy propagacji oraz całą szerokość widma.

Niszczący wpływ impulsu elektromagnetycznego na urządzenia półprzewodnikowe opisano przy okazji badań nad zjawiskami zachodzącymi podczas eksplozji nuklearnej. W ostatnich latach zostały skonstruowane generatory fal elektromagnetycznych, których celem może być zniszczenie urządzeń elektronicznych, pracujących w systemach informatycznych.

4.2.2.5. Środki i mechanizmy ograniczające emisję ujawniającą oraz efekt działania impulsu elektromagnetycznego

Problematyka zwalczania niekontrolowanej emisji jest w dużej mierze dziedziną kompatybilności elektromagnetycznej, należy zatem w pierwszym rzędzie zagwarantować spełnienie przez urządzenia elektryczne techniki informatycznej krajowych norm dotyczących ograniczenia emisji elektromagnetycznej [11, 12].

Dodatkowe środki zabezpieczenia przed emisją ujawniającą można podzielić na trzy kategorie:
- modyfikacje urządzeń i przyrządów;
- stosowanie urządzeń maskujących;
- ekranowanie, blokowanie i filtrowanie.

Możliwości modyfikowania urządzeń przez zwykłego użytkownika systemu informatycznego są bardzo ograniczone z uwagi na brak specjalistycznej aparatury oraz utratę gwarancji producenta na posiadany sprzęt. Z kolei, oferowane na rynku urządzenia o obniżonym poziomie emisji elektromagnetycznej są bardzo kosztowne.

Stosowanie urządzeń maskujących (generatorów szumu elektromagnetycznego) jest prawnie zabronione, ponieważ są one źródłem zakłóceń dla wszystkich innych urządzeń elektrycznych pracujących w pobliżu.

Podstawowymi technikami dodatkowego ograniczania niekontrolowanej emisji dla większości systemów informatycznych jest ekranowanie. Można ekranować urządzenia, budynki i pomieszczenia oraz przenośne kabiny.

Praktycznie jedyną ochroną przed impulsem elektromagnetycznym jest instalowanie metalowych osłon. Stosuje się je przeważnie do zabezpieczenia najbardziej narażonych elementów systemów teleinformatycznych, np. anten. W zastosowaniach cywilnych zabezpieczenia przed impulsem elektromagnetycznym spotyka się bardzo rzadko.

4.3. Bezpieczeństwo użytkowników

Celem zdefiniowania tego obszaru jest zmniejszenie ryzyka popełnienia błędu, kradzieży, defraudacji, niewłaściwego użycia aktywów systemu informatycznego przez użytkowników tego systemu. W obszarze bezpieczeństwa użytkowników można rozpatrywać wyłącznie jego organizacyjny aspekt.

4.3.1. Organizacja bezpieczeństwa użytkowników

W zabezpieczeniu systemów informacyjnych najważniejszą rolę odgrywają ludzie. Oni też są przeważnie najsłabszym jego ogniwem. Wdrożenie, a następnie eksploatacja najlepszego planu zabezpieczenia nie będzie efektywna, jeśli użytkownicy pozostaną nieświadomi celów działań, jakie są podejmowane albo brakuje odpowiednich instrumentów weryfikujących, czy zasady organizacji bezpieczeństwa we wszystkich obszarach bezpieczeństwa są przestrzegane.

4.3.1.1. Separacja stanowisk i odpowiedzialności

Wszelkie stanowiska pracy w systemie informacyjnym powinny być definiowane z uwzględnieniem podstawowej zasady rozdzielenia obowiązków i odpowiedzialności.

Rozdzielenie obowiązków zmniejsza ryzyko niewłaściwego wykorzystywania aktywów systemu. Dotyczy to zwłaszcza separacji funkcji zarządzających, wykonawczych oraz kontrolnych. We wszystkich organizacjach, niezależnie od ich wielkości, należy przestrzegać rozdziału obowiązków i odpowiedzialności w zakresie następujących funkcji związanych z:

- użytkowaniem aktywów systemu (tzn. wprowadzaniem, przetwarzaniem, kontrolą przekazywania danych);
- zarządzaniem aktywami (tzn. systemem, siecią, komputerami, aplikacjami i bazami danych, pracami rozwojowymi);
- zarządzaniem bezpieczeństwem (np. konfiguracją systemu i jej zmianami, audytem, planami postępowania w sytuacjach awaryjnych i katastrofalnych oraz w warunkach naruszenia bezpieczeństwa).

4.3.1.2. Znaczenie polityki kadrowej dla bezpieczeństwa użytkowania systemu informatycznego

Przy kształtowaniu polityki kadrowej, uwzględniającej aspekt bezpieczeństwa systemu informatycznego należy kierować się następującymi zasadami:

- należy definiować stanowiska, zgodnie z wyżej wspomnianą zasadą separacji oraz zasadą minimalnych przywilejów (tzn. pracownik nie powinien mieć przydzielonych praw większych niż te, które są wystarczające do wykonania swoich obowiązków);
- należy definiować przywileje z uwzględnieniem efektywności pracy grup pracowników (możliwości zastępowania nieobecnych) oraz możliwości działania w stanach awaryjnych i katastrofalnych (np. warunkowe przydzielenie przywilejów) - patrz także 4.9.1.2;
- należy stworzyć klasyfikację stanowisk, uwzględniającą znaczenie dla bezpieczeństwa systemu i na tej podstawie różnicować wymagania dotyczące naboru pracowników;
- należy stworzyć procedury postępowania w przypadku wykrycia naruszenia bezpieczeństwa systemu na skutek działania rozmyślnego lub błędu użytkownika (patrz także 4.10.1);
- należy stworzyć procedury związane z zakończeniem użytkowania systemu informatycznego (na skutek zwolnienia, ustania kontraktu itp.) lub zmianą organizacyjną w instytucji (np. przesunięcia pracowników do pracy w innym dziale).

4.3.1.3. Uświadamianie, edukacja i szkolenie użytkowników

Zminimalizowanie zagrożeń w postaci błędów i przeoczeń, nadużyć oraz nieupoważnionych działań podejmowanych przez użytkowników wymaga ciągłego uświadamiania, szkolenia i edukacji.

Użytkownicy systemu informacyjnego powinni uzyskać odpowiednie informacje dotyczące zabezpieczenia tego systemu. Programy uświadamiania i szkolenia oraz edukacji użytkowników systemu informacyjnego powinny uwzględniać zróżnicowane potrzeby w zakresie znajomości zabezpieczenia systemu informacyjnego.

Uświadomienie pracowników w zakresie zabezpieczenia systemów informacyjnych obejmuje:

- przedstawienie celów polityki bezpieczeństwa prowadzonej w instytucji oraz pokazanie, w jaki sposób ta polityka przyczynia

się do realizacji celów działalności i ochrony aktywów tej instytucji;
- całkowite zrozumienie wytycznych w zakresie zabezpieczenia systemu informacyjnego.

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

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

Proces uświadamiania i szkolenia oraz edukacji w zakresie bezpieczeństwa powinien mieć charakter ciągły.

4.4. Zarządzanie siecią i komputerami

Obszar zarządzania systemem informacyjnym zawiera podstawowe rozwiązania techniczne i organizacyjne zabezpieczenia tego systemu. Obejmuje swym zakresem dość rozległe zagadnienia, które w tej części zostaną jedynie przedstawione, natomiast ich omówienie znajdzie się w części następnej cyklu artykułów.

Działania związane z zarządzaniem systemem informatycznym silnie zależą od typu i rodzaju systemu, wielkości instytucji, natury i wrażliwości przetwarzanych danych. Niemniej jednak, co do zasady, procedury zabezpieczenia powinny być takie same, natomiast mogą różnić się stopniem szczegółowości. Celem zdefiniowania

obszaru zabezpieczenia jest bowiem zapewnienie **niezawodności, dostępności i integralności** urządzeń sieciowych, komputerów oraz informacji.

4.4.1. Organizacyjny aspekt bezpieczeństwa zarządzania systemem informatycznym

4.4.1.1. Bezpieczeństwo systemu zarządzania

Zarządzanie infrastrukturą techniczną systemu informatycznego dzieli się na dwie kategorie: zarządzanie siecią i komputerami. Z punktu widzenia zabezpieczenia, system zarządzania siecią nadzoruje wykorzystanie sieci i zasobów telekomunikacyjnych do przenoszenia danych między komputerami (terminalami) oraz między komputerem (terminalem) a jego użytkownikiem. System zarządzania komputerami powinien zapewniać zestaw narzędzi i procedur do ochrony plików oraz baz danych przechowywanych na poszczególnych komputerach.

- **Zarządzanie siecią**

Wśród problemów organizacji bezpieczeństwa zarządzania siecią można wymienić:

- zdefiniowanie obowiązków administratora systemu w zakresie zabezpieczenia jego działań w systemie w taki sposób, aby ograniczyć ryzyko błędów i nadużyć;
- określenie zasad zdalnego dostępu do systemu zarządzania (m. in. do przeprowadzenia działań diagnostycznych i utrzymaniowych);
- określenie zasad zarządzania kontami użytkowników, tak aby zapewnić rozliczalność ich działań (zgodnie z wyznaczonym w polityce bezpieczeństwa zakresem rozliczalności) oraz aktualność informacji związanej z tymi kontami;
- określenie trybu i procedur prowadzenia działań testowych oraz rozwojowych w sieci;

- opracowanie trybu i procedur tworzenia kopii bezpieczeństwa systemów odpowiedzialnych za działanie sieci (patrz także 4.9.1.3).

- **Zarządzanie komputerami**

Podstawowym aspektem organizacji bezpieczeństwa komputerów jest określenie zasad ochrony integralności danych i oprogramowania (np. dotyczących wprowadzania do systemu nie licencjonowanego oprogramowania oraz konfiguracji sprzętowej komputerów i stacji roboczych), a także ochrony danych przechowywanych na tych komputerach.

- **Bezpieczeństwo komputerów przenośnych**

Powinna być wprowadzona polityka użytkowania komputerów przenośnych określająca zasady: przechowywania istotnych danych, transportu komputerów, przekazywania komputerów osobom trzecim. Celem tej polityki jest zabezpieczenie przed utratą poufności, modyfikacją lub zniszczeniem danych. Polityka ta powinna uwzględniać większe ryzyko utraty informacji przechowywanej i przetwarzanej na komputerach tego typu.

4.4.1.2. Bezpieczeństwo komunikacji

W zakresie ogólnej polityki bezpieczeństwa powinny być przyjęte zasady komunikowania się systemu informacyjnego za pośrednictwem sieci rozległej (ze światem zewnętrznym) lub lokalnej (miedzy podsystemami w obrębie jednej instytucji). Ryzyko, jakie niesie ze sobą udostępnienie aktywów systemu informacyjnego na zewnątrz, powinno być minimalizowane. W przypadku stosowania „zapory ogniowej" (*firewall* - patrz 4.4.2.2) organizacja bezpieczeństwa komunikacji obejmuje odpowiedzi na następujące pytania:

- jaka informacja powinna być przepuszczana przez „zaporę ogniową" do i z chronionego systemu?

- jaka powinna być polityka w zakresie udostępniania usług przez zaporę ogniową (co jest zabronione, a co dozwolone)?
- jaką informację powinna „zapora ogniowa" zasłonić (np. wewnętrzną strukturę sieci lub nazwy użytkowników)?
- jakie jest szacowane zapotrzebowanie użytkowników na przepustowość i jak może ono zmienić się w przyszłości?

Zarówno w przypadku stosowania zapór ogniowych, jak i wirtualnych sieci prywatnych jednym z głównych problemów organizacyjnych jest zarządzanie kluczami kryptograficznymi, na podstawie których jest realizowane uwierzytelnianie, ochrona integralności i poufności przesyłanych danych (patrz 4.8.2).

4.4.1.3. Kopie bezpieczeństwa

Regularnie powinny być tworzone kopie bezpieczeństwa istotnych danych systemowych (np. plików konfiguracyjnych), oprogramowania, dokumentów. Odpowiednie ustalenia dotyczące przechowywania danych oraz dostępu do tych danych powinny być elementem planu zachowania ciągłości działania (patrz 4.9). Definiując zasady tworzenia kopii bezpieczeństwa w systemie należy uwzględniać konieczność:

- fizycznej separacji kopii bezpieczeństwa od innych aktywów systemu informacyjnego;
- właściwego dokumentowania tych kopii;
- testowania kopii bezpieczeństwa w celu weryfikacji gotowości użycia.

4.4.1.4. Dokumentacja systemu

Dokumentacja jest jednym z podstawowych aktywów systemu informatycznego i jako taka powinna być odpowiednio zabezpieczana. Dokumentacja powinna obejmować:

- dokumentację systemu, w szczególności jego konfiguracji;
- dokumentację procedur, zwłaszcza związanych z planowaniem, testowaniem i eksploatacją systemu, postępowanie z plikami danych;

- dokumentację zabezpieczenia systemu, zawierającą plany zabezpieczenia, plany utrzymania ciągłości działania, analizę ryzyka, politykę zabezpieczenia i procedury zabezpieczenia (np. uwierzytelnienia, kontroli dostępu itp.).

Określając dostępność poszczególnych części dokumentacji należy brać pod uwagę różne czynniki np. konieczność dostatecznie szybkiego uruchomienia planu zachowania ciągłości działania w przypadku awarii lub katastrofy.

4.4.1.5. Zarządzanie zmianami

Wprowadzanie zmian jest procesem, który powinien być kontrolowany tak, aby zminimalizować ryzyko uszkodzenia systemu informatycznego i, w szczególności, jego zabezpieczeń. W zakresie organizacji zarządzania zmianami należy przyjąć zasady:

- bezpieczeństwa wprowadzania zmian (tzn. kontrolowaną modyfikację systemów operacyjnych i aplikacji programowych);
- planowania pojemności systemu (tzn. uwzględnienia przyszłych potrzeb użytkowników przy określaniu wymaganych parametrów technicznych, np. mocy przetwarzania i pojemności pamięci);
- rutynowych procedur awaryjnych (zmian w systemie na skutek uszkodzeń lub awarii o drugorzędnym znaczeniu dla bezpieczeństwa systemu);
- identyfikacji, rejestracji i rozpowszechniania informacji o znaczących zmianach w systemie informatycznym.

4.4.2. Mechanizmy zabezpieczenia stosowane w zarządzaniu siecią i komputerami

4.4.2.1. Mechanizmy zabezpieczenia systemu zarządzania

Wśród środków zabezpieczenia systemu zarządzania w pierwszym rzędzie należy wymienić:

- prawidłową konfigurację elementów aktywnych sieci;
- prawidłową konfigurację sieciowego systemu operacyjnego;
- silne mechanizmy uwierzytelnienia i autoryzacji dostępu uprawnionych użytkowników do poszczególnych funkcji zarządzania systemem informatycznym oraz aktywów tego systemu (patrz 4.5.1 i 4.6.2);
- szyfrowane sesje połączeniowe w obrębie systemu zarządzania;
- szyfrowane sesje zdalnego dostępu;
- kryptograficzne sumy kontrolne plików systemowych (ochrona integralności tych plików);
- prawidłową konfigurację usług sieciowych.

Wśród mechanizmów zabezpieczenia komputerów można wymienić:

- blokady różnych elementów komputera (wyświetlacza, klawiatury, stacji dyskietkowych);
- hasła blokady dostępu do plików konfiguracyjnych;
- szyfrowanie plików, katalogów i partycji dyskowych;
- kontrolę antywirusową plików.

Dla komputerów przenośnych istnieją dodatkowe mechanizmy zabezpieczenia, np.:

- formatowanie twardego dysku i reinstalacja oprogramowania przy każdorazowej zmianie użytkownika;
- fizyczna ochrona przed kradzieżą.

4.4.2.2. Bezpieczeństwo komunikacji

Typowe mechanizmy zabezpieczenia komunikacji to:

- odpowiednia konfiguracja dostępu modemowego (np. uaktywnienie po stronie systemu funkcji *callback*);
- serwer dostępu, umożliwiający zdalne dołączenie urządzeń, zapewniający m.in.: uwierzytelnienie użytkowników, automatyczne wywołanie zwrotne oraz pełną rozliczalność prób dostępu;

- zapory ogniowe - serwer usytuowany na styku sieci prywatnej oraz publicznej, umożliwiający kontrolę ruchu do i z sieci prywatnej, zabezpieczenie usług sieci publicznej oraz rozliczalność użytkowników tych usług;
- tworzenie prywatnych sieci rozległych (tzw. ekstranetów);
- wirtualne sieci prywatne, umożliwiające tworzenie prywatnych połączeń za pośrednictwem sieci publicznych (np. Internetu); jest to rozwiązanie konkurencyjne dla fizycznych sieci prywatnych.

4.5. Identyfikacja i uwierzytelnienie

W tradycyjnym ujęciu nie rozpatrywano oddzielnie zagadnień związanych z identyfikacją i uwierzytelnieniem, ale traktowano jako element procesu logicznej kontroli dostępu. W podstawowym procesie kontroli dostępu można bowiem wyodrębnić trzy fazy: zidentyfikowania, uwierzytelnienia i autoryzacji użytkownika.

Identyfikacja jest procesem, dzięki któremu użytkownik systemu może przedstawić swą tożsamość. Uwierzytelnienie jest procesem weryfikacji przedstawionej tożsamości. Autoryzacja oznacza udzielenie pozwolenia na użycie określonych zasobów systemu informacyjnego. Takie pozwolenie jest wystawiane, bezpośrednio lub pośrednio, przez system operacyjny, aplikację programową lub gestora informacji.

Za pomocą mechanizmów kontroli dostępu jest zatem realizowane jedno z podstawowych kryteriów bezpieczeństwa: zapewnienie autentyczności użytkowników. Niemniej jednak identyfikacja i uwierzytelnienie ma zasadnicze znaczenie także dla realizacji innego kryterium: rozliczalności.

Celem zdefiniowania obszaru bezpieczeństwa jest zapewnienie autentyczności użytkowników systemu oraz rozliczalności wszystkich działań i zdarzeń zachodzących w systemie.

Z punktu widzenia bezpieczeństwa systemów informatycznych najistotniejszy jest podział na słabe i mocne uwierzytelnienie. W słabych

mechanizmach uwierzytelnienia użytkownik jest identyfikowany i uwierzytelniany na podstawie wiedzy, którą posiada. Mocne mechanizmy uwierzytelnienia opierają się na **dowodzie wiedzy** realizowanym na podstawie przekształceń kryptograficznych. Najnowszą, dynamicznie rozwijającą się dziedziną mechanizmów identyfikacji i uwierzytelniania, jest dowód tożsamości osoby oparty na specyficznych, niepowtarzalnych parametrach biometrycznych.

4.5.1. Mechanizmy identyfikacji i uwierzytelnienia użytkownika

Wybór mechanizmu identyfikacji i uwierzytelnienia zależy od typu systemu informatycznego oraz potrzeb i możliwości w zakresie bezpieczeństwa tego systemu.

4.5.1.1. Mechanizmy oparte na wiedzy

Do tej kategorii mechanizmów należą najbardziej rozpowszechnione w systemach informatycznych:
- mechanizm identyfikacji i uwierzytelnienia oparty na jednoznacznym identyfikatorze oraz tajnym haśle;
- mechanizm identyfikacji i uwierzytelniania oparty na kartach z pamięcią (z odczytem lub odczytem/zapisem, lecz bez możliwości przetwarzania informacji).

4.5.1.2. Mechanizmy oparte na dowodzie wiedzy

Zastosowanie przekształcenia kryptograficznego (np. algorytmów klucza publicznego) umożliwiło wprowadzenie dowodu wiedzy do procesu identyfikacji i uwierzytelnienia, co wydatnie zwiększyło poziom zabezpieczenia systemów informacyjnych. Przekształcenie kryptograficzne jest realizowane za pomocą kart inteligentnych, które stanowią następny etap rozwoju technologicznego kart z pamięcią.

Dowód wiedzy może być zrealizowany na podstawie:
- synchronizowanych generatorów haseł - urządzenie uwierzytelniające jest zsynchronizowane z serwerem, dzięki czemu może w danym (krótkim) momencie czasowym obliczyć poprawne hasło; po upływie ustalonego czasu, zgodnie z realizowanym algorytmem kryptograficznym, hasło ma już nową, inną wartość;
- mechanizmu „wyzwanie - odpowiedź" - serwer wysyła do użytkownika wyzwanie, które jest wpisywane na kartę; wyzwanie jest szyfrowane kluczem przechowywanym na karcie, a następnie odsyłane do serwera; jeśli otrzymana odpowiedź jest identyczna z wynikiem obliczeń przeprowadzonych przez serwer, użytkownik jest uwierzytelniony.

4.5.1.3. Mechanizm identyfikacji i uwierzytelnienia oparty na parametrach biometrycznych

W przypadku stosowania mechanizmów identyfikacji opartych na parametrach biometrycznych (np. odcisk palca, wzór siatkówki oka, itp.) należy zapewnić, że urządzenia identyfikujące spełniają międzynarodowe standardy opracowane dla urządzeń tego typu w zakresie parametrów technicznych takich, jak współczynniki: błędu identyfikacji (brak identyfikacji osoby upoważnionej) oraz błędu akceptacji (identyfikacja i uwierzytelnienie osoby nieupoważnionej), a także zabezpieczenia przed uszkodzeniem.

4.5.1.4. Serwer uwierzytelnienia

Zarządzanie identyfikacją i uwierzytelnieniem w systemie informacyjnym może być realizowane za pośrednictwem wydzielonego serwera. Zastosowanie serwera uwierzytelnienia może uprościć definiowanie reguł dostępu do aktywów systemu oraz prowadzenie rejestrów, umożliwiających indywidualne rozliczenie użytkowników.

4.5.2. Organizacyjny aspekt bezpieczeństwa identyfikacji i uwierzytelniania

Należy określić reguły zarządzania elementami uwierzytelniania. W przypadku mechanizmów opartych na wiedzy:

- odpowiednie zarządzanie hasłami i/lub PIN-ami oraz zabezpieczanie (np. za pomocą szyfrowania) plików, w których ta informacja jest przechowywana, a także właściwe zarządzanie obejmuje prawidłowe generowanie, wymianę i unieważnianie haseł;
- powinny istnieć procedury wydawania, rejestrowania, blokady, wymiany i niszczenia kart z pamięcią.

Stosując mechanizm uwierzytelnienia oparty na dowodzie wiedzy należy określić reguły, jak w przypadku kart z pamięcią, z uwzględnieniem wymagania na zarządzanie kluczami kryptograficznymi (patrz 4.8.2.2).

Należy zauważyć, że nie ma potrzeby definiować procedur organizacyjnych w przypadku mechanizmów identyfikacji i uwierzytelnienia opartych na parametrach biometrycznych.

4.6. Logiczna kontrola dostępu do systemu

Wymagania użytkowania aktywów systemu informatycznego, w tym dostęp do informacji, mogą zmieniać się w zależności od wielu czynników, takich jak: typ systemu, rodzaj instytucji, charakter prowadzonej działalności. Proces kontroli dostępu składa się z następujących elementów:

- identyfikacji i uwierzytelnienia (omówienie w poprzednim punkcie);
- fizycznej kontroli dostępu do aktywów systemu informatycznego (patrz 4.2.2.3);
- logicznej kontroli dostępu do aktywów systemu informatycznego, w tym:

- zarządzania przywilejami dla aplikacji programowych,
- monitorowania dostępu.

Celem zdefiniowania obszaru zabezpieczenia jest ochrona przed nieuprawnionym dostępem do systemu informatycznego i jego aktywów, zapewnienie poufności informacji oraz jednoznacznego przyporządkowania działań realizowanych w wyniku uzyskania dostępu.

4.6.1. Organizacyjny aspekt kontroli dostępu

Należy zdefiniować następujące zasady:

- udzielania, rejestrowania i odwoływania pozwolenia dostępu (autoryzacji) do pomieszczeń;
- udzielania, rejestrowania i odwoływania pozwolenia na dostęp (autoryzacji) do systemu/ sieci (zgodnie z zasadą separacji funkcji);
- kontroli dostępu do komputerów i stacji roboczych;
- kontroli dostępu do aplikacji i ich danych, ze szczególnym uwzględnieniem:
  - zasady separacji funkcji i odpowiedzialności (np. administratorom aplikacji, administratorom baz danych), zgodnie z zasadą separacji obowiązków i odpowiedzialności);
  - rozliczalności użytkowników, niezależnie od użytej metody definiowania praw dostępu (np. na podstawie grup lub profili);
  - zasady minimum przywilejów;
  - dodatkowych warunków ograniczenia praw dostępu (np. poza wyznaczonymi godzinami, tylko dla określonego zadania, przy przekroczeniu wartości progowych, typu usługi);
- monitorowania dostępu do systemu i użytkowania aktywów (rejestry dostępu).

4.6.2. Mechanizmy logicznej kontroli dostępu

W systemach informatycznych stosuje się następujące mechanizmy:

- listę kontroli dostępu (przyporządkowanie praw dostępu użytkownikom lub grupom użytkowników identyfikowanych przez nazwy);
- schemat posiadanych uprawnień (zbiór operacji dozwolonych użytkownikowi (lub grupie użytkowników na wskazanych aktywach);
- mechanizm oparty na etykietach (wykorzystanie etykiet "wrażliwości" przypisanych użytkownikom, obiektom (aktywom) i przenoszonym danym; zezwolenie na dostęp następuje po porównaniu etykiet);
- kontrola dostępu oparta na informacji kontekstowej; informacjami kontekstowymi mogą być:
  - przedział czasowy;
  - trasa (np. dostęp tylko wtedy, gdy użyta droga ma ściśle określoną charakterystykę);
  - miejsce (np. dostęp tylko z określonych systemów lub stacji roboczych);
  - stan systemu (np. zezwolenie udzielane tylko w nadzwyczajnych sytuacjach;
  - zezwolenie na dostęp (dany użytkownik uzyskuje dostęp tylko w przypadku, gdy takie zezwolenie już otrzymał inny, określony użytkownik).

4.7. Audyt systemu zabezpieczenia

Pojęcie audytu jest definiowane w literaturze (i stosowane w praktyce) w dwojaki sposób. Zgodnie z pierwszą definicją, "audyt" oznacza przegląd rejestrów (sekwencji rekordów), zawierających informacje o zdarzeniach w systemie operacyjnym, aplikacjach programowych oraz działaniach użytkowników. Rejestry te zapewniają systemowi **rozliczalność.** Obszar bezpieczeństwa dotyczy audytu w rozumieniu tej definicji. Należy podkreślić, że audyt rejestrów systemowych to także podstawowe źródło informacji przy wykrywaniu incydentów i rekonstrukcji zdarzeń (patrz 4.10.2).

Zgodnie z drugą definicją, "audyt" jest pojęciem szerszym i obejmuje: przegląd dokumentacji oraz analizę mechanizmów zabezpieczeń w obszarze zarządzania, eksploatacji i techniki. „Audyt" jest wtedy elementem procesu szacowania poziomu bezpieczeństwa systemu informatycznego wymaganego przy akredytacji polityki bezpieczeństwa.

4.7.1. Mechanizmy zabezpieczenia audytu

W systemie informatycznym powinny być prowadzone rejestry zdarzeń: poziomu systemowego, aplikacji i użytkowników. W niektórych systemach mogą być wdrożone mechanizmy, zapewniające monitorowanie znaków wprowadzanych z klawiatury.

Rejestr powinien zawierać informację wystarczającą do określenia, jakiego rodzaju zdarzenie wystąpiło, kto i kiedy je spowodował.

Rejestry zdarzeń systemowych są zwykle wykorzystywane do monitorowania oraz korygowania parametrów jakościowych systemu operacyjnego.

Rejestry zdarzeń z poziomu aplikacji programowych umożliwiają zapis działań użytkowników w aplikacji, w szczególności dotyczących żądania zawarcia transakcji (rekord zawierający identyfikację stron transakcji, typ żądanej transakcji, informację o zakończeniu przerwania transakcji i ewentualnej przyczynie przerwania).

Rejestr działań użytkowników powinien rejestrować wszystkie polecenia inicjowane bezpośrednio przez użytkownika, wszystkie próby uwierzytelnienia oraz dostęp do aktywów systemu.

4.7.2. Organizacyjny aspekt audytu systemu zabezpieczenia

Powinny zostać zdefiniowane zasady zarządzania informacją na potrzeby audytu systemu zabezpieczenia, w tym:

- rodzaj zbieranych danych w poszczególnych rejestrach zdarzeń;
- zasady utrzymywania i ochrony rejestrów zdarzeń:

- metody zabezpieczenia plików rejestrów zdarzeń (ochrona integralności i poufności);
- przyczyny przeprowadzania audytu (np. w wyniku wykrycia naruszenia, zgodnie z ustalonym harmonogramem, jako element analizy statystycznej);
- procedury archiwizacji.

4.8. Bezpieczeństwo systemów operacyjnych i aplikacji programowych

Celem zdefiniowania obszaru zabezpieczenia jest:
- pewność, że aspekt zabezpieczenia został uwzględniony na etapie tworzenia lub modyfikacji systemów operacyjnych i aplikacji programowych;
- przeciwdziałanie utracie, modyfikacji lub niewłaściwemu wykorzystaniu danych przetwarzanych za pomocą aplikacji programowych na platformach systemów operacyjnych.

4.8.1. Ogólne wymagania w zakresie zabezpieczenia systemów operacyjnych i aplikacji programowych

Analiza wymagań zabezpieczenia powinna być przeprowadzona na etapie tworzenia wymagań w fazie projektowania produktu (systemu operacyjnego lub aplikacji programowej). Mechanizmy zabezpieczeń są wtedy tańsze i bardziej efektywne. Ogólne wymagania powinny zawierać analizę takich kwestii (część z nich była już przedmiotem rozważań), jak:
- kontrola dostępu do informacji i usług, w tym zasada separacji usług oraz obowiązków;
- weryfikacja i ochrona integralności istotnych danych na wszystkich lub wybranych etapach przetwarzania;
- ochrona poufności danych;
- wyjście ze stanu uszkodzenia, w szczególności możliwość zdefiniowania i wdrożenia procedur alternatywnego przetwarzania;

- tworzenie kopii bezpieczeństwa istotnych danych;
- rejestrowanie istotnych zdarzeń do celów monitorowania zabezpieczeń lub w przypadku działań związanych z naruszeniem zabezpieczenia;
- zgodność z regulacjami wewnętrznymi, prawnymi i wynikającymi z umów;
- skonstruowanie interfejsu użytkownika w sposób, umożliwiający bezpieczne korzystanie z produktu przez przeszkolonego użytkownika.

Wszystkie wbudowane w produkcie zabezpieczenia powinny być właściwie udokumentowane.

Zabezpieczenie niektórych elementów danego systemu informacyjnego może wymagać niezależnej oceny i certyfikacji produktów systemu informacyjnego. Taka ocena oraz certyfikat (atest) może być wydana na podstawie, np. szczegółowych wymagań zawartych w [8].

4.8.2. Ochrona poufności, integralności i autentyczności informacji realizowana za pomocą metod kryptograficznych

Poziom ochrony za pomocą algorytmów kryptograficznych zależy od dwóch czynników: o charakterze technicznym (jakość algorytmu) oraz organizacyjnym (procesy zarządzania kluczami kryptograficznymi).

4.8.2.1. Kryptograficzne mechanizmy zabezpieczeń

Wyboru algorytmów kryptograficznych stosowanych w aplikacjach programowych należy dokonać na podstawie właściwych norm, krajowych i międzynarodowych [13].

Metody kryptograficzne mogą być oparte na symetrycznym przekształceniu kryptograficznym (integralność informacji jest chroniona za pomocą kodu uwierzytelnienia wiadomości MAC - (*Message Authentication Code*), a jej poufność za pomocą tajnego klucza sto-

sowanego w przekształceniu szyfrowania i deszyfrowania) albo na przekształceniu asymetrycznym - integralność gwarantuje podpis cyfrowy, a poufność jest osiągana za pomocą klucza sesyjnego, uzgodnionego w protokole opartym na przekształceniach kryptografii asymetrycznej.

4.8.2.2. Organizacyjny aspekt mechanizmów kryptograficznych

Należy określić zasady zarządzania kluczami kryptograficznymi, w szczególności:

- zasady generowania kluczy kryptograficznych (z ustaleniem wymagań na parametry jakościowe generatorów liczb pseudolosowych);
- zasady bezpiecznej dystrybucji kluczy kryptograficznych;
- metody bezpiecznego przechowywania tajnych, prywatnych i publicznych kluczy kryptograficznych;
- zasady wymiany i unieważniania kluczy kryptograficznych;
- zasady archiwizowania kluczy kryptograficznych (z uwzględnieniem problemu odtwarzania tajnych kluczy - *key recovery*).

4.8.3. Bezpieczeństwo baz danych

Wymagania bezpieczeństwa baz danych oraz programów zarządzania powinny uwzględniać wiele dodatkowych elementów, wynikających ze specyfiki tych struktur informacyjnych, które narzucają stosowanie rozszerzonych mechanizmów zabezpieczeń. Aspekty organizacyjne bezpieczeństwa w przypadku baz danych są analogiczne jak dla innych aplikacji programowych.

4.8.3.1. Mechanizmy zabezpieczenia baz danych

Mechanizmy zabezpieczeń można pogrupować w następujące kategorie.

- **Integralność i niezawodność bazy danych**

Na integralność i niezawodność bazy danych składa się:
- integralność (fizyczna i logiczna) struktury bazy danych (zabezpieczenie przed skutkami błędów i awarii, np. zniszczeniem głównych plików indeksujących);
- regularne archiwizowanie zawartości bazy danych;
- implementacja dwufazowej modyfikacji elementów bazy danych;
- wprowadzenie nadmiarowości i weryfikacja spójności bazy danych (np. przy użyciu kodów detekcji i korekcji błędów lub pól dublujących);
- wprowadzenie do programów zarządzania bazą danych jednostek odpowiedzialnych za integralność struktury (tzw. monitorów).

- **Integralność elementu bazy danych**

Pojęcie integralności elementu bazy danych oznacza jego prawidłowość i dokładność. Za integralność elementową jest odpowiedzialny program zarządzający bazą danych. Powinien on zapewniać weryfikację integralności w następujących sposób:
- sprawdzać poprawność wprowadzanych danych;
- stosować mechanizmy kontroli dostępu (patrz omówienie kontroli dostępu w bazach danych);
- utrzymywać rejestr wprowadzanych zmian, zawierający zestawienie starej wartości pola i zmodyfikowanej tak, aby można było skorygować błędnie wprowadzoną wartość.

- **Ochrona informacji w bazie danych**

W szczególności powinny być stosowane mechanizmy zabezpieczające przed ujawnieniem poufnych danych w wyniku wnioskowania na podstawie odpowiedzi na poprawnie skonstruowane pytanie o parametry jawne.

Do zapewnienia poufności danych powinny być stosowane także inne mechanizmy zabezpieczenia w postaci: podziału bazy na niezależne od siebie części, szyfrowania wybranych pól lub rekordów, etykiet poufności i kryptograficznych sum kontrolnych (zapewniających ponadto integralność danych), monitora odniesienia *(trusted front-end)* oraz mechanizmów kontroli dostępu.

- **Kontrola dostępu do bazy danych, w tym identyfikacja i uwierzytelnienie**

Jeśli nie został wdrożony mechanizm jednokrotnego uwierzytelnienia *(single sign-on)*, to program zarządzający bazą danych powinien zawierać własny, niezależny od systemu operacyjnego mechanizm identyfikacji i uwierzytelnienia. Procedura identyfikacji i uwierzytelnienia umożliwia poprawne przydzielenie praw dostępu do bazy (autoryzację), przy stosowaniu zasady separacji funkcji i minimum przywilejów, dostępności danych (np. blokada dostępu w momencie aktualizacji elementu bazy), weryfikacji tożsamości.

- **Rozliczalność dostępu do bazy danych**

Program zarządzający bazą danych powinien umożliwiać tworzenie rejestrów, zawierających każdą próbę dostępu oraz zapis zrealizowanych działań tak, aby istniała możliwość odtworzenia zaktualizowanych elementów bazy jednoznacznego przypisania poszczególnych działań zidentyfikowanym użytkownikom.

4.8.4. Inne mechanizmy zabezpieczeń systemów operacyjnych i aplikacji programowych

Do środków bezpieczeństwa należy zaliczyć:

- mechanizmy zapewniające poprawność wewnętrznego przetwarzania (np. bilanse plików przed i po modyfikacji, sumy kontrolne);
- mechanizmy, zapewniające integralność i zgodność kodów źródłowych, kodów wykonawczych i bibliotek.

4.8.5. Inne aspekty organizacyjne bezpieczeństwa systemów operacyjnych i aplikacji

Należy opracować zasady:
- rejestrowania wszystkich zmian w bibliotekach oprogramowania operacyjnego;
- wprowadzania do aplikacji danych testowych i ich relacji do danych rzeczywistych;
- zarządzania zmianami w aplikacjach programowych (uzgadniania zmian, dokumentowania, analizy wpływu zmian, archiwizowania poprzednich wersji);
- stałego nadzorowania informacji o wykrywanych słabościach i błędach w systemach operacyjnych i aplikacjach programowych oraz instalowania korekt lub nowych wersji dostarczanych przez producenta.

4.9. Utrzymanie ciągłości działania

Dwa kolejne obszary bezpieczeństwa odnoszą się do problemu funkcjonowania systemu informatycznego w nadzwyczajnych sytuacjach: rozległej awarii lub katastrofy (utrzymanie ciągłości działania) oraz poważnego naruszenia bezpieczeństwa. Podstawą rozróżnienia tych dwóch obszarów jest natura zdarzeń powodujących powstanie nadzwyczajnych warunków działania. W pierwszym przypadku przyczyny zdarzeń mają charakter przypadkowy i przeważnie pozbawiony udziału ludzkiego, w drugim - przyczyną incydentu jest działanie człowieka (najczęściej rozmyślne, rzadko przypadkowe). Z tego względu cele działania w obu obszarach są odmienne. Należy zaznaczyć, że w pewnym zakresie oba obszary mogą wymagać dość podobnych mechanizmów zabezpieczeń. Na przykład w przypadku reakcji na naruszenie zabezpieczenia, jak i wyjścia ze stanu awarii lub katastrofy procedury odtworzeniowe opierają się prawidłowej polityce tworzenia kopii bezpieczeństwa (zapasowych).

Celem zdefiniowania obszaru zabezpieczenia jest opracowanie i wdrożenie planu utrzymania dostępności podstawowych funkcji instytucji oraz minimalizowania strat związanych z przerwą w pracy systemu informatycznego, spowodowaną zaistnieniem sytuacji awaryjnych i katastrofalnych.

Z punktu widzenia bezpieczeństwa systemu informatycznego kluczowe znaczenie ma sposób organizacji planu utrzymania ciągłości działania.

4.9.1. Organizacja utrzymania ciągłości działania

4.9.1.1. Kryteria określania sytuacji awaryjnych i katastrofalnych

Nie każde częściowe lub całkowite uszkodzenie systemu informatycznego wymaga uaktywnienia planów utrzymania ciągłości działania. Często uszkodzenia systemu można usunąć w krótkim czasie, zgodnie z rutynowymi procedurami (patrz 4.4.1.5). Sytuacja awaryjna lub katastrofalna pojawia się wtedy, gdy przywrócenie normalnego stanu pracy systemu informacyjnego w wymaganym czasie nie jest możliwe.

4.9.1.2. Podział obowiązków i odpowiedzialności

W trakcie realizacji planu utrzymania ciągłości działania systemu informatycznego powinna istnieć specjalna struktura organizacyjna. Obejmuje ona osoby odpowiedzialne za inicjowanie, kierowanie i koordynowanie działań ekip ratowniczych oraz wykonanie poszczególnych elementów planu na każdym szczeblu. W sytuacjach określonych planami utrzymania może być wymagane udzielenie uprzywilejowanego dostępu do aktywów systemu.

4.9.1.3. Zasady planowania utrzymania ciągłości działania

Proces planowania utrzymania ciągłości działania powinien uwzględniać następujące elementy:

a) identyfikację i klasyfikację najważniejszych funkcji instytucji realizowanych za pomocą systemu informacyjnego;
b) identyfikację aktywów systemu informatycznego, które realizują funkcje określone w punkcie a); aktywa te można klasyfikować w następujących kategoriach: zasobów ludzkich, zdolności przetwarzania, aplikacji i danych, serwisów technicznych, infrastruktury fizycznej; dokumentacji;
c) wybór strategii utrzymania ciągłości działania w zakresie: doboru zespołów ludzkich, utrzymania zdolności przetwarzania (konfiguracja ośrodków zapasowych), utrzymania ciągłości aplikacji i danych (kopie bezpieczeństwa) oraz wykorzystania serwisu technicznego (alternatywne łącza, przekierowania itp.);
d) opracowanie odpowiednich procedur dla poszczególnych faz planu utrzymania ciągłości działania, tzn. reakcji na wystąpienie zdarzenia, przejścia do alternatywnego przetwarzania, odtworzenia stanu systemu informacyjnego sprzed zdarzenia.

4.9.1.4. Warunki wdrożenia planów utrzymania ciągłości działania systemu informatycznego

Wdrożenie planu utrzymania ciągłości działania powinno być poprzedzone pracami przygotowawczymi takimi, jak:
- opracowanie i wdrożenie procedur tworzenia kopii bezpieczeństwa systemów, danych oraz aplikacji programowych;
- zawarcie lub renegocjacja kontraktów zawartych z dostawcami sprzętu i usług, uwzględniających potrzeby utrzymania ciągłości działania systemu informacyjnego;
- utworzenie rezerwowych systemów i/lub zarezerwowanie budynków na potrzeby alternatywnego przetwarzania lub przechowywania kopii bezpieczeństwa.

Pracom wdrożeniowym powinny towarzyszyć prace dokumentacyjne oraz szkolenia.

Przeszkolenia w zakresie obowiązków związanych z utrzymaniem ciągłości działania powinny być częścią ogólnego szkolenia użytkowników systemu informatycznego i obejmować, poza działaniami uświadamiajacymi oraz szkoleniem teoretycznym, także ćwiczenia praktyczne, łącznie z symulacją zdarzeń.

4.9.1.5. Zasady testowania i modyfikacji planów utrzymania ciągłości działania

Regularnie powinny być przeprowadzane testy gotowości planów utrzymania ciągłości działania.

Modyfikacji planów utrzymania ciągłości działania należy dokonać w przypadku:

- istnienia niedociągnięć stwierdzonych w trakcie przeglądów lub testów gotowości;
- wprowadzenia zmian w systemie informatycznym.

Należy zaznaczyć, że koszty opracowania i wdrożenia planów ciągłości działania mogą być znaczące, zwłaszcza gdy wynika z nich konieczność organizowania ośrodków alternatywnego przetwarzania. Decyzja, jaką przyjąć strategię utrzymania ciągłości działania, powinna być efektem starannej analizy potrzeb i możliwości danej instytucji.

4.10. Działanie w przypadku wykrycia naruszenia bezpieczeństwa systemu informacyjnego

Naruszenie bezpieczeństwa jest szczególnym rodzajem nadzwyczajnej sytuacji, w której może znaleźć się system informatyczny. Jak wspomniano wcześniej, naruszenie bezpieczeństwa ma charakter działania rozmyślnego (aczkolwiek do tej kategorii są zaliczane także poważne błędy użytkowników), często określanego mianem ataku. Jest to przypadek, w którym na rozmiar szkód decydujący wpływ ma

dostatecznie szybka reakcja zarówno o charakterze organizacyjnym, jak i technicznym. Dlatego należy wydzielić niezależny obszar bezpieczeństwa, a następnie zdefiniować i wdrożyć plan zabezpieczenia (procedury organizacyjne i mechanizmy).

Celem zdefiniowania obszaru zabezpieczenia jest zminimalizowanie negatywnych skutków niepożądanych zdarzeń w systemie informatycznym będących następstwem rozmyślnych działań na szkodę tego systemu.

4.10.1. Organizacja działań w przypadku wykrycia naruszenia bezpieczeństwa

Plan postępowania w przypadku wykrycia poważnego naruszenia bezpieczeństwa systemu informatycznego powinien obejmować takie zagadnienia, jak:

a) przygotowanie do podjęcia potencjalnych działań jako reakcji na wykrycie naruszenia - w tym:
   - rozpoznanie prawnego aspektu naruszeń bezpieczeństwa;
   - zdefiniowanie założeń - określenie początkowego poziomu bezpieczeństwa (np. na podstawie wymagań opisanych w tym artykule), typów potencjalnych zdarzeń, sposobu reakcji na naruszenie;
   - ustalenie priorytetów ochrony aktywów (w kolejności malejącej ważności, np. od ochrony życia ludzkiego, do minimalizowania przerw w funkcjonowaniu systemu);
b) identyfikacja naruszenia, w tym:
   - wykrycie naruszenia (pojawienie się jednego lub kilku symptomów z listy anormalnych zdarzeń);
   - określenie typu i zakresu naruszenia (np. liczba komputerów dotkniętych następstwami zdarzenia, identyfikacja punktu, gdzie nastąpiło naruszenie, szacowanie potencjalnych szkód);
c) reakcja na wykrycie naruszenia, w tym:

- powiadamianie i/lub uzyskanie pomocy od specjalistycznego zespołu reagowania na naruszenia bezpieczeństwa (CERT);
- zabezpieczanie dowodów i dokumentowanie przeprowadzonych działań;
- powstrzymanie rozszerzania się naruszenia (np. całkowite unieruchomienie systemu, blokada niektórych funkcji, monitorowanie działań użytkowników); podstawą podjętych działań powinna być analiza ryzyka, w której zostały rozpatrzone różnorakie aspekty (finansowe, organizacyjne i ludzkie) zakłócenia funkcjonowania systemu (np. koszty przerwy w działalności, konsekwencje ujawnienia informacji podlegających ochronie, uciążliwości związane z anormalnym funkcjonowaniem systemu);
- likwidacja źródła naruszenia;
- odtworzenie stanu normalnej pracy systemu (z oryginalnych źródeł oprogramowania oraz kopii bezpieczeństwa);

d) analiza wpływu naruszenia na stan bezpieczeństwa systemu (tzw. analiza "post mortem"), zawierająca informacje:
   - co i kiedy się stało;
   - opis działań (zastosowana metoda wykrycia naruszenia, procedura naprawcza, procedura monitorowania);
   - oszacowanie wyrządzonych szkód (zawierające koszty związane z utratą oprogramowania i plików z danymi, uszkodzeniem sprzętu oraz koszty przywrócenia normalnej pracy systemu);
   - ocena działania własnego personelu i/lub zewnętrznych zespołów technicznego wsparcia;
   - postulowane zmiany w zabezpieczeniu, zmniejszające ryzyko wystąpienia podobnego naruszenia w przyszłości;
e) administracyjne środki podjęte jako reakcja na naruszenie, jeśli istnieją przesłanki, umożliwiające ukaranie sprawcy incydentu.

4.10.2. Techniczne środki bezpieczeństwa

W działaniach związanych z naruszeniem bezpieczeństwa systemu informatycznego są stosowane następujące mechanizmy:
- oprogramowanie antywirusowe oraz programy sprawdzające integralność plików;
- automatyzowane narzędzia wykrywania naruszeń (*intrusion detection)*: systemy eksperckie porównujące wzory i profile zachowań systemu, monitory (analiza pasywna), skanery (z elementami analizy aktywnej, np. zgodności z polityką bezpieczeństwa);
- sprzętowo-programowe systemu kontroli zewnętrznych połączeń do i z systemu (tzw. "zapory ogniowe" - patrz także 4.4.2.2).

4.11. Akredytacja zabezpieczenia systemu informacyjnego

Akredytacja oznacza formalne stwierdzenie uzyskania odpowiedniego poziomu bezpieczeństwa systemu informacyjnego. Zgodność przyjętych mechanizmów zabezpieczeń oraz rozwiązań organizacyjnych z wymaganiami, które zostały określone w polityce bezpieczeństwa, powinna być przedmiotem niezależnej oceny przeprowadzonej przez zewnętrzną instytucję. Należy jednakże podkreślić, że zorganizowany system akredytacji istnieje tylko w jednym kraju (Wielka Brytania). Instytucje mogą otrzymać tam certyfikat zgodności swej polityki bezpieczeństwa z wymaganiami w zakresie zarządzania bezpieczeństwem informacji zdefiniowanymi w normie [3]. Niezależnie od tego, że istnieje potrzeba utworzenia takich instytucji akredytujących także i w Polsce, to uzyskanie pewności, że wprowadzona polityka zabezpieczenia spełnia wymagania, może być również przedmiotem oceny wewnętrznej, jako warunek przyjęcia proponowanych rozwiązań przez czynniki decyzyjne samej instytucji.
Celem zdefiniowania obszaru bezpieczeństwa jest uzyskanie odpowiedniego stopnia pewności, że przyjęte rozwiązania są zgodne z postawionymi wymaganiami bezpieczeństwa w zakresie prawnym, organizacyjnym i technicznym.

4.11.1. Prawny aspekt bezpieczeństwa systemów informatycznych

Należy zapewnić zgodność wprowadzonych zabezpieczeń z obowiązującymi w państwie uregulowaniami prawnymi. Dokument polityki bezpieczeństwa systemu informacyjnego powinien przejść weryfikację prawną w zakresie:

- ochrony informacji;
- prawa karnego (obowiązuje od 1 września 1998 r[2]) kodeksu cywilnego, ustawy o ochronie osób i mienia[3], w przypadku wszczęcia postępowania wobec sprawcy naruszenia bezpieczeństwa systemu informatycznego (patrz 4.10.1);
- prawa autorskiego i prawa o wynalazczości, w szczególności w przypadku korzystania oraz udzielania licencji na oprogramowanie nabywane lub będące własnością danej instytucji;
- wewnętrznych uregulowań, np. regulaminu pracy, instrukcji przeciwpożarowych, planów awaryjnych w przypadku klęsk żywiołowych lub awarii technicznych itp.

Warto podkreślić, że informacja podlega ochronie, ponieważ może mieć dla instytucji wymierną wartość. Taka informacja jest wtedy tajemnicą przedsiębiorstwa[4]. W niektórych systemach informacyjnych może mieć zastosowanie wiele innych aktów prawnych traktujących o ochronie informacji (np. prawo bankowe).

Na odrębne omówienie zasługują systemy, w których może pojawić się informacja podlegająca ochronie z tytułu ustaw szczególnych. Do nich należy zaliczyć: ustawę o ochronie informacji niejawnych[5] oraz o ochronie danych osobowych[6]. Ich szczególność, z punktu

---

[2] Dz.U. 1997, nr 88, poz. 553.

[3] Dz.U. 1997, nr 114, poz. 740.

[4] Dz.U. 1993, nr 47, poz. 221.

[5] Dz.U. 1999, nr 11, poz. 95.

[6] Dz.U. 1997, nr 133, poz. 883.

widzenia bezpieczeństwa, polega na tym, że w rozporządzeniach im towarzyszących zawarto szczegółowe wymagania bezpieczeństwa systemów i sieci teleinformatycznych. Należy zaznaczyć, że obszary bezpieczeństwa zdefiniowane w tym artykule pokrywają całkowicie wymagania bezpieczeństwa stawiane zarówno w ustawie o ochronie informacji niejawnych (dla informacji będącej tajemnicą służbową), jak i w ustawie o ochronie danych osobowych.

4.11.2. Organizacyjny aspekt akredytacji bezpieczeństwa systemu informatycznego

Osoba przeprowadzająca akredytację powinna podejmować końcową decyzję o adekwatności osiągniętego poziomu bezpieczeństwa w stosunku do wymagań opartych na znanych metodach uzyskiwania pewności takich, jak: szacowanie ryzyka, testowanie zabezpieczeń oraz akceptacja ryzyka szczątkowego. Akredytacja powinna uwzględniać poszczególne fazy rozwoju systemu informacyjnego, tzn. planowanie i wdrożenie oraz eksploatację. Wszystkie fazy akredytacji powinny być prawidłowo udokumentowane.

4.11.3. Techniczne środki stosowane w procesie akredytacji na etapie planowania i wdrożenia systemu informatycznego

Akredytowanie systemu informatycznego na tym etapie oznacza potwierdzenie, że funkcje bezpieczeństwa zostały w prawidłowy sposób zintegrowane z funkcjami systemu, aplikacji lub elementu na etapie ich projektowania oraz wdrożenia (patrz część cyklu dotycząca rozwoju systemu i oprogramowania). Pewność taka powinna być uzyskana w rezultacie stosowania niżej podanych działań.

- **Testowanie parametrów technicznych**

Testowanie parametrów technicznych wykonuje się, np. za pomocą testów funkcjonalnych (sprawdzenie, czy dana funkcja działa zgodnie

z wymaganiami) lub testów penetracyjnych (sprawdzenie, czy mechanizmy zabezpieczenia nie mają obejścia).

- **Stosowanie certyfikowanych produktów informatycznych**

W przypadku niektórych systemów informatycznych należy stosować produkty informacyjne, których poziom bezpieczeństwa został określony za pomocą niezależnych kryteriów szacowania. Takie kryteria są zdefiniowane, np. w projekcie normy [8][7]. Podwyższony poziom zabezpieczenia produktów informacyjnych jest definiowany w klasach bezpieczeństwa opartych na formalnym modelowaniu, matematycznym dowodzie bezpieczeństwa oraz zaufanej architekturze systemowej (np. zaufana baza komputerowa lub monitor odniesienia).

- **Stosowanie niezawodnej architektury systemu**

W przypadku niektórych systemów o podwyższonych wymaganiach niezawodnościowych powinny być stosowane dodatkowe elementy, takie jak: systemy z odpornością na błędy, nadmiarowość architektury (dublowanie krytycznych elementów sprzętowych i programowych) i/lub specjalnie zaprojektowane elementy, np. jak matryce macierzowe.

- **Stosowanie koncepcji "niezawodnego bezpieczeństwa"**

Przez pojęcie stosowania koncepcji "niezawodnego bezpieczeństwa" rozumie się wdrażanie tylko takich produktów, dla których uzyskanie zadanego poziomu bezpieczeństwa jest łatwe (parametry ustawienia początkowego i/lub parametry domyślne są określone jako "najbardziej bezpieczne") oraz takich, o których wiadomo, że są dobrze przetestowane, cieszą się renomą wśród użytkowników i mają ugruntowaną pozycję na rynku (np. starsza wersja aplikacji programo-

[7] Prace nad polskim tłumaczeniem tej normy rozpoczną się w 1999 roku.

wej może być bardziej godna zaufania niż oprogramowanie będące nowością na rynku).

4.11.4. Techniczne środki stosowane w procesie akredytacji na etapie eksploatacji systemu informatycznego

Uzyskanie pewności działania zabezpieczeń na etapie eksploatacji systemu informatycznego polega na sprawdzeniu utrzymywania skuteczności tych zabezpieczeń w czasie (wykrycie ewentualnych metod obchodzenia zabezpieczeń, ich podatności na dynamicznie zmieniające się środowisko lub braku przestrzegania odpowiednich procedur). Dla utrzymania stanu bezpieczeństwa systemu informacyjnego powinny być stosowane dwie podstawowe metody:

- audytu systemu - jednorazowego lub okresowo powtarzającego się całościowego szacowania poziomu zabezpieczenia;
- monitorowania systemu i działań o charakterze ciągłym, mających na celu nadzór nad zmieniającym się systemem, jego użytkownikami oraz środowiskiem[8)].

3.11.4.1. Narzędzia i metody audytu

Wśród narzędzi, służących do realizacji audytu można wymienić:

- zautomatyzowane narzędzia wyszukiwania słabości systemu zabezpieczenia (np. narzędzia weryfikacji integralności plików, wyszukiwania słabych haseł, kontroli aktualności modyfikacji oraz łat w systemach i aplikacjach);
- wewnętrzne mechanizmy audytu (w tym badania, ankiety, obserwacje, testy zabezpieczeń i danych);

[8)] Rozróżnienie pojęć: audyt (*audit*), przegląd (*review*), monitorowanie (*monitoring*) może nastręczać trudności. Codzienne lub cotygodniowe sprawdzanie rejestrów zdarzeń mieści się w definicji monitorowania, natomiast analiza tych rejestrów za okres, np. pół roku to już audyt. Mniej formalny audyt jest zwykle nazywany przeglądem [14].

- testy penetracyjne (próby włamania się do systemu, z wykorzystaniem różnych metod, w tym uzyskanie informacji od użytkowników).

4.11.4.2. Narzędzia i metody monitorowania

Do narzędzi takich należą:
- przegląd rejestrów zdarzeń (patrz także 4.7.1);
- zautomatyzowane narzędzia (takie jak: skanery wirusów, programy weryfikujące integralność plików i baz danych), wykrywające naruszenie zabezpieczeń (*intrusion detectors*), narzędzia kontroli i oceny parametrów jakościowych działania systemu;
- narzędzia zarządzania konfiguracją (patrz także 4.4.1);
- zewnętrzne źródła informacji o stanie bezpieczeństwa systemów i poszczególnych produktów informatycznych, pojawiających się nowych zagrożeniach, wykrytych słabościach oraz podatnościach, a także metody i rozpowszechniane (np. za pomocą Internetu) narzędzia do usuwania dostrzeżonych błędów.

5. PODSUMOWANIE

W ostatnich latach pojęcie bezpieczeństwa systemów informatycznych zostało znacznie rozszerzone. Bezpieczeństwo to przestało być utożsamiane z bezpieczeństwem samej informacji. Równie ważne stało się bezpieczeństwo świadczenia usług za pośrednictwem systemu informatycznego. Komercyjne podejście do problemu bezpieczeństwa systemów, które można wyrazić jako uzyskanie zgodności celów zabezpieczenia z celami działania danej instytucji, skutkuje uznaniem nowych kryteriów bezpieczeństwa. Niezbędnym czynnikiem osiągnięcia i utrzymania bezpieczeństwa, określonego jako spełnienie tych kryteriów, jest sformułowanie polityki bezpieczeństwa systemu informatycznego.

Politykę bezpieczeństwa można definiować na poziomie celów, strategii i działań. W zaproponowanym modelu polityka bezpieczeństwa ma budowę wielopoziomową, w której cele przekładają się na strategie, a strategie na działania. Wyraźnie rozdzielenie poziomów polityki ma wiele zalet. Do nich należy zaliczyć: łatwość tworzenia oraz wdrożenia polityki, jednoznaczne przyporządkowanie zakresu odpowiedzialności różnych grup pracowników, łatwość modyfikowania polityki.

Tworzenie polityki bezpieczeństwa w tym modelu to hierarchiczne powiązanie ze sobą wielu dokumentów. Dokument poziomu pierwszego operuje w obszarze celów i definiuje kształt danej polityki. Jest to dokument, który można przedstawić jako obszerną deklarację celów, przyświecających kierownictwu danej instytucji w zakresie bezpieczeństwa jej systemu teleinformatycznego. Wszystkie inne dokumenty są określane mianem "dokumentów związanych" i nie mogą być sprzeczne z dokumentem definiującym cele.

Polityka poziomu drugiego odpowiada na pytanie "jak", definiując strategie oraz procesy zarządzania. Na tym poziomie polityka staje się efektywna, ponieważ dobrze zdefiniowane procesy zarządzania umożliwiają wyodrębnienie faz cyklu życia systemu bezpieczeństwa, powiązanie ich zarówno z ogólnymi procesami zarządzania w instytucji, jak i cyklem życia samego systemu teleinformatycznego.

Wreszcie, na poziomie działań są formułowane wymagania bezpieczeństwa. Te wymagania mają zarówno techniczny, jak i organizacyjny aspekt. Wszystkie podejmowane działania zdefiniowane w wymaganiach są efektem konkretnych procesów zarządzania. Przykładowo, obszerne omówienie zależności między strategią analizy ryzyka a postacią wymagań bezpieczeństwa dla danego systemu teleinformatycznego można znaleźć w [1]. Procesy zarządzania w sytuacjach awaryjnych i katastrofalnych umożliwiają zdefiniowanie

strategii, którymi należy kierować się przy tworzeniu planów utrzymania ciągłości działania (awaryjnych).

Jeśli polityka bezpieczeństwa zostanie utworzona zgodnie z tym modelem, to dana instytucja może mieć gwarancję, że będzie ona efektywna w dowolnym momencie cyklu życia systemu zabezpieczeń.

Obszerny opis procesów zarządzania bezpieczeństwem przedstawiono w [2]. Z kolei, przełożenie procesu planowania bezpieczeństwa, a w szczególności strategii analizy ryzyka, na wymagania bezpieczeństwa systemu informatycznego można znaleźć w [1]. W niniejszym artykule wymagania te sklasyfikowano w obszarach bezpieczeństwa i kolejno omówiono. W każdym obszarze poddano analizie techniczny i organizacyjny aspekt bezpieczeństwa systemu. Uzyskany obraz umożliwia opracowanie polityki bezpieczeństwa dla większości współczesnych systemów informatycznych.

Polityka bezpieczeństwa na poziomie celów będzie przedmiotem rozważań w następnym artykule.

Nowe spojrzenie na bezpieczeństwo systemów informatycznych polega na powiązaniu rozszerzonych, odpowiadających aktualnym potrzebom kryteriów bezpieczeństwa z każdym z poziomów modelu polityki, co gwarantuje osiągnięcie i utrzymanie odpowiedniego poziomu bezpieczeństwa. Przejście z jedno- do wielopoziomowego modelu polityki gwarantuje długookresową efektywność przyjętych rozwiązań, niezależnie od zmieniających się warunków działania danej instytucji.

WYKAZ LITERATURY

1. Andrukiewicz E.: Wybór strategii zarządzania ryzykiem w procesie planowania zabezpieczeń. II Krajowa Konferencja Zastosowań Kryptografii, Enigma'98, Warszawa, 26-28 maja 1998.
2. Andrukiewicz E.: Zarządzanie zabezpieczeniami systemu informacyjnego. Prace IŁ, nr 107, 1997.

3. BS 7799: 1995: Code of Practice for information Security management.
4. Business Information Security Survay (BISS'98). National Computer Centre, Manchester, UK.
5. Cameron D.: Security Issues for the Internet and the World Wide Web. Computer Technology Research Corp., Charleston, South Carolina (USA), 1997.
6. Cheswick B.: Internet Attacks: The Gory Details. The 15th World Conference on Computer Security, Audit & Control, London, UK, 11-13 November 1998.
7. Cohen F.: Managing Network Security - Integrity first, usually. Network Security, March 1997.
8. ISO/IEC FDIS 14508: Evaluation Criteria for IT Security (Common Criteria), *http://csrc.nist.gov/cc/*
9. ISO/IEC TR 13335-2:1997: Information Technology - Security Techniques - Guidelines for the management of IT Security (GMITS) - Part 2: Managing and planning IT Security.
10. Moller E.: Protective Measures Against Compromising Electromagnetic Radation Emitted by Video Display Terminals. InterPact Press, 1991.
11. PN EN 50081-1: 1996: Kompatybilność elektromagnetyczna. Wymagania ogólne dotyczące odporności na zakłócenia. Środowisko mieszkalne, handlowe i lekko uprzemysłowione Electromagnetic Compability. Generic emmission standard. Part 1: Residential, commercial and light industry.
12. PN EN 55022: 1996: Kompatybilność elektromagnetyczna. Dopuszczalne poziomy i metody pomiaru parametrów zakłóceń radioelektrycznych wytwarzanych przez urządzenia informatyczne. (CISPR 22:1993) Limits and methods of measurement of radio disturbance characteristics of information technology equipment.
13. Preneel B.: State of the art.Ciphers for Commertial Applications. The 15th World Conference on Computer Security, Audit & Control, London, UK, 11-13 November 1998.
14. RFC 2196: Site Security Handbook. B. Fraser, September 1997.

Эльжбета Андрукевич

НОВЫЙ ПОДХОД К ЗАЩИЩЕННОСТИ ИНФОРМАТИЧЕСКИХ СИСТЕМ

Резюме

Представлено эволюцию понятия защищенности информатических систем, которую можно наблюдать в последнее время. Показано что защищенность системы это больше чем защита информации и следует это понятие расширить на защищенность предоставляемых услуг. Вызывает это необходимость формулировки новых и модификации существующих критерий защищенности. Выполнение этих критерий может обеспечить политика защищенности определяемая на уровне целей, стратегии и действий. Основной тематикой настоящей работы является реализация политики на уровне действий. Для этого требования защищенности были сосредоточены в одинадцати зонах защищенности. В каждой такой зоне рассмотрено организационные и технические аспекты информатической системы.

Elżbieta Andrukiewicz

NEW APPROACH TO IT SECURITY

Summary

The evolution of IT security concepts, which can be observed in recent years, is presented in the article. It is clear that IT security is more than only information security and also includes service management security. This approach means that new security criteria should be addressed and existing ones - modified. IT security policy defined on the levels of objectives, strategies and activities can meet those criteria. The activity level policy

is the main subject of the article. Security requirements are collected in eleven areas. Organizational and technical aspects of IT security are discussed in each area.

Elżbieta Andrukiewicz

UNE NOUVELLE VUE SUR LA SECURITE DES SYSTEMES INFORMATIQUES

Résumé

Il est démontré l'évolution de la notion de sécurité des systèmes informatiques observable au cours des derniéres années. Il est prouvé que la sécurité d'un système signifie plus que la sécurité de l'information et il faut l'élargir avec la notion „la sécurité de moyen de rendre les services". Cela a pour conséquence la necessité de formuler les nouveaux critéres de la sécurité et modifier ceux qui existent. Pour accomplir les critères en question il faut mettre en oeuvre la politique de sécurité définie sur les niveaux des objectifs, de la stratégie et des actions. Le sujet principal de cet article est la réalisation de cette politique au niveau des actions. Pour cela nous avons classifié les exigences sur la sécurité dans onge domaines de la sécurité. Pour chaque de ces domaines nous avons présenté les aspects d'organisation et de technique d'un système informatique de la sécurité.

Elżbieta Andrukiewicz

NEUE ANSTELLUNG ZU IT-SICHERHEIT

Zusammenfassung

Beschrieben wird der in letzten Jahren gesehene enorme Fortschritt im Sinne der IT-Sicherheit. Est ist klar, daß IT-Sicherheit mehr als nur Informationssicherheit bedeutet und auch die Service-Management-Sicherheit

beeinhaltet. Das heißt, daß neue Sicherheitskriteria bestimmt und die altbegründete modifiziert werden sollen. Nur die auf dem Niveau von Zielen, Strategien und Tätigkeiten definierte IT-Sicherheitspolitik kann diesen Kriterien entgegenkommen. Die auf dem Höhe der Tätigkeit zu realisierende Politik stellt Hauptthema des Beitrags dar. Sicherheitserfordernisse wurden in elf Bereichen gruppiert. Organisatorische und technische Aufgaben wurden in jedem Bereich behandelt.

Zbigniew Rymarowicz

621.396.97:621.396.7:621.376.32

OGRANICZENIA MOCY STACJI UKF FM DLA OCHRONY SŁUŻB LOTNICZYCH PRZED ZAKŁÓCENIAMI

Omówiono zagadnienie występowania zakłóceń w urządzeniach odbiorczych służb radionawigacji lotniczej ILS i VOR, spowodowane sygnałami stacji UKF FM z zakresu 87,5 ÷ 108 MHz oraz metody zabezpieczania tych służb przed zakłóceniami. Krótko scharakteryzowano typy występujących zakłóceń i przedstawiono sposób ich analizowania, podając odpowiednie zależności. Określono obszary występowania potencjalnych zakłóceń w otoczeniu stacji UKF FM w zależności od jej mocy i częstotliwości, dla modelu odbiornika pokładowego samolotu ICAO Aneks 10, 1998. Zaproponowano wzory na maksymalną dopuszczalną moc stacji UKF FM, przy której byłyby spełnione warunki kompatybilności między radiofonią FM i radionawigacją lotniczą w określonych punktach testowych, w obszarze działania ILS i VOR. Wzory te dają możliwość przeanalizowania wartości mocy stacji UKF FM w zadanym zakresie częstotliwości, umożliwiając tym samym wykluczenie wszystkich częstotliwości kolizyjnych już na samym początku planowania stacji.

1. WPROWADZENIE

Radiofonia UKF FM w zakresie 87 ÷ 108 MHz stwarza niebezpieczeństwo powstawania zakłóceń w sąsiednim zakresie 108 ÷ 118 MHz użytkowanym przez radionawigację lotniczą. Ochrona przed tymi zakłóceniami jest niezwykle ważna ze względu na bezpieczeństwo. Błędy w nawigacji, których przyczyną mogą być zakłócenia, mogą do-

prowadzić do zejścia samolotu z kursu w czasie podchodzenia do lądowania lub w czasie przelotu.

W analizie kompatybilności między stacjami radiofonicznymi i służbami lotniczymi rozważa się zakłócenia typu A, spowodowane niezamierzonymi emisjami stacji radiofonicznych FM w pasmie lotniczym oraz zakłócenia typu B wytwarzane w odbiorniku pokładowym samolotu, pochodzące od sygnałów stacji radiofonicznych, pracujących na częstotliwościach spoza pasma lotniczego.

Metody zabezpieczania pracy tych służb przed zakłóceniami od stacji radiofonicznych zostały ustalone wstępnie w 1982 r. [3], a następnie sformułowane na konferencji w Genewie w 1984 r. [5]. W późniejszych latach były modyfikowane, a ostatnia ich wersja została ujęta w zaleceniu ITU-R IS 1009-1 [6] z 1996 r. Zasadniczym celem opracowanych metod jest wychwycenie i usunięcie wszystkich mogących pojawić się niekompatybilności w obszarze działania służb radionawigacji lotniczych (ILS - *Instrument Landing System*, VOR - *VHF Omnidirectional Radio Range*), jeszcze na etapie planowania stacji UKF FM.

W zaleceniu ITU-R IS 1009-1 przyjęto dla zakłóceń typu B dwa modele odbiornika pokładowego samolotu:

- model dla okresu przejściowego, uzgodniony w 1992 r. na zebraniu Grupy Roboczej 12/1 w Montrealu, nazwany w dalszej części opracowania Montreal 1992;
- model o większej odporności na zakłócenia, określony przez *International Civil Aviation Organization* (Aneks 10, 1998), nazwany ICAO 1998.

Pierwszy z tych modeli dopuszcza większe poziomy zakłóceń. Wprowadzono go, ponieważ część użytkowanych wówczas odbiorników ILS i VOR wykazywała małą odporność na zakłócenia typu B. Drugi model, który powinno stosować się w analizie kompatybilności od 1 stycznia 1998 r., zakłada, że użytkowane odbiorniki ILS i VOR spełniają wymagania odpornościowe ICAO Aneks 10 [4].

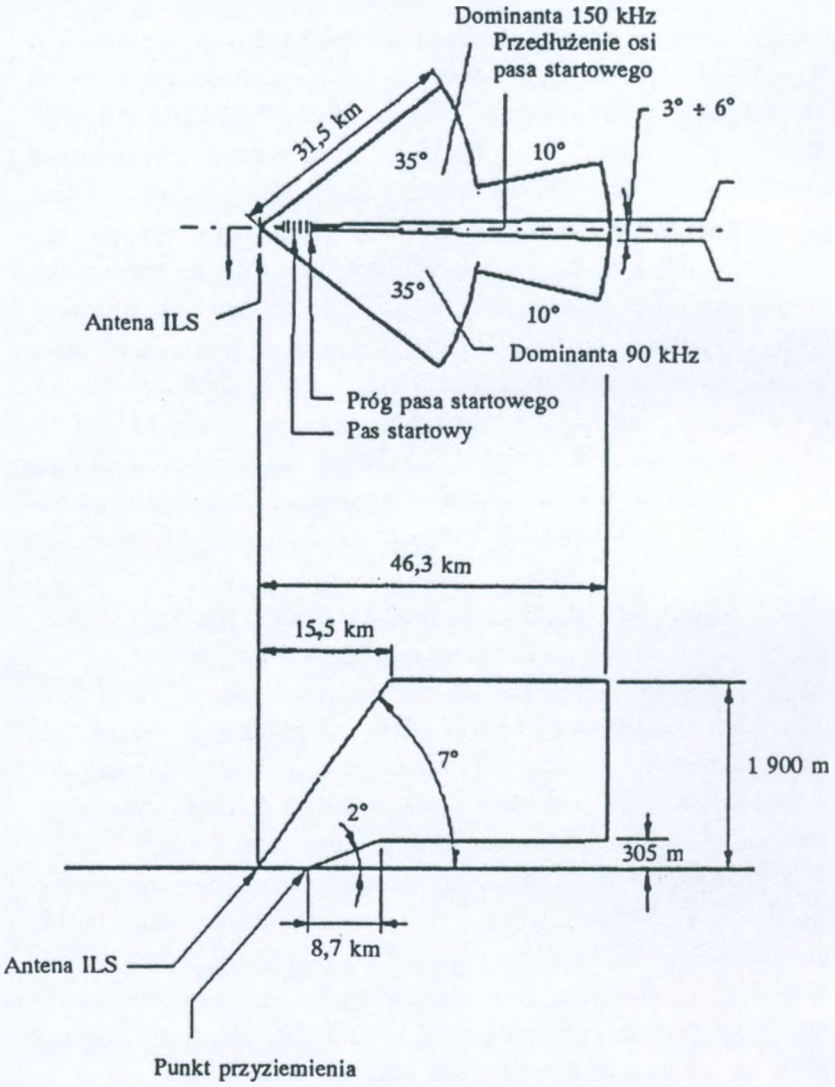
Wprowadzanie dodatkowej stacji UKF FM do istniejącej sieci nadawczych wiąże się z możliwością dobrania dla niej odpowiedniego kanału częstotliwościowego i mocy. Dobierając te parametry trzeba respektować stacje radiofoniczne, telewizyjne i radionawigacyjne, zawarte w planie przydziałów częstotliwości, tak aby w obszarze ich działania nie powodować wzrostu zakłóceń. Ponieważ o maksymalnej dopuszczalnej mocy dla stacji UKF FM na poszczególnych częstotliwościach decydują w pierwszej kolejności warunki, wynikające z kompatybilności między radiofonią i radionawigacją lotniczą, dlatego w niniejszym artykule przedstawiono jedynie ten aspekt. Pominięto natomiast ograniczenia, wynikające z warunków kompatybilności wewnętrznej sieci UKF FM i zewnętrznej z telewizją, które oczywiście również przy planowaniu stacji należy brać pod uwagę. Omówiono także metody zabezpieczania pracy systemu ILS i VOR przed zakłóceniami ze strony stacji UKF FM dla modelu odbiornika ICAO 1998 oraz określono obszar występowania potencjalnych zakłóceń w otoczeniu stacji UKF FM w zależności od jej parametrów.

2. SYSTEMY RADIONAWIGACJI LOTNICZEJ I ICH PARAMETRY

Pasmo częstotliwości 108 ÷ 118 MHz jest użytkowane przez dwa systemy radionawigacji lotniczej: system ILS, który przekazuje pilotowi dane o położeniu samolotu w stosunku do osi pasa startowego i system VOR, który służy do określenia kursu samolotu.

System ILS jest instalowany na wszystkich ważniejszych lotniskach. Stacje tego systemu pracują na częstotliwościowych: 108,10, 108,15, 108,30, 108,35 MHz itd. aż do 111,70, 111,75, 111,90 i 111,95 MHz, z polaryzacją poziomą. Emitują one falę nośną modulowaną sygnałami o częstotliwościach 90 i 150 Hz. Jeśli samolot znajduje się na lewo od kierunku osi pasa, dominuje sygnał o częstotliwości 90 Hz, jeśli zaś na prawo - sygnał o częstotliwości 150 Hz.

Różnica głębokości modulacji obu tych sygnałów jest proporcjonalna do wielkości odchylenia od osi pasa startowego.



Rys. 1. Obszar działania ILS [6]

Typowy obszar działania ILS od strony podejścia do lądowania pokazano na rys. 1. Obszar ten niekiedy może się rozciągać po przeciwnej stronie podejścia do lądowania, ponieważ niektóre administracje wykorzystują ILS także jako pomocniczy system naprowadzający.

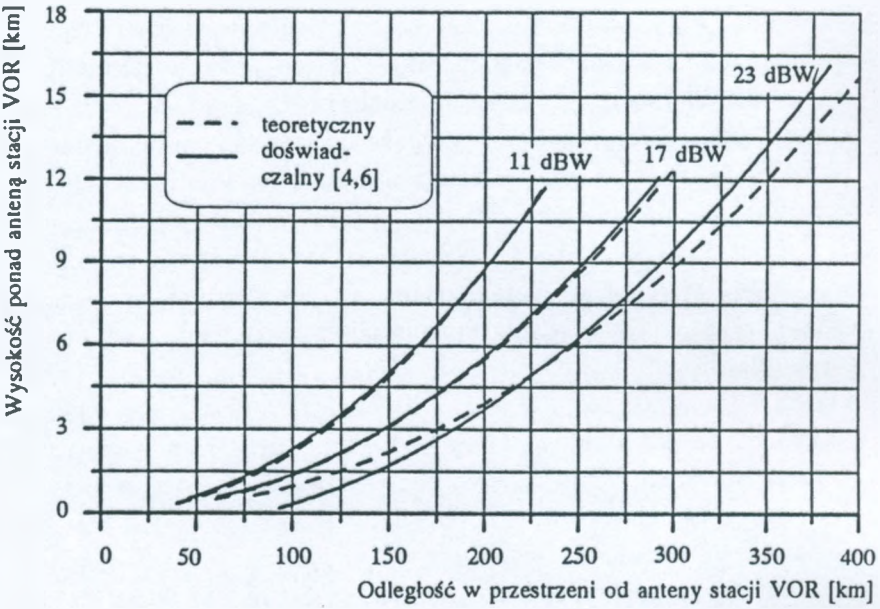
Minimalne natężenie pola, zabezpieczające pracę systemu ILS, wynosi 32 dB (μV/m). Wyższe natężenie pola, dla zwiększenia stosunku sygnał/zakłócenie, jest wymagane od punktu przyziemienia do 18,5 km. W obszarze tym, w zależności od kategorii ILS (I, II, III) wartość natężenia pola powinna wynosić 39 ÷ 46 dB (μV/m).

System VOR umożliwia uzyskanie wskazań o kursie samolotu. Stacje tego systemu są rozmieszczone na skrzyżowaniach i zagięciach korytarzy powietrznych. Pracują one z polaryzacją poziomą na częstotliwościach: 108,05, 108,20, 108,25 MHz itd. aż do 111,85, 111,85 MHz w pasmie 108 ÷ 112 MHz i częstotliwościach 112,00, 112,05, ... 117,95 MHz w pasmie 112 ÷ 118 MHz. Minimalne natężenie pola sygnału VOR, zapewniające niezakłóconą pracę tego sytemu wynosi 39 dB (μV/m).

Stacja VOR emituje dwa sygnały, przy czym jeden z nich jest modulowany sygnałem akustycznym o częstotliwości 9960 Hz. Po odebraniu ich przez samolot otrzymuje się dwa sygnały 30 Hz. Jeden o stałej fazie, drugi zaś o fazie zależnej od kierunku, w którym jest on emitowany przez stację naziemną VOR. Różnica faz między tymi dwoma sygnałami wyznacza kurs samolotu.

Zasięgi VOR mogą różnić się w zależności od zastosowania. W strefie przylotniskowej wynosić one mogą 75 km, a w przypadku nawigacji przelotowej nawet 370 km. Na rys. 2 pokazano typowe zasięgi stacji VOR dla minimalnego natężenia pola sygnału, zapewniającego niezakłóconą pracę tego systemu przy różnych mocach. Zasięgi te zostały wykreślone dla trzech wartości mocy promieniowanej (ERP) i anteny umieszczonej 4,9 m n.p.t. [4, 6]. Na rys. 2 naniesiono również zasięgi stacji oparte na teoretycznej zależności natężenia pola od odległości. Przy wykreślaniu tych krzywych założono,

że natężenie pola w punkcie odbioru powstaje w wyniku interferencji fali bezpośredniej i fali odbitej od ziemi.



Rys. 2. Zasięg stacji VOR

Sygnały stacji UKF FM odbierane w samolocie przez urządzenia systemu ILS i VOR są w postaci szumu. Ponieważ częstotliwości 90 i 150 Hz w przypadku ILS oraz 30 i 9960 Hz w przypadku VOR są podatne na ten rodzaj zakłóceń, dlatego jest niezbędna ich ochrona.

3. RODZAJE ZAKŁÓCEŃ

Jak już wspomniano, w analizie kompatybilności między radiofonią FM i radionawigacją lotniczą rozważa się zakłócenia typu A oraz typu B.

Zakłócenia typu A obejmują:

- zakłócenia A1, spowodowane produktami intermodulacji powstającymi w urządzeniach nadawczych stacji radiofonicznych wspólnie zlokalizowanych lub innymi niezamierzonymi produktami, promieniowanymi przez te stacje w pasmie lotniczym; zakłócenia te rozważa się, jeżeli różnica między częstotliwością produktu intermodulacji i częstotliwością ILS lub VOR nie przekracza 200 kHz;
- zakłócenia A2, spowodowane emisją pozapasmową stacji UKF FM, pracujących na częstotliwościach bliskich pasma lotniczego; zakłócenia te rozważa się, jeżeli różnica między częstotliwościami stacji UKF FM i ILS lub VOR nie przekracza 300 kHz.

Zakłócenia typu B obejmują:

- zakłócenia B1, spowodowane produktami intermodulacji powstającymi w odbiorniku lotniczym, w wyniku jego nieliniowości, od sygnałów stacji UKF FM spoza pasma lotniczego; co najmniej dwa sygnały radiofoniczne mogą stanowić przyczynę powstawania tego rodzaju zakłóceń: jeden z nich musi być dostatecznie silnym sygnałem, niezbędnym do zainicjowania tego rodzaju zakłóceń, a pozostałe sygnały mogą być o znacznie niższym poziomie, po przekroczeniu którego uczestniczą w przemianie częstotliwości; w zakłóceniach typu B1 uwzględnia się produkty intermodulacji trzeciego rzędu o następujących częstotliwościach dla dwóch sygnałów:

$$f_{intermod} = 2f_1 - f_2 \qquad \text{dla } f_1 > f_2, \tag{1}$$

i trzech sygnałów:

$$f_{intermod} = f_1 + f_2 - f_3 \qquad \text{dla } f_1 \geq f_2 > f_3, \tag{2}$$

gdzie:

$f_{intermod}$ - częstotliwość produktu intermodulacji [MHz],
f_1, f_2, f_3 - częstotliwości stacji UKF FM [MHz];

- zakłócenia B2, spowodowane tzw. blokowaniem odbiornika; występują one wtedy, gdy odbiornik pokładowy samolotu jest narażony na przesterowanie przez silny sygnał stacji UKF FM.

4. MODELE ODPORNOŚCI ODBIORNIKA NA ZAKŁÓCENIA TYPU B

4.1. Zakłócenia typu B1

Dwa lub trzy sygnały stacji UKF FM przenikając do obwodów nieliniowych wejściowych stopni odbiornika pokładowego mogą w pewnych przypadkach stanowić przyczynę powstawania zakłóceń. Na nieliniowości tych obwodów powstaje przemiana częstotliwości, a w jej wyniku wytwarzają się składowe, na które może reagować odbiornik. Zakłócenia tego typu wystąpią, gdy jeden z sygnałów będzie dostatecznie silnym sygnałem, niezbędnym do zainicjowania tego rodzaju zakłóceń, przekraczającym wartość N_{inic}. Pozostałe sygnały mogą być znacznie słabsze, lecz po przekroczeniu określonej wartości N_{ucz} będą uczestniczyć w przemianie częstotliwości. Wartości N_{inic} i N_{ucz} na wejściu odbiornika pokładowego samolotu są określone następującymi wzorami [6]:

- w przypadku intermodulacji trzeciego rzędu przy dwóch sygnałach:

$$N_{inic} = \frac{L_C - K - S}{3} + C_i \tag{3}$$

- i trzech sygnałach:

$$N_{inic} = \frac{L_C - K - 6 - S}{3} + C_i \tag{4}$$

oraz

$$N_{ucz} = -66 + 20 \lg \frac{\max (0{,}4;\ 108{,}1 - f_i)}{0{,}4}, \tag{5}$$

w których

$$C_i = B \lg \frac{\max (f_g; f_o - f_i)}{f_g} \tag{6}$$

i

$$L_C = N_L - N_{ref}, \tag{7}$$

gdzie:

N_{inlc} - poziom sygnału inicjującego zakłócenia intermodulacyjne [dBm],

N_{ucz} - poziom sygnału [dBm], po przekroczeniu którego stacje uczestniczą w przemianie częstotliwości,

L_C - współczynnik korekcyjny, uwzględniający zmianę poziomu sygnału ILS lub VOR w odniesieniu do odpowiedniego minimalnego poziomu sygnału zabezpieczającego pracę tych systemów [dB],

N_L - poziom sygnału ILS lub VOR [dBm] na wejściu odbiornika pokładowego samolotu,

f_i - częstotliwość i-tej stacji radiofonicznej [MHz],

f_g, f_o, K, N_{ref}, S - stałe zależne od modelu odbiornika lotniczego (tablica 1).

Tablica 1

Wartości parametrów w uzgodnionych modelach odbiornika

Parametr	Model odbiornika Montreal 1992	Model odbiornika ICAO 1998
S [dBm]	0	3,0
B	28	20,0
f_g [MHz]	1	0,4
f_o [MHz]	częstotliwość ILS lub VOR	108,1
K_{ILS} [dBm]	140	78,0
K_{VOR} [dBm]	133	78,0
$N_{ref,ILS}$ [dBm]	-89	-86,0
$N_{ref,VOR}$ [dBm]	-82	-79,0

Rozpatrując produkty intermodulacji wpadające w pasmo od 108 do 118 MHz, bada się, czy zaistniały warunki na powstanie zakłóceń B1. Zakłócenia tego typu mogą wystąpić, jeżeli poziomy N_1, N_2, N_3 sygnałów pochodzących od stacji UKF FM na wejściu odbiornika pokładowego samolotu spełniają nierówność w przypadku [6]:

- dwóch sygnałów:

$$2N_1 + N_2 - 3W_o - 2C_1 - C_2 + K - L_C + S > 0 \qquad (8)$$

- i trzech sygnałów:

$$N_1 + N_2 + N_3 - 3W_o - C_1 - C_2 - C_3 + K + 6 - L_C + S > 0, \qquad (9)$$

gdzie:

N_1, N_2, N_3 - poziomy sygnałów stacji UKF FM [dBm] na wejściu odbiornika pokładowego samolotu,

W_o - współczynnik uwzględniający odstrojenie produktu intermodulacji od sygnału radionawigacyjnego (tablica 2).

Tablica 2

Wartości współczynnika W_o w zależności od wartości odstrojenia produktu intermodulacji od sygnału radionawigacyjnego [6]

Różnica częstotliwości ILS lub VOR i produktu intermodulacji [kHz]	Współczynnik W_o [dB]	
	model odbiornika Montreal 1992	model odbiornika ICAO 1998
0	0	0
50	2	2
100	8	5
150	16	11
200	26	-

4.2. Zakłócenia typu B2

Zakłócenia tego typu mogą wystąpić, jeżeli wartość maksymalna sygnału stacji UKF FM na wejściu odbiornika pokładowego modelu Montreal 1992 przekroczy poziom [6]:

$$N_{max} = -20 + 20 \lg \frac{\max (0{,}4; f_L - f_i)}{0{,}4}, \tag{10}$$

a na wejściu odbiornika ICAO 1998 poziom [6]:

$$N_{max} = \min\left\{15; -10 + 20 \lg \frac{\max (0{,}4; 108{,}1 - f_i)}{0{,}4} + L_{CI} - S\right\}, \tag{11}$$

przy czym:

$$L_{CI} = \max \{0; 0{,}5\ L_C\}, \tag{12}$$

gdzie:

N_{max} - poziom maksymalny sygnału stacji UKF FM [dBm], po przekroczeniu którego występuje blokowanie odbiornika pokładowego samolotu,

f_i - częstotliwość stacji UKF FM [MHz],

f_L - częstotliwość stacji ILS lub VOR [MHz],

S - stała zależna od modelu odbiornika lotniczego (tabl. 1).

5. LOKALIZACJA ORAZ WYSOKOŚĆ PUNKTÓW TESTOWYCH ILS I VOR

Analizę kompatybilności stacji radiofonicznych ze służbami radionawigacji lotniczej przeprowadza się w wielu zdefiniowanych punktach testowych. Analiza ta dla ILS oparta jest na stałych punktach testowych rozmieszczonych w obszarze jego działania i dodatkowych

punktach testowych dla każdej stacji UKF FM znajdującej się w jego zasięgu. Natomiast dla VOR punkty testowe są zlokalizowane na odpowiedniej wysokości nad stacjami UKF FM znajdującymi się w jego zasięgu. Dodatkowe punkty wyznacza się dla stacji UKF FM znajdujących się poza jego zasięgiem, jeśli stacje te spełniają określone warunki.

Ze zwiększaniem wysokości punktu testowego liczba stacji, które mogą przyczynić się do powstania zakłóceń, wzrasta i dlatego dla zakłóceń B1 przeprowadza się dodatkowe obliczenia w punktach testowych położonych na większych wysokościach, jednak nie większych od maksymalnej wysokości przewidzianej dla danego obszaru działania ILS lub VOR i nie większej od wysokości, przy której poziom sygnału od stacji UKF FM osiąga wartość wyzwalającą zakłócenia. Obliczenia w tych punktach mają na celu uchwycenie wszystkich przypadków, w jakich mogą pojawić się zakłócenia.

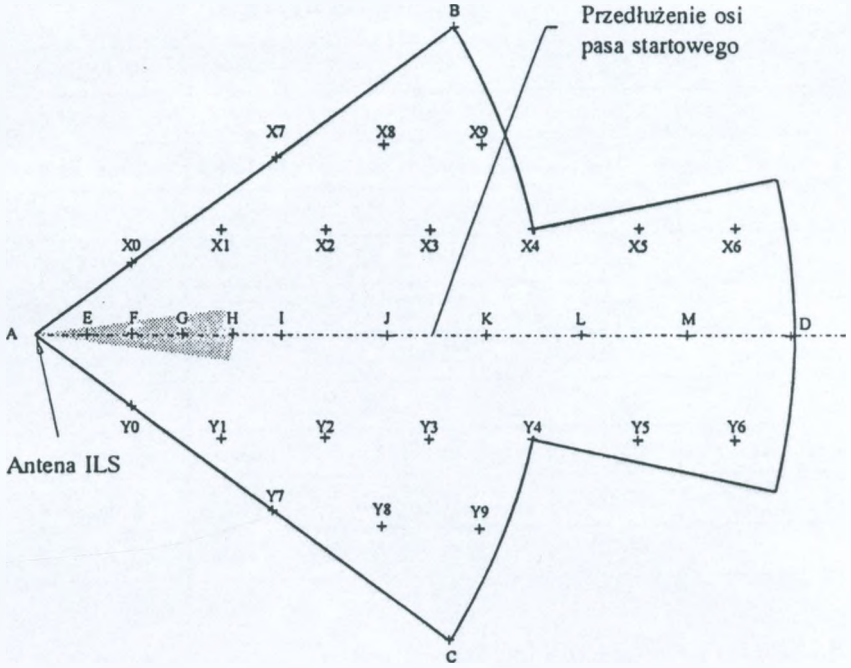
5.1. Punkty testowe dla ILS

Rozmieszczenie stałych punktów testowych w obszarze działania ILS pokazano na rys. 3. Dane dotyczące ich lokalizacji zamieszczono w tablicy 3. Dla punktów A, E, F, G i H minimalne wysokości względem ILS wynoszą odpowiednio 0, 0, 150, 300 i 450 m. Wartości te reprezentują ścieżkę schodzenia samolotu o nachyleniu 3°. Dla pozostałych stałych punktów testowych minimalne wysokości wynoszą 600 m. Ciemniejszym kolorem na rys. 3 zaznaczono strefę ścieżki schodzenia samolotu, która jest zawarta w kącie ±7° od osi pasa startowego i rozciąga się do 12 km od anteny stacji ILS.

Przy wyznaczaniu natężenia pola sygnału stacji UKF FM w stałych punktach testowych, bierze się pod uwagę odległość między nimi w przestrzeni. Odległość ta nie powinna być mniejsza od 150 m dla stacji UKF FM znajdującej się w strefie ścieżki schodzenia samolotu (zacieniony obszar na rys. 3) i od 300 m dla stacji znajdujących

się w zasięgu ILS, lecz na zewnątrz strefy ścieżki schodzenia samolotu do lądowania.

Dla stacji UKF FM znajdującej się w zasięgu ILS na zewnątrz strefy ścieżki schodzenia samolotu, dodatkowe punkty testowe są tworzone na różnych wysokościach w miejscu lokalizacji stacji, w obszarze działania ILS, powyżej: 600 m ponad miejscem posadowienia ILS i 150 m ponad anteną stacji UKF FM.



Rys. 3. Rozmieszczenie stałych punktów testowych w obszarze działania ILS [6]

Jeśli natomiast stacja UKF FM znajduje się w strefie ścieżki schodzenia samolotu, to dalsze punkty testowe są tworzone w odległości 150 m od miejsca lokalizacji stacji i na tych samych wysokościach jak jej antena.

Tablica 3

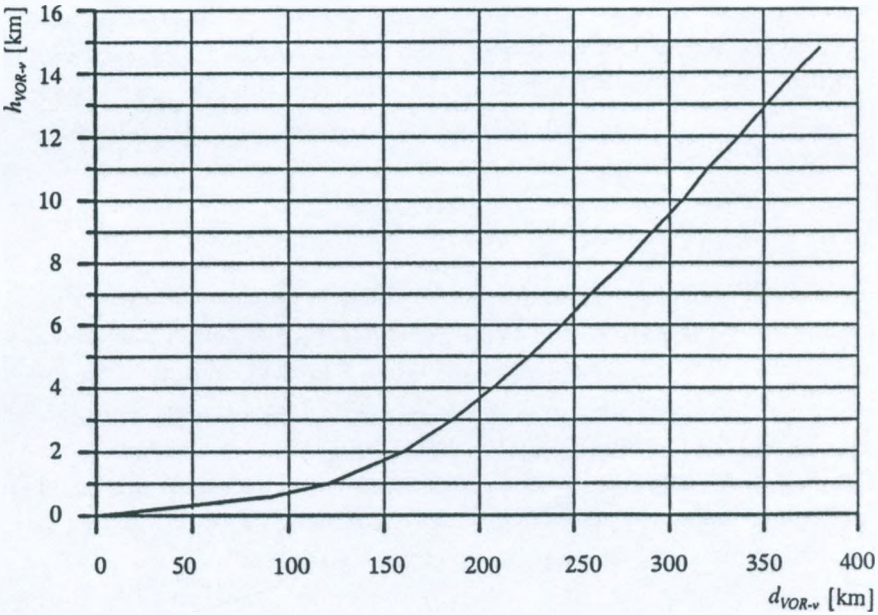
Rozmieszczenie punktów testowych w obszarze działania ILS [6]

Punkty testowe na lub powyżej osi pasa startowego			Punkty poza osią pasa startowego (wszystkie na wysokości 600 m)		
oznaczenie punktu	odległość [km]	wysokość minimalna [m]	oznaczenie punktu	odległość [km]	kąt odchylenia od osi pasa startowego [°]
A	0,00	0	B, C	31,5	-35,0; 35,0
E	3,00	0	XO, YO	7,7	-35,0; 35,0
F	6,00	150	X1, Y1	12,9	-25,5; 25,5
G	9,00	300	X2, Y2	18,8	-17,2; 17,2
H	12,00	450	X3, Y3	24,9	-12,9; 12,9
I	15,00	600	X4, Y4	31,5	-10,0; 10,0
J	21,25	600	X5, Y5	37,3	- 8,6; 8,6
K	27,50	600	X6, Y6	43,5	-7,3; 7,3
L	33,75	600	X7, Y7	18,5	-35,0; 35,0
M	40,00	600	X8, Y8	24,0	-27,6; 27,6
D	46,20	600	X9, Y9	29,6	-22,1; 22,1

5.2. Punkty testowe dla VOR

Punkty testowe dla stacji UKF FM znajdującej się w zasięgu VOR lub na zewnątrz tego zasięgu, w odległości do 3 km od jego granicy, są tworzone na różnych wysokościach w miejscu jej lokalizacji, powyżej: 600 m nad poziomem lokalnego terenu (w przybliżeniu 600 m nad poziomem terenu u podstawy masztu), 300 m nad jej anteną i powyżej dolnej granicy obszaru działania VOR (rys. 4).

Z porównania rys. 2 i 4 widać, że przy mniejszych mocach dolna granica obszaru działania VOR znajduje się powyżej wysokości podanej na rys. 4. Oznacza to, że przy wyznaczaniu minimalnej wysokości punktu testowego powinno się również uwzględniać moc stacji VOR.



Rys. 4. Wysokość minimalna położenia punktu testowego względem stacji VOR w funkcji odległości [6]

Biorąc powyższe pod uwagę, minimalna wysokość punktu testowego v n.p.m. wyrazi się wzorem:

$$h_{v-m,\min} = \max\,(300 + h_{a-m};\ 600 + h_{t-m};\ h_{d-m})\,, \qquad (13)$$

gdzie:

$h_{v-m,\min}$ - wysokość minimalna punktu testowego n.p.m. [m],

h_{a-m} - wysokość zawieszenia anteny stacji UKF FM n.p.m. [m],

$h_{t\text{-}m}$ - wysokość terenu n.p.m. [m] w miejscu lokalizacji stacji UKF FM,

$h_{d\text{-}m}$ - wysokość dolnej granicy obszaru działania VOR n.p.m. [m].

Punkty testowe dla stacji znajdujących się na zewnątrz obszaru działania VOR, w odległości większej od 3 km od jego granicy, są tworzone na różnych wysokościach w punkcie przecięcia granicy obszaru z prostą łączącą stację VOR ze stacją UKF FM, powyżej: 600 m n.p.m., wysokości anteny stacji UKF FM n.p.m. i wysokości n.p.m. dolnej granicy obszaru działania VOR (rys. 4). Minimalna wysokość punktu testowego v n.p.m. wyrazi się zatem wzorem:

$$h_{v\text{-}m,\min} = \max\left(h_{a\text{-}m};\ 600 + h_{t\text{-}m};\ h_{d\text{-}m}\right). \tag{14}$$

Punkty testowe znajdujące się na granicy obszaru działania VOR w odległości mniejszej niż 250 m są uważane za te same. Inne dodatkowe punkty testowe mogą być tworzone wewnątrz obszaru działania VOR, jeżeli system ten jest stosowany przy kącie mniejszym od 0° względem horyzontu, pod jakim widać punkt testowy ze środka anteny lub stosowany jako pomoc przy lądowaniu. Przy tym minimalna odległość między stacją UKF FM i punktem testowym, stosowana w obliczeniach natężenia pola, powinna wynosić 300 m.

6. METODY OBLICZANIA NATĘŻENIA POLA

6.1. Natężenie pola sygnału UKF FM

W analizie kompatybilności między radiofonią i radionawigacją lotniczą zakłada się, że występuje bezpośrednia widoczność między anteną stacji UKF FM i punktem testowym. Wobec tego natężenie pola w punkcie testowym v wyrazi się wzorem:

$$E_v = 76{,}9 + P - 20 \lg D_{a\text{-}v} + H + V, \tag{15}$$

przy czym odległość punktu testowego od anteny stacji UKF FM i kąt elewacji, pod jakim widać punkt testowy v ze środka anteny są zdefiniowane następująco:

$$D_{a-v} = \sqrt{\left(\frac{h_{v-m} - h_{a-m} - (d_{a-v}/4{,}1)^2}{1000}\right)^2 + d_{a-v}^{\,2}} \qquad (16)$$

$$\theta = \operatorname{arctg}\left(\frac{h_{v-m} - h_{a-m} - (d_{a-v}/4{,}1)^2}{1000\, d_{a-v}}\right), \qquad (17)$$

gdzie:

E_v - natężenie pola [dB(μV/m] w punkcie testowym v,

P - moc promieniowana stacji (E.R.P) [dBW],

D_{a-v} - odległość punktu testowego v od anteny stacji UKF FM [km],

H - współczynnik kierunkowości anteny w płaszczyźnie poziomej [dB],

V - współczynnik kierunkowości anteny w płaszczyźnie pionowej [dB],

θ - kąt elewacji, pod jakim widać punkt testowy v ze środka anteny [°],

d_{a-v} - odległość w poziomie punktu testowego v od anteny stacji UKF FM [km],

h_{v-m} - wysokość punktu testowego v n.p.m. [m],

h_{a-m} - wysokość anteny stacji UKF FM n.p.m. [m].

W zaleceniu ITU-R IS 1009-1 [6] przyjęto, że suma wartości współczynników kierunkowości anteny w płaszczyźnie poziomej i pionowej (H + V) jest ograniczona do -20 dB, a dla kąta elewacji większego od 45° nie uwzględnia się współczynnika kierunkowości anteny w płaszczyźnie poziomej H. W przypadku stacji o polaryzacji mieszanej za moc promieniowaną stacji przyjmuje się wartość większą, wynikającą z podziału mocy na składową pionową i pozio-

mą. Jeśli moce obu tych składowych będą równe, to za moc promieniowaną stacji przyjmuje się moc składowej poziomej powiększoną o 1 dB.

Wprowadzony do wzoru (15) współczynnik kierunkowości anteny w płaszczyźnie pionowej V dla $A_a > 2$ ma postać [6]:

$$V = -\begin{cases} 0 & ; \text{ dla } \theta \le \arcsin(1/(\pi A_a)) \\ 20 \lg(\pi A_a \sin\theta); & \text{dla } \arcsin(1/(\pi A_a)) < \theta \le \arcsin(5/(\pi A_a)) \\ 14 & ; \text{ dla } \theta > \arcsin(5/(\pi A_a)) \end{cases} \tag{18}$$

gdzie A_a jest wartością apertury pionowej anteny wyrażoną w jednostkach długości fali. Wartości A_a w zależności od mocy stacji UKF FM są podane są w tablicy 4.

Tablica 4

Apertura pionowa anteny A_a w funkcji mocy promieniowanej stacji UKF FM [6]

Moc promieniowana [dBW]	Apertura pionowa anteny [długość fali]
$P \ge 44$	8
$37 \le P < 44$	4
$30 \le P < 37$	2
$P < 30$	1

Ograniczenie do -14 dB dla kąta θ większego od $\arcsin(5/(\pi A_a))$ stosuje się także w przypadku znanych konstrukcji anten o większym współczynniku wytłumienia w płaszczyźnie pionowej.

Jeżeli natomiast $A_a \le 2$, to wtedy współczynnik kierunkowości anteny w płaszczyźnie pionowej V jest określony wzorem:

$$V = \begin{cases} 0 & ; \text{ dla } \theta \le 10^\circ \\ 2{,}3 \sin\theta - 13{,}2 (\sin\theta)^2 & ; \text{ dla } 10^\circ < \theta \le 60^\circ \\ -8 & ; \text{ dla } \theta > 60^\circ \end{cases} \tag{19}$$

Podaną zależność otrzymano na podstawie danych tabelarycznych zawartych w zaleceniu ITU-R IS 1009-1 [6].

6.2. Natężenia pola sygnału ILS

Do obliczeń natężenia pola sygnału ILS stosuje się dwie metody: metodę interpolacyjną i metodę interferencyjną, zwaną także metodą dwupromieniową. Z obliczeń metodą interpolacyjną otrzymuje się wartości minimalne określone przez ICAO, nie wymagające stosowania marginesu bezpieczeństwa. Natomiast z obliczeń metodą interferencyjną otrzymuje się dokładniejsze wartości natężenia pola, jednak metoda ta wymaga wielu dodatkowych danych, takich jak: moc promieniowana, charakterystyka promieniowania anteny w płaszczyźnie poziomej, wysokość zawieszenia anteny ILS n.p.m. i wysokość płaszczyzny odbicia n.p.m.

Metoda interpolacyjna jest przeznaczona zasadniczo do obliczeń natężenia pola na wysokościach większych od 60 m względem ILS. Dla tych wysokości wartość natężenia pola $E_{ILS\,1}$ wyznacza się ze wzoru [6]:

$$E_{ILS,1} = \begin{cases} 39 - \max\left(0; \dfrac{d_{ILS\text{-}v} - 18{,}5}{4}\right); & \text{dla } \alpha \le \pm 10^{\circ},\ d_{ILS\text{-}v} \le 46{,}3 \text{ km} \\ 39 - \dfrac{d_{ILS\text{-}v}}{4{,}5} & ;\ \text{dla } 10^{\circ} < \alpha \le 35^{\circ},\ d_{ILS\text{-}v} \le 18{,}5 \text{ km} \end{cases} \tag{20}$$

gdzie:

$E_{ILS\,1}$ - natężenie pola [dB(μV/m)] sygnału ILS,

$d_{ILS\text{-}v}$ - odległość punktu testowego v od anteny ILS [km] (rys. 5).

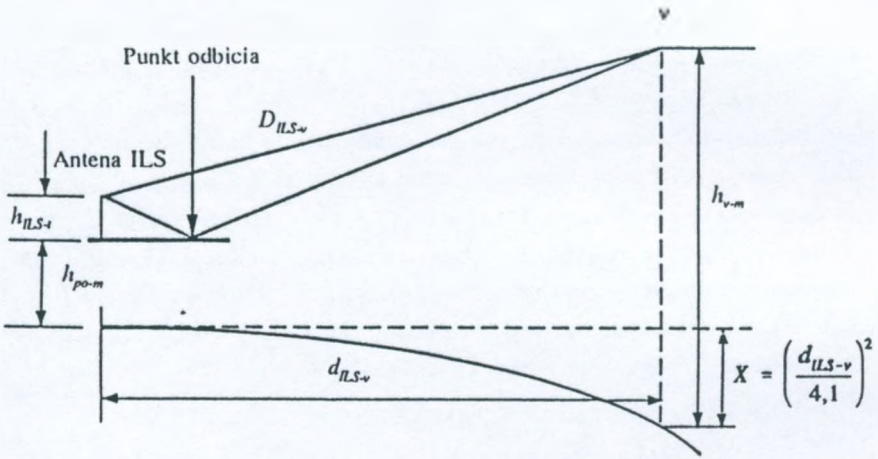
Dla wysokości mniejszej od 60 m zakłada się, że wartość natężenia pola jest stała i wynosi 32 dB(μV/m).

Natomiast w metodzie interferencyjnej (rys. 5) natężenie pola $E_{ILS\,2}$ wyznacza się [6] ze wzoru:

$$E_{ILS,2} = \max\left(E_{ILS,1};\ E_{ILS} - 8\right), \tag{21}$$

w którym $E_{ILS,1}$ jest wartością natężenia pola obliczoną metodą interpolacyjną, 8 dB zapewnia pewien margines bezpieczeństwa, a E_{ILS} ma postać [6]:

$$E_{ILS} = 82{,}9 + P_{ILS} - 20 \lg D_{ILS\text{-}v} + H_{ILS} + 20 \lg \sin\left(\frac{\pi \Delta}{\lambda}\right), \tag{22}$$



Rys. 5. Metoda interferencyjna

przy czym

$$\Delta = \frac{2h_{ILS\text{-}t}\left[h_{v\text{-}m} - h_{po\text{-}m} - (d_{ILS\text{-}v}/4{,}1)^2\right]}{1000\, d_{ILS\text{-}v}}, \tag{23}$$

gdzie:

P_{ILS} - moc promieniowana ILS [dBW],

$D_{ILS\text{-}v}$ - odległość punktu testowego v od anteny ILS [km],

H_{ILS} - współczynnik kierunkowy anteny ILS w płaszczyźnie poziomej [dB],

Δ - różnica długości dróg fali bezpośredniej i odbitej od ziemi w punkcie testowym v [m],
λ - długość fali [m],
$h_{ILS\text{-}t}$ - wysokość zawieszenia anteny ILS n.p.t. [m],
$h_{v\text{-}m}$ - wysokość punktu testowego v n.p.m. [m],
$h_{po\text{-}m}$ - wysokość płaszczyzny odbicia n.p.m. [m].

W metodzie tej zakłada się, że w punktach testowych A i E (rys. 3) wartość natężenia pola jest stała i wynosi 32 dB(μV/m).

6.3. Natężenia pola sygnału VOR

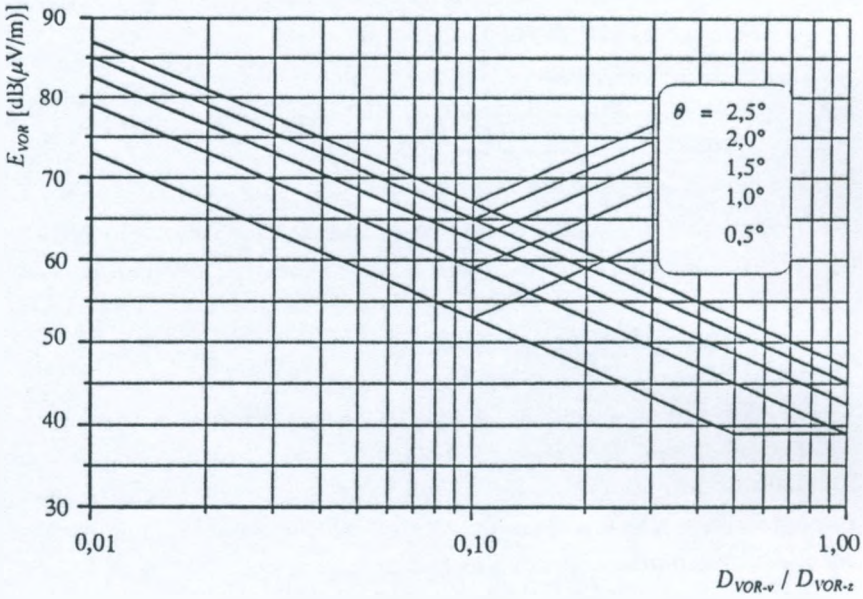
Do obliczeń natężenia pola sygnału stacji VOR jest stosowana metoda interpolacyjna. Nie wymaga ona uwzględniania marginesu bezpieczeństwa, ponieważ otrzymane na jej podstawie wartości natężenia pola są wartościami minimalnymi. Natężenie pola, jakie można oczekiwać w punkcie testowym v dla kąta elewacji $0° \le \theta \le 2{,}5°$ i wysokości anteny stacji VOR n.p.t. mniejszej od 7 m, oblicza się [6] z zależności:

$$E_{VOR} = E_{\min} + \max\left(0;\ 20 \lg\left(\theta\, D_{VOR\text{-}z} / D_{VOR\text{-}v}\right)\right), \tag{24}$$

w której:

$$\theta = \operatorname{arctg}\left(\frac{h_{v\text{-}m} - h_{VOR\text{-}m} - (D_{VOR\text{-}v}/4{,}1)^2}{1000\, D_{VOR\text{-}v}}\right), \tag{25}$$

gdzie:
$E_{\min}$ - minimalne natężenie pola określone przez ICAO [dB],
$D_{VOR\text{-}z}$ - zasięg stacji VOR [km] dla $\theta = 1°$ [1],
$D_{VOR\text{-}v}$ - odległość punktu testowego v od anteny VOR [km],
θ - kąt elewacji, pod jakim widać punkt testowy ze środka anteny [°],
$h_{v\text{-}m}$ - wysokość punktu testowego v n.p.m. [m],
$h_{VOR\text{-}m}$ - wysokość anteny VOR n.p.m. [m].



Rys. 6. Natężenie pola od stacji VOR w funkcji $D_{VOR\text{-}v}/D_{VOR\text{-}z}$

Na rys. 6 przedstawiono zależność E_{VOR} od $D_{VOR\text{-}v}/D_{VOR\text{-}z}$ dla różnych wartości kąta θ. Jeśli θ > 2,5°, to wtedy do wzoru (24) wstawia się θ = 2,5°. Natomiast dla kąta elewacji θ < 0° lub wysokości anteny stacji VOR nad poziomem terenu większej od 7 m E_{VOR} równa się 39 dB(μV/m).

7. POZIOM SYGNAŁU NA WEJŚCIU ODBIORNIKA LOTNICZEGO

Poziom sygnału na wejściu odbiornika pokładowego równoważny wartości natężenia pola na wejściu systemu antenowego dla sygnału UKF FM w pasmie 87,5 ÷ 108 MHz wyznacza się [6] ze wzoru:

$$N = E - 118 - L_s - L(f) - L_a, \tag{26}$$

a dla sygnałów ILS, VOR i zakłóceń A1 w pasmie radionawigacji lotniczej 108 ÷ 118 MHz [6] ze wzoru:

$$N_L = E_L - 118 - L_s - L_a, \tag{27}$$

gdzie :

N - poziom sygnału stacji UKF FM [dBm] na wejściu odbiornika pokładowego samolotu,

N_L - poziom sygnału ILS, VOR lub zakłóceń A1 [dBm] na wejściu odbiornika pokładowego samolotu,

E - natężenie pola [dB(μV/m)] sygnału stacji UKF FM na wejściu systemu antenowego samolotu,

E_L - natężenie pola [dB(μV/m)] sygnału ILS, VOR lub zakłóceń A1 na wejściu systemu antenowego samolotu,

L_a - straty systemu antenowego samolotu (9 dB),

L_s - straty, wynikające z rozdzielenia sygnału (3,5 dB),

$L(f)$ - straty systemu antenowego samolotu na częstotliwości f dla sygnału stacji UKF FM [dB].

W zaleceniu ITU-R IS 1009-1 [6] przyjęto, że straty systemu antenowego samolotu $L(f)$ wynoszą 1,2 dB/MHz.

8. MAKSYMALNA DOPUSZCZALNA MOC STACJI UKF FM

Jak już wspomniano we wstępie, włączenie dodatkowych stacji UKF FM do istniejącej sieci nadawczej wymaga dobrania dla nich odpowiednich kanałów częstotliwościowych i mocy. Dobierając te parametry trzeba respektować stacje radionawigacyjne, telewizyjne i pozostałe stacje UKF FM, zawarte w planie przydziałów częstotliwości, tak aby w obszarze ich działania nie powodować wzrostu zakłóceń.

Ponieważ ochrona obszarów działania ILS i VOR przed zakłóceniami ze strony stacji UKF FM jest niezwykle ważna ze względu na

bezpieczeństwo życia ludzkiego, dlatego o wielkości maksymalnej dopuszczalnej mocy dla stacji UKF FM na poszczególnych częstotliwościach w pierwszej kolejności będą decydować ograniczenia, wynikające z warunków kompatybilności między radiofonią i radionawigacją. Procedurę doboru parametrów dla stacji rozpoczyna się od wyznaczenia maksymalnej dopuszczalnej mocy na wszystkich kanałach częstotliwościowych z zakresu 87,5 ÷ 108 MHz. W obliczeniach tych bierze się pod uwagę zakłócenia typu A i B i uwzględnia się możliwość jednoczesnego ich wystąpienia. Następnie dobiera się dla niej taki kanał częstotliwościowy, który zapewnia pokrycie przez nią zamierzonego obszaru.

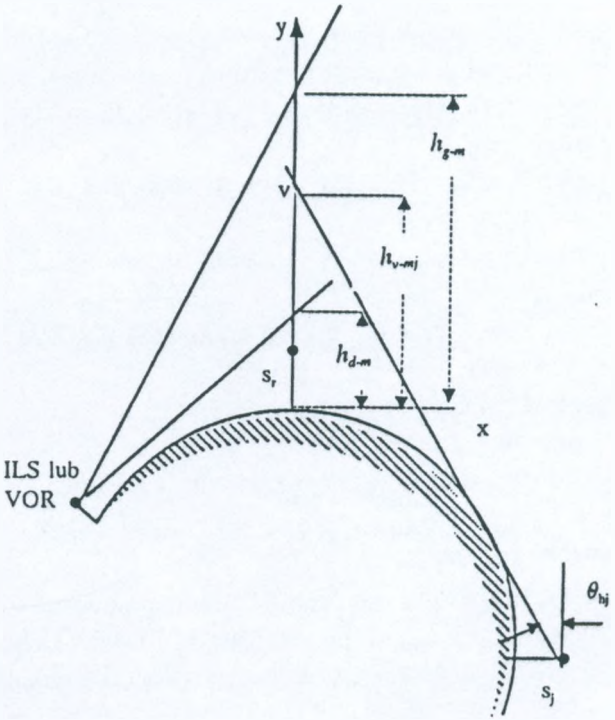
Przy ostatecznym wyborze parametrów dla stacji, oprócz kompatybilności zewnętrznej dotyczącej radionawigacji, trzeba brać również pod uwagę pozostałe ograniczenia, wynikające z warunków kompatybilności wewnętrznej sieci UKF FM oraz zewnętrznej dotyczącej telewizji. Należy liczyć się jednak z tym, że w niektórych przypadkach liczba będących do dyspozycji kanałów częstotliwościowych może być znacznie ograniczona i wtedy może być trudno znaleźć zadowalające rozwiązanie.

Stacje, które mogą przyczynić się do powstania zakłóceń, uwzględnia się w obliczeniach, jeżeli:

- występuje bezpośrednia widoczność między anteną stacji UKF FM i punktem testowym (rys. 7), a dodatkowo przy rozpatrywaniu zakłóceń B1 obliczony poziom sygnału od stacji UKF FM jest większy od wartości, przy której stacje uczestniczą w przemianie częstotliwości;
- poziom sygnału od stacji radiofonicznej przekracza wartość, powodującą wystąpienie zakłóceń A1, A2 lub B2.

Liczba stacji, które mogą się przyczynić do powstania zakłóceń wzrasta wraz ze wzrostem wysokości położenia punktu testowego. Dlatego przy obliczeniach maksymalnej mocy dla stacji planowanej

bierze się pod uwagę punkty testowe położone na większych wysokościach niż dolna granica obszaru działania ILS lub VOR, ale nie większych od górnej granicy przewidzianej dla danego obszaru. Istotne to jest przy rozpatrywaniu zakłóceń typu A2 i B1, gdzie zasięgi zakłócające stacji UKF FM są znaczne.



Rys. 7. Określenie wysokości punktu testowego v oraz dolnej i górnej granicy obszaru działania ILS lub VOR

Dla zakłóceń typu A2 wysokość minimalna położenia punktu testowego v n.p.m. przynależnego do stacji radiofonicznej s_j, w którym mają być spełnione określone warunki kompatybilności, wynosi:

$$h^{*}_{v-m} = \max\left(h_{d-m}, \min\left(h_{g-m}, h_{v-m,j}\right)\right), \tag{28}$$

przy czym:

$$h_{v-m,j} = h_{a-m,j} + \left(\frac{D_{a-v,j}}{4{,}12}\right)^{2} + 10^{3} D_{a-v,j} \operatorname{tg} \theta_{h,j}, \tag{29}$$

gdzie:

h^{*}_{v-m} - wysokość minimalna punktu testowego v n.p.m.[m],

$h_{v-m,j}$ - wysokość najniższa punktu testowego v n.p.m. [m], na jakiej może jeszcze wystąpić sygnał zakłócający od stacji radiofonicznej s_j [m],

h_{d-m} - wysokość dolnej granicy obszaru działania ILS lub VOR n.p.m. [m],

h_{g-m} - wysokość górnej granicy obszaru działania ILS lub VOR n.p.m. [m],

$h_{a-m,j}$ - wysokość zawieszenia anteny stacji radiofonicznej s_j n.p.m. [m],

$D_{a-v,j}$ - odległość punktu testowego v od anteny stacji radiofonicznej s_j [km],

$\theta_{h,j}$ - kąt elewacji dominującej przeszkody przy antenie nadawczej stacji radiofonicznej s_j; sposób wyznaczania tego kąta przedstawiono na rys. 8.

Natomiast w przypadku zakłóceń B1 minimalna wysokość położenia punktu testowego v n.p.m. przynależnego do stacji radiofonicznej s_r, w którym mają być spełnione określone warunki kompatybilności, wynosi:

$$h^{*}_{v-m} = \max\left(h_{d-m}, \min\left(h_{g-m}, h_{v-m,int}\right)\right) \tag{30}$$

przy czym:

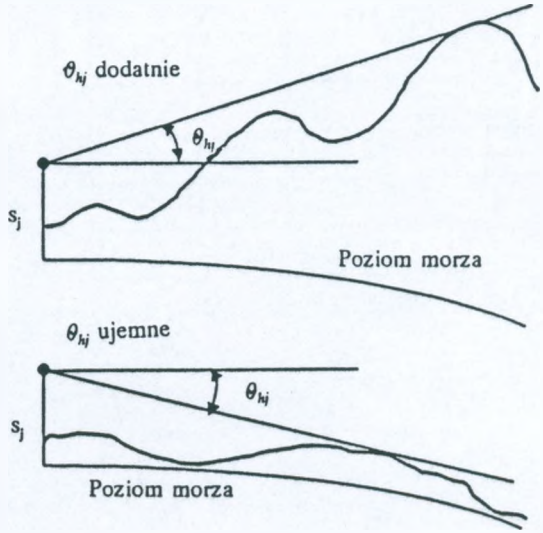
$$h_{v-m,int} = \max_{j}\left\{h_{v-m,j} : j \in U_{int}\right\}, \tag{31}$$

gdzie:

$h_{v-m,int}$ - wysokość najniższa n.p.m. [m], na jakiej może wystąpić produkt intermodulacji od stacji UKF FM, tworzących kom-

binację dwóch lub trzech sygnałów na wejściu odbiornika pokładowego samolotu,

U_{int} - zbiór wskaźników stacji, tworzących produkt intermodulacji.

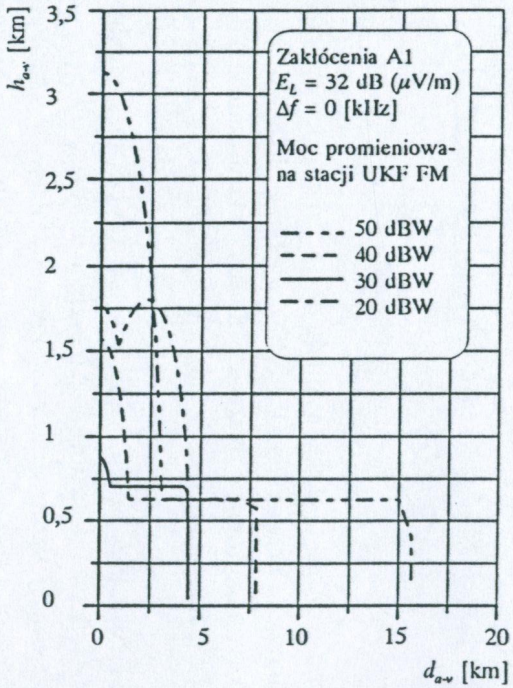


Rys. 8. Sposób określenia kąta dominującej przeszkody

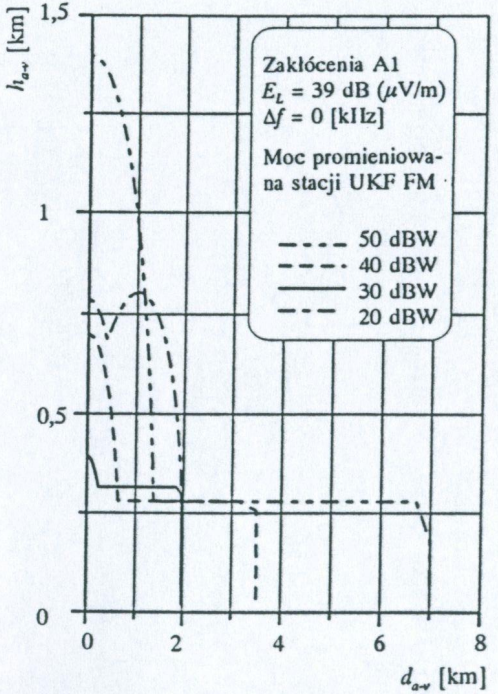
8.1. Zakłócenia A1

Do zakłóceń typu A1 zalicza się produkty intermodulacji trzeciego rzędu, emitowane przez stacje UKF FM wspólnie zlokalizowane. Powstają one w urządzeniach nadawczych przy stosowaniu multipleksera w przypadku pracy dwóch lub więcej stacji ze wspólną anteną.

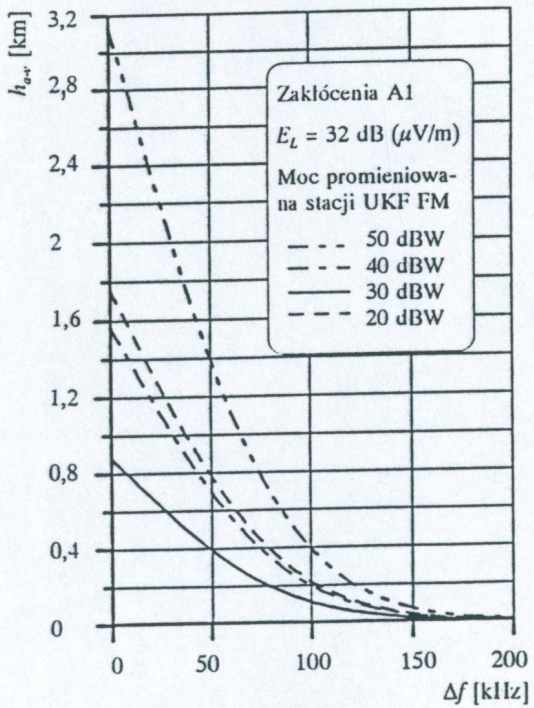
Na rys. 9 i 10 pokazano oddzielnie dla ILS i VOR maksymalne wysokości występowania zakłóceń A1 względem płaszczyzny poziomej przechodzącej przez środek anteny nadawczej. Wykreślono je dla minimalnego natężenia pola E_L sygnału radionawigacyjnego



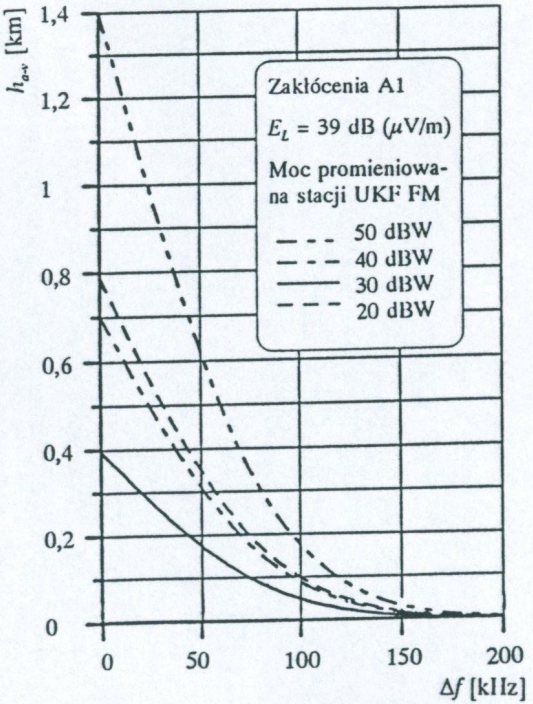
Rys. 9. Wysokość maksymalna występowania zakłóceń A1 w funkcji odległości od stacji UKF FM przy minimalnym natężeniu pola sygnału ILS



Rys. 10. Wysokość maksymalna występowania zakłóceń A1 w funkcji odległości od stacji UKF FM przy minimalnym natężeniu pola sygnału VOR



Rys. 11. Wysokość maksymalna występowania zakłóceń A1 nad stacją UKF FM w funkcji różnicy częstotliwości między sygnałem ILS i produktem intermodulacji przy minimalnym natężeniu pola sygnału ILS



Rys. 12. Wysokość maksymalna występowania zakłóceń A1 nad stacją UKF FM w funkcji różnicy częstotliwości między sygnałem VOR i produktem intermodulacji przy minimalnym natężeniu pola sygnału VOR

oraz częstotliwości produktu intermodulacji $f_{intermod}$ dostrojonego do częstotliwości sygnału radionawigacyjnego f_L. Jak można zauważyć na tych rysunkach, dla stacji o mocy $P \geq 30$ dBW zakłócenia występują najwyżej nad samą stacją, a dla kąta elewacji $\arcsin(1/\pi A_a) < \theta < \arcsin(5/\pi A_a)$ granice obszaru występowania tych zakłóceń przebiegają na stałej wysokości, zależnej od apertury anteny A_a. Dla stacji o mocy $P < 30$ dBW, krzywa wysokości występowania zakłóceń ma dwa maksima. Pierwsze z nich występuje dla kąta elewacji 90°, zaś drugie ma nieco wyższą wysokość i występuje dla kąta elewacji 38,2°.

Przy podanych na rys. 9 i 10 wysokościach występowania zakłóceń osiągnięcie kompatybilności przy dużych mocach stacji UKF FM i małym odstrojeniu częstotliwości produktu intermodulacji od częstotliwości sygnału radionawigacyjnego w obszarze działania ILS jest niemożliwe, a w obszarze działania VOR dopiero wówczas, kiedy wysokość punktu testowego wyznaczonego na podstawie rys. 4 będzie większa od wysokości występowania zakłóceń. Jak widać na rys. 11 i 12, redukcję potencjalnych zakłóceń A1 w punkcie testowym można uzyskać dopiero przez odpowiedni dobór mocy i częstotliwości stacji UKF FM.

Jeżeli częstotliwość produktu intermodulacji promieniowanego przez stacje UKF FM wspólnie zlokalizowane będzie zawierać się w pasmie lotniczym i spełniać nierówność:

$$|f_L - f_{intermod}| \leq 200 \text{ kHz}, \tag{32}$$

to warunkiem koniecznym do osiągnięcia kompatybilności między radiofonią i radionawigacją w obszarze działania ILS lub VOR jest zapewnienie w punkcie testowym ν odpowiedniego stosunku natężenia pola sygnału użytecznego do zakłócającego. Wartość tego stosunku w mierze logarytmicznej powinna być większa od wymaganego współczynnika ochronnego:

$$E_{L,v} - \max_{1 \le i \le n} \{E_{i,v} - T_i\} \ge A, \tag{33}$$

gdzie:

$E_{L,v}$ - natężenie pola [dB(μV/m)] sygnału ILS lub VOR w punkcie testowym v,

A - współczynnik ochronny [dB],

$E_{i,v}$ - natężenie pola [dB(μV/m)] sygnału stacji radiofonicznej s_i w punkcie testowym v,

T_i - tłumienie [dB(μV/m)] składowej produktu intermodulacji wnoszone przez stację radiofoniczną s_i,

n - liczba składowych produktu intermodulacji (2 lub 3).

Wartości tłumienia składowych produktu intermodulacji T_i w zależności od mocy stacji UKF FM zamieszczono w tablicy 5. Natomiast wartość współczynnika ochronnego A w zależności od wartości odstrojenia częstotliwości sygnału radionawigacyjnego od częstotliwości produktu intermodulacji podano w tablicy 6. Jeżeli różnica częstotliwości między sygnałem użytecznym ILS lub VOR a produktem intermodulacji wynosi 0 albo 50 kHz, to wpływ jednoczesnego efektu pojawienia się pozostałych rodzajów zakłóceń uwzględnia się zwiększając o 3 dB współczynnik ochronny [6].

Tablica 5

Tłumienie składowych produktu intermodulacji emitowanych przez stacje UKF FM wspólnie zlokalizowane [6]

Maksymalna moc promieniowana (E.R.P.) [dBW]	Tłumienie T_i względem maksymalnej mocy promieniowanej (E.R.P.) [dB]
≥ 48	85
30	76
< 30	46 + E.R.P. [dBW]

Tablica 6

Wartości współczynnika ochronnego dla zakłóceń A1 [6]

Różnica częstotliwości między sygnałem ILS lub VOR i produktem intermodulacji [kHz]	Współczynnik ochronny [dB]
0	14
50	7
100	-4
150	-19
200	-38

Korzystając z danych zawartych w tabl. 5 oraz wzorów (15) i (33), moc maksymalną, jaką można będzie przydzielić stacji radiofonicznej s_j, aby stacja ta nie powodowała zakłóceń A1 w punkcie testowym v znajdującym się w obszarze działania ILS lub VOR, wyraża się zależnością:

$$P_j^{(m)} = \min\,(100x + 4630;\ 2x + 122;\ x + 85)\,, \tag{34}$$

w której:

$$x = \frac{E_{L,v} - A_m}{k_m} - H_j - V_j + 20\ \lg D_{a-v,j} - 76{,}9\,, \tag{35}$$

przy czym wprowadzony do wzoru (35) współczynnik k_m ma następującą postać:

$$k_m = \frac{\max\limits_{1 \le i \le n} \{E_{i,v}^{(m)} - T_i^{(m)}\}}{E_{J,v}^{(m)} - T_J^{(m)}} \tag{36}$$

gdzie:

$P_j^{(m)}$ - moc maksymalna [dBW], jaką można będzie przydzielić stacji radiofonicznej s_j w przypadku m-tej kombinacji częstotliwości tworzącej produkt intermodulacji,

A_m - współczynnik ochronny [dB] w przypadku m-tej kombinacji częstotliwości tworzącej produkt intermodulacji,

H_j - współczynnik kierunkowości anteny w płaszczyźnie poziomej stacji s_j [dB],

V_j - współczynnik kierunkowości anteny w płaszczyźnie pionowej stacji s_j [dB],

$D_{a\text{-}\nu,j}$ - odległość punktu testowego ν od anteny stacji radiofonicznej s_j [km],

$E_{i,\nu}^{(m)}$ - natężenie pola [dB(μV/m)] sygnału stacji radiofonicznej s_i w punkcie testowym ν, w przypadku m-tej kombinacji częstotliwości tworzącej produkt intermodulacji,

$T_i^{(m)}$ - tłumienie [dB(μV/m)] składowej produktu intermodulacji wnoszone przez stację radiofoniczną s_i, w przypadku m-tej kombinacji częstotliwości.

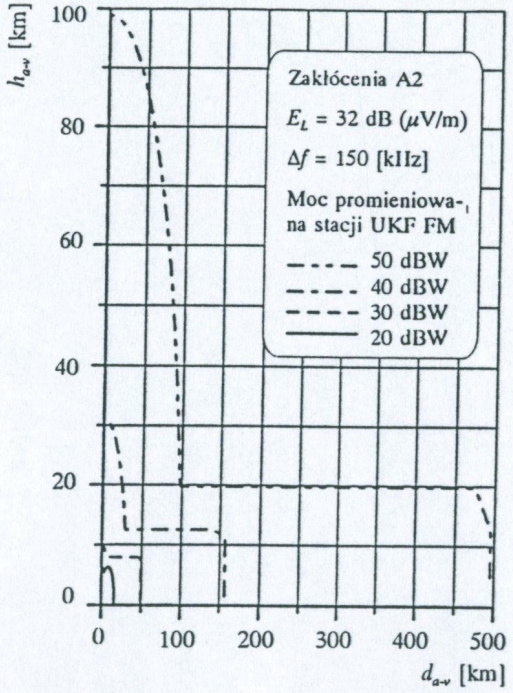
Wyznaczając wartości mocy $P_j^{(m)}$ dla poszczególnych kombinacji częstotliwości tworzących produkt intermodulacji, gdzie $1 \leq m \leq q$, otrzyma się zbiór wartości mocy $P_j^{(1)}, P_j^{(2)}, ..., P_j^{(q)}$. Następnie na podstawie tych danych wyznacza się wartość mocy maksymalnej $P_{j,\max}$ dla stacji s_j z poniżej podanego wzoru:

$$P_{j,\max} = \min\left(P_j^{(1)}, P_j^{(2)}, ..., P_j^{(q)}\right). \tag{37}$$

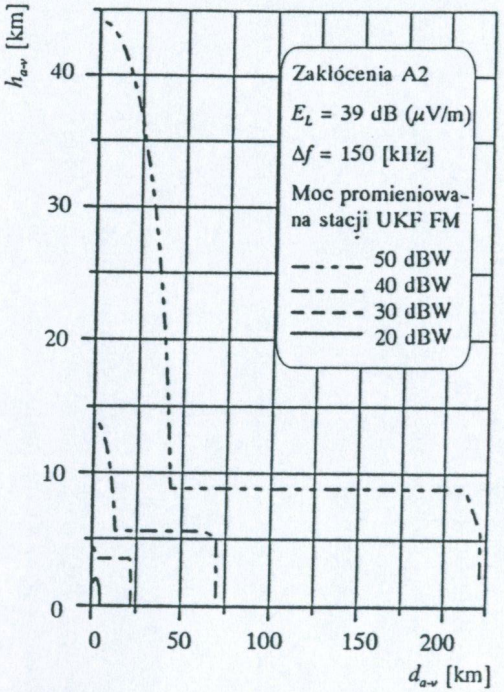
8.2. Zakłócenia A2

Stacje UKF FM oprócz sygnału pożądanego emitują także składowe niepożądane w sąsiedztwie kanału podstawowego. Stanowić one mogą przyczynę powstawania zakłóceń A2, jeżeli częstotliwości tych składowych będą zawierać się w pasmie lotniczym i spełniać warunek:

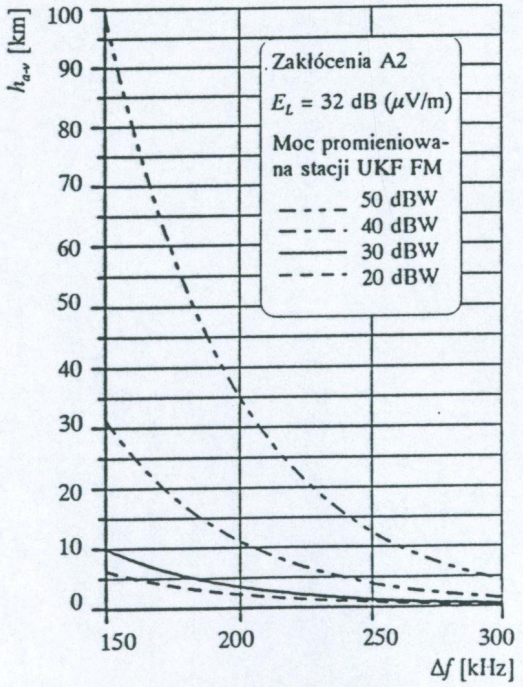
$$f_L - f \leq 300 \text{ kHz}, \tag{38}$$



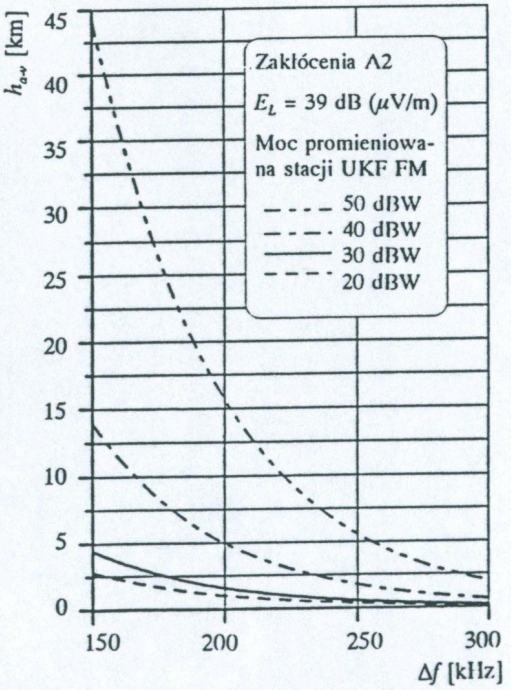
Rys. 13. Wysokość maksymalna występowania zakłóceń A2 w funkcji odległości od stacji UKF FM przy minimalnym natężeniu pola sygnału ILS



Rys. 14. Wysokość maksymalna występowania zakłóceń A2 w funkcji odległości od stacji UKF FM przy minimalnym natężeniu pola sygnału VOR



Rys. 15. Wysokość maksymalna występowania zakłóceń A2 nad stacją UKF FM w funkcji różnicy częstotliwości między sygnałami ILS i UKF FM przy minimalnym natężeniu pola sygnału ILS



Rys. 16. Wysokość maksymalna występowania zakłóceń A2 nad stacją UKF FM w funkcji różnicy częstotliwości między sygnałami stacji VOR i UKF FM przy minimalnym natężeniu pola sygnału VOR

gdzie:

f_L - częstotliwości stacji ILS lub VOR,

f - częstotliwości stacji UKF FM.

Na rys. 13 i 14 pokazano maksymalne wysokości występowania zakłóceń A2 względem płaszczyzny poziomej przechodzącej przez środek anteny nadawczej. Wysokości te wykreślono dla minimalnego natężenia pola zabezpieczającego pracę systemów radionawigacyjnych ILS i VOR. Jak widać na tych rysunkach, wysokości obszaru występowania zakłóceń A2 znacznie przekraczają wysokości punktów testowych, w których mają być spełnione określone wymagania podane w zaleceniu ITU-R IS 1009-1 [6]. Spełnienie warunków kompatybilności można osiągnąć jedynie przez odpowiedni dobór mocy i częstotliwości stacji UKF FM (patrz rys. 15 i 16).

Warunkiem niezbędnym do osiągnięcia kompatybilności między radiofonią i radionawigacją, podobnie jak w przypadku zakłóceń A1, jest zapewnienie odpowiedniego stosunku sygnału użytecznego do zakłócającego w punkcie testowym. Wyrażając ten stosunek w mierze logarytmicznej otrzyma się:

$$E_{L,\nu} - E_{\nu} \geq A\,, \tag{39}$$

gdzie:

$E_{L\nu}$ - natężenie pola sygnału ILS lub VOR w punkcie testowym ν [dB(μV/m)],

E_{ν} - natężenie pola sygnału UKF FM w punkcie testowym ν [dB(μV/m)],

A - współczynnik ochronny [dB].

Korzystając ze wzorów (15) i (39), moc maksymalną, jaką można będzie przydzielić stacji radiofonicznej s_j, aby stacja ta nie powodowała zakłóceń A2 w punkcie testowym ν znajdujących się w obszarze działania ILS lub VOR, wyraża się zależnością:

$$P_{j,\max} = E_{L,\nu} - H_j - V_j - A + 20 \lg D_{a-\nu,j} - 76{,}9\,, \tag{40}$$

gdzie:

$P_{j,max}$ - moc maksymalna, jaką można przydzielić stacji radiofonicznej s_j [dBW],

H_j - współczynnik kierunkowości anteny w płaszczyźnie poziomej stacji s_j [dB],

V_j - współczynnik kierunkowości anteny w płaszczyźnie pionowej stacji s_j [dB],

$D_{a-v,j}$ - odległość punktu testowego v od anteny stacji radiofonicznej s_j [km].

Wartość współczynnika ochronnego A w zależności od wartości odstrojenia częstotliwości sygnału radionawigacyjnego od częstotliwości sygnału radiofonicznego podano w tablicy 7.

Tablica 7

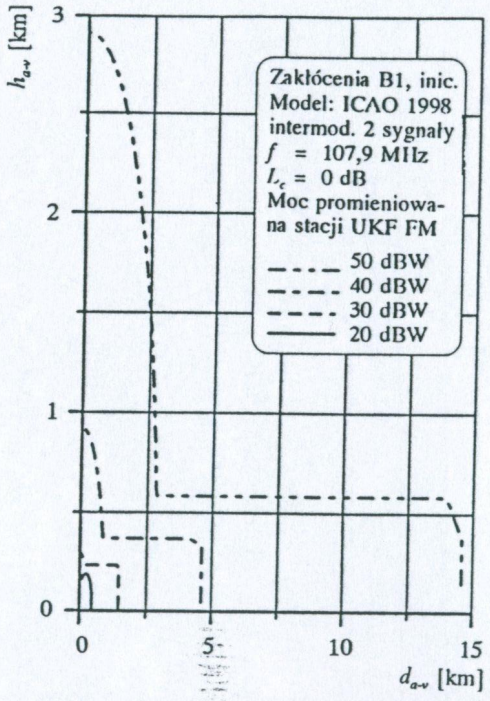
Wartości współczynnika ochronnego dla zakłóceń A2 [6]

Różnica częstotliwości między sygnałami ILS lub VOR i UKF FM [kHz]	Współczynnik ochronny [dB]
150	-41
200	-50
250	-59
300	-68

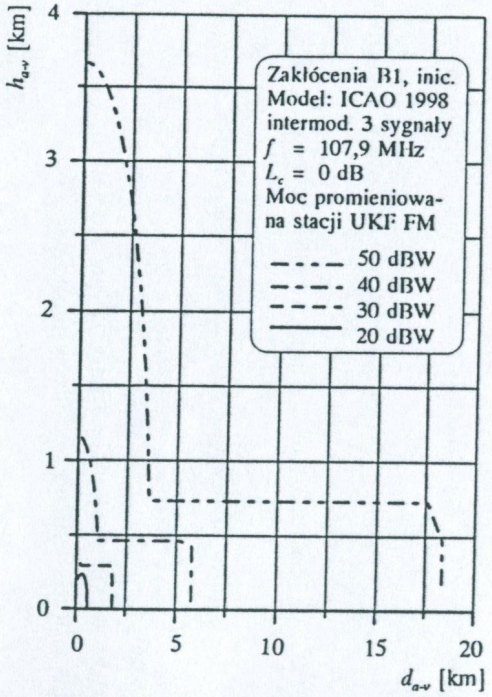
Ze wzoru (40) wynika, że przy odstrojeniu 300 kHz moc maksymalna, jaką można przydzielić stacji UKF FM w strefie ścieżki schodzenia samolotu, wynosi 14 dBW, a poza tą strefą w obszarze działania ILS - 32 dBW.

8.3. Zakłócenia B1

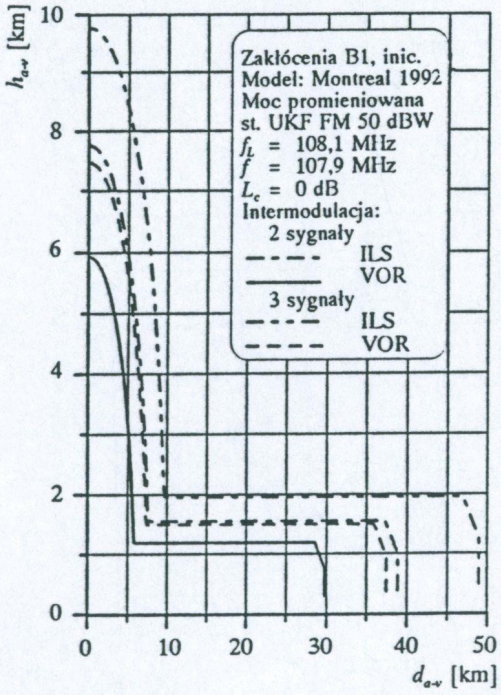
W analizie zakłóceń B1 uwzględnia się tylko te stacje UKF FM, których sygnały na wejściu odbiornika pokładowego samolotu



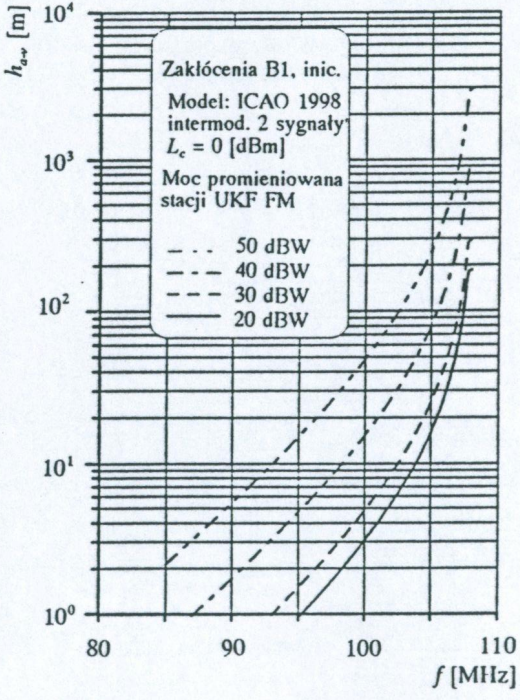
Rys. 17. Wysokość maksymalna występowania sygnału inicjującego zakłócenia B1 w funkcji odległości od stacji UKF FM przy intermodulacji dwusygnałowej



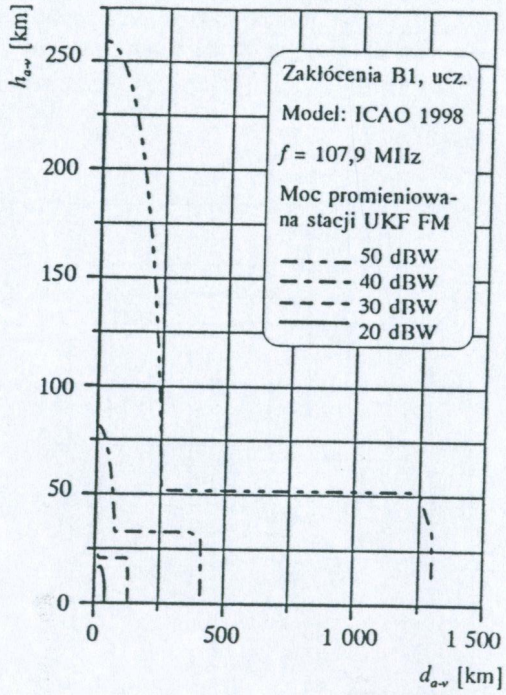
Rys. 18. Wysokość maksymalna występowania sygnału inicjującego zakłócenia B1 w funkcji odległości od stacji UKF FM przy intermodulacji trójsygnałowej



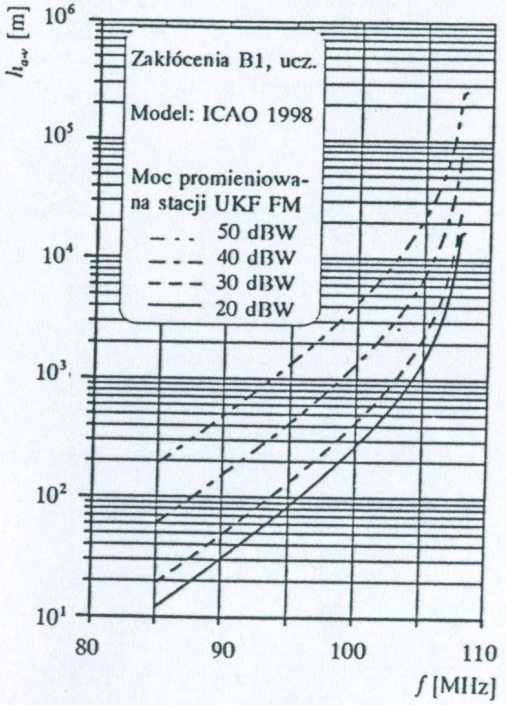
Rys. 19. Wysokość maksymalna występowania sygnału inicjującego zakłócenia B1 w funkcji odległości od stacji UKF FM przy intermodulacji dwu- i trójsygnałowej



Rys. 20. Wysokość maksymalna występowania sygnału inicjującego zakłócenia B1 nad stacją UKF FM w funkcji częstotliwości przy intermodulacji dwusygnałowej



Rys. 21. Wysokość maksymalna występowania sygnału uczestniczącego w zakłóceniach B1 w funkcji odległości od stacji UKF FM



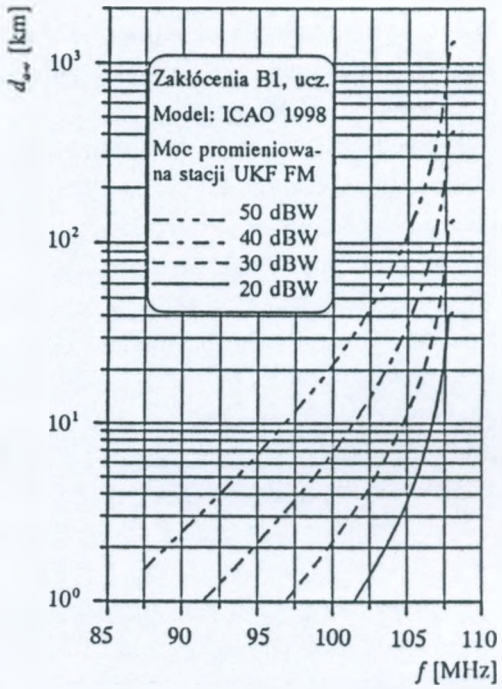
Rys. 22. Wysokość maksymalna występowania sygnału uczestniczącego w zakłóceniach B1 nad stacją UKF FM w funkcji częstotliwości

w punkcie testowym v przekraczają określone w zaleceniu ITU-R IS 1009-1 wartości N_{inic} dla sygnału inicjującego zakłócenia i N_{ucz} dla sygnału uczestniczącego w zakłóceniach.

Na rys. 17 i 18 przedstawiono maksymalne wysokości występowania sygnału inicjującego zakłócenia B1 względem płaszczyzny poziomej przechodzącej przez środek anteny nadawczej. Z rysunków tych wynika, że stacjami inicjującymi zakłócenia mogą być jedynie stacje znajdujące się w odległości do 20 km od punktu testowego. Dotyczy to modelu odbiornika ICAO 1998. Dla modelu odbiornika Montreal 1992 odległości te będą znacznie większe (rys. 19). Jeśli punkt testowy v będzie znajdować się na wysokości 300 m nad anteną stacji UKF FM, to wtedy stacjami inicjującymi zakłócenia B1 będą stacje o mocy $P > 24$ dBW i częstotliwości f > 105,3 MHz w przypadku dwóch sygnałów na wejściu odbiornika lotniczego (rys. 20) oraz stacje o mocy $P > 22$ dBW i częstotliwości f > 104,8 MHz w przypadku trzech sygnałów. Dla punktu testowego położonego w strefie ścieżki schodzenia samolotu do lądowania, stacjami inicjującymi zakłócenia będą wszystkie stacje o mocy większej od -5 dBW.

Obszar występowania sygnału uczestniczącego w zakłóceniach (rys. 21) jest wielokrotnie większy niż w przypadku sygnału inicjującego zakłócenia, stąd do zbioru stacji uczestniczących w zakłóceniach należeć będzie duża liczba stacji UKF FM ze znacznej odległości od punktu testowego i znacznie szerszego przedziału częstotliwości (rys. 22), które wraz z sygnałem inicjującym zakłócenia będą wytwarzać w odbiorniku pokładowym samolotu dużą liczbę produktów intermodulacji. Liczba tych stacji zależeć będzie od maksymalnej wysokości występowania sygnału inicjującego zakłócenia oraz od częstotliwości i mocy stacji uczestniczących w zakłóceniach (rys. 23).

Do zbioru stacji uczestniczących w zakłóceniach w punkcie testowym v przynależnym do stacji s_r inicjującej zakłócenia intermodulacyjne, zalicza się stacje, dla których poziom sygnału na wejściu od-



Rys. 23. Odległość stacji UKF FM uczestniczącej w zakłóceniach B1 od punktu testowego w funkcji częstotliwości przy różnych mocach

biornika pokładowego samolotu $N \geq N_{ucz}$ i dla których występuje bezpośrednia widoczność między anteną stacji UKF FM a punktem testowym ν, tzn. kiedy zachodzi:

$$d_{ucz-\nu,j} \leq 4{,}12 \left(\sqrt{h_{ucz-m,j}} + \sqrt{h_{inic-m,r}} \right), \tag{41}$$

pod warunkiem, że najniższa wysokość, na której może pojawić się sygnał od stacji uczestniczącej w zakłóceniach

$$h_{\nu-m,j} = h_{ucz-m,j} + \left(\frac{d_{ucz-\nu,j}}{4{,}12} \right)^2 + 10^3 \, d_{ucz-\nu,j} \operatorname{tg} \theta_{h,j} \tag{42}$$

znajdzie się w obszarze działania ILS lub VOR, co można zapisać w postaci:

$$h_{d-m} \leq h_{v-m,j} \leq h_{g-m}, \tag{43}$$

gdzie:

$h_{ucz\text{-}m,j}$ - wysokość zawieszenia anteny stacji s_j n.p.m.[m], uczestniczącej w zakłóceniach [m],

$h_{inic\text{-}m,r}$ - wysokość maksymalna n.p.m. [m] występowania sygnału inicjującego zakłócenia B1 stacji s_r,

$d_{ucz\text{-}v,j}$ - odległość w poziomie punktu testowego v od anteny stacji s_j uczestniczącej w zakłóceniach [km],

$\theta_{h,j}$ - kąt elewacji dominującej przeszkody przy antenie nadawczej stacji radiofonicznej s_j (rys. 8),

h_{d-m} - wysokość dolnej granicy obszaru działania ILS lub VOR n.p.m. [m] (rys. 7),

h_{g-m} - wysokość górnej granicy obszaru działania ILS lub VOR n.p.m.[m] (rys. 7).

Kompatybilność między radiofonią i radionawigacją można osiągnąć wówczas, gdy w punkcie testowym v zaistnieją odpowiednie warunki częstotliwościowe i amplitudowe. Warunkiem częstotliwościowym będzie wielkość odstrojenia częstotliwości produktu intermodulacji f_{intmod} od częstotliwości sygnału radionawigacyjnego f_L. Warunek ten dla modelu odbiornika ICAO 1998 wyrazi się wzorem:

$$|f_L - f_{intmod}| \leq 150 \text{ kHz}, \tag{44}$$

gdzie:

f_L - częstotliwość ILS lub VOR [MHz],

f_{intmod} - częstotliwość produktu intermodulacji [MHz], w punkcie v przynależnym do stacji s_r.

Z kolei warunki amplitudowe (8) i (9) posłużą do wyznaczenia mocy maksymalnej $P_{i,max}$, jaką można będzie przydzielić stacji plano-

wanej s_i. Wielkość tej mocy jest uwarunkowana osiągnięciem kompatybilności:

1) w punkcie testowym ε przynależnym do stacji s_i inicjującej zakłócenia intermodulacyjne, gdzie stacjami uczestniczącymi w tych zakłóceniach są stacje:
   - s_j o wskaźniku $j \in U_{i(\varepsilon)}$ dla dwóch sygnałów na wejściu odbiornika lotniczego,
   - s_j, s_k o wskaźnikach $j,k \in U_{i(\varepsilon)}$ dla trzech sygnałów,
2) w punktach testowych γ przynależnych do stacji s_j inicjujących zakłócenia intermodulacyjne, gdzie:
   - stacją uczestniczącą w tych zakłóceniach dla dwóch sygnałów jest stacja planowana s_i o wskaźniku $i \in U_{j(\gamma)}$,
   - stacjami uczestniczącymi w tych zakłóceniach dla trzech sygnałów są stacje s_i, s_q o wskaźnikach $i,q \in U_{j(\gamma)}$.

W pierwszym przypadku kompatybilność zostanie osiągnięta w punkcie testowym ε, jeśli moc P_i stacji planowanej s_i będzie spełniać warunek $P_i \le P_i^{(1)}$, gdzie $P_i^{(1)}$ jest mocą maksymalną, jaką można przydzielić w tym przypadku stacji. Wartość tej mocy wyznacza się ze wzoru:

$$P_i^{(1)} = \min\left\{\min_j \{P_{i(\varepsilon),j} : j \in U_{i(\varepsilon)}\},\ \min_{j,k} \{P_{i(\varepsilon),j,k} : j,k \in U_{i(\varepsilon)}\}\right\}, \quad (45)$$

w którym:

$$P_{i(\varepsilon),j} = G_{i,i(\varepsilon)} + \begin{cases} 0{,}5(-N_{j(\varepsilon)} + 3W_o + 2C_i + C_j - K + L_{c(\varepsilon)} - S); & \text{dla } f_i > f_j \\ -2N_{j(\varepsilon)} + 3W_o + 2C_j + C_i - K + L_{c(\varepsilon)} - S \ ; & \text{dla } f_i < f_j \end{cases}, \quad (46)$$

$$P_{i(\varepsilon),j,k} = G_{i,i(\varepsilon)} - N_{j(\varepsilon)} - N_{k(\varepsilon)} + 3W_o + C_i + C_j + C_k - K - 6 + L_{C(\varepsilon)} - S, \quad (47)$$

przy czym:

$$G_{i,i(\varepsilon)} = 53{,}6 - H_i - V_i + L(f_i) + 20 \lg D_{i\text{-}i(\varepsilon)}, \quad (48)$$

oraz

$$N_{r(\varepsilon)} = P_r + H_r + V_r - L(f_r) - 20 \lg D_{r-i(\varepsilon)} - 53{,}6; \text{ dla } r = j,k, \quad (49)$$

i

$$C_r = B \lg \frac{\max(f_g; f_o - f_r)}{f_g}; \quad \text{dla } r = i,j,k, \quad (50)$$

gdzie:

$U_{i(\varepsilon)}$ - zbiór wskaźników stacji uczestniczących w zakłóceniach intermodulacyjnych w punkcie testowym ε przynależnym do stacji s_i inicjującej zakłócenia,

W_o - współczynnik, uwzględniający odstrojenie produktu intermodulacji od sygnału radionawigacyjnego (tabl. 2),

$L_{c(\varepsilon)}$ - współczynnik [dB], uwzględniający zmianę poziomu sygnału ILS lub VOR w odniesieniu do odpowiedniego minimalnego poziomu zabezpieczającego pracę tych systemów w punkcie testowym ε,

f_r - częstotliwość stacji s_r dla $r = i, j, k$ [MHz],

H_r - współczynnik kierunkowości anteny w płaszczyźnie poziomej stacji s_r [dB],

V_r - współczynnik kierunkowości anteny w płaszczyźnie pionowej stacji s_r [dB],

$L(f_r)$ - straty systemu antenowego samolotu na częstotliwości f_r dla sygnału stacji radiofonicznej s_r [dB],

$D_{r-i(\varepsilon)}$ - odległość punktu testowego ε przynależnego do stacji s_i od anteny stacji s_r [km],

K,S,B,f_g,f_o - stałe zależne od modelu odbiornika lotniczego (tabl. 1).

W drugim przypadku kompatybilność zostanie osiągnięta w punkcie testowym γ przynależnym stacji s_j, jeśli moc P_i stacji planowanej s_i spełniać będzie warunek $P_i \le P_i^{(2)}$, gdzie $P_i^{(2)}$ jest mocą maksymalną, jaką można przydzielić w tym przypadku stacji. Wartość tej mocy wyznacza się ze wzoru:

$$P_i^{(2)} = \min\left\{\min_j \{P_{i,j(\gamma)} : i \in U_{j(\gamma)}\},\ \min_{j,q} \{P_{i,j(\gamma),q} : i,q \in U_{j(\gamma)}\}\right\}_j, \quad (51)$$

w którym:

$$P_{j,j(\gamma)} = G_{j,j(\gamma)} + \begin{cases} 0{,}5(-N_{j(\gamma)} + 3W_o + 2C_i + C_j - K + L_{c(\gamma)} - S); & \text{dla } f_j > f_i \\ -2N_{j(\gamma)} + 3W_o + 2C_j + C_i - K + L_{c(\gamma)} - S \quad ; & \text{dla } f_j < f_i \end{cases}, \quad (52)$$

$$P_{j,j(\gamma),q} = G_{j,j(\gamma)} - N_{i(\gamma)} - N_{q(\gamma)} + 3W_o + C_i + C_j + C_q - K - 6 + L_{c(\gamma)} - S, \quad (53)$$

przy czym:

$$G_{j,j(\gamma)} = 53{,}6 - H_j - V_j + L(f_j) + 20 \lg D_{j\text{-}j(\gamma)}, \quad (54)$$

oraz

$$N_{r(\gamma)} = P_r + H_r + V_r - L(f_r) - 20 \lg D_{r\text{-}j(\gamma)} - 53{,}6; \text{ dla } r = i,q, \quad (55)$$

i

$$C_r = B \lg \frac{\max(f_g; f_o - f_r)}{f_g}; \quad \text{dla } r = i,j,q, \quad (56)$$

gdzie:

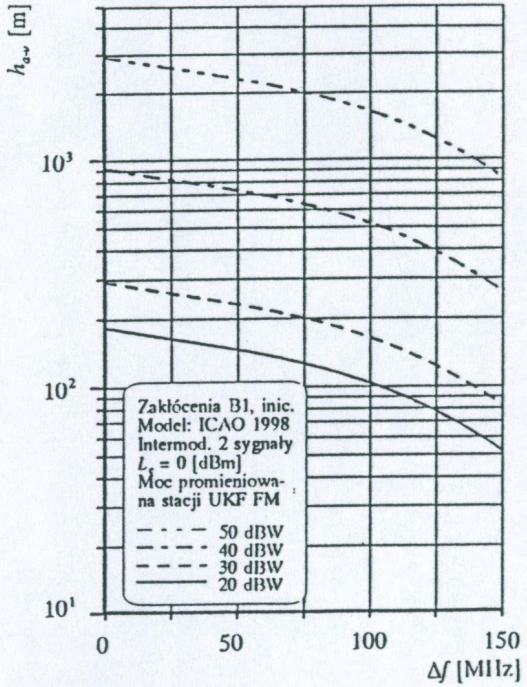
$U_{j(\gamma)}$ - zbiór wskaźników stacji, w których stacja s_i uczestniczy w zakłóceniach intermodulacyjnych w punkcie testowym γ przynależnym do stacji s_j inicjującej zakłócenia,

$L_{c(\gamma)}$ - współczynnik, uwzględniający zmianę poziomu sygnału radionawigacyjnego w punkcie testowym γ [dB],

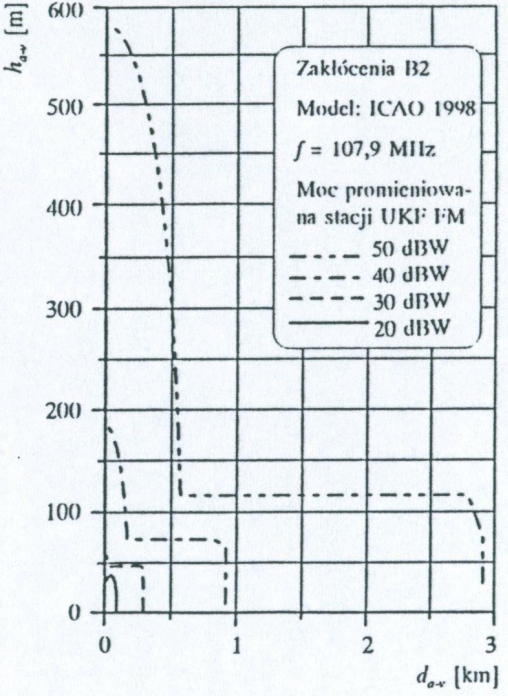
f_r - częstotliwość stacji s_r dla $r = i, j, q$ [MHz],

$D_{r\text{-}j(\gamma)}$ - odległość punktu testowego γ przynależnego do stacji s_j od anteny stacji s_r [km].

Moc maksymalna $P_{i,\max}$, jaką można będzie przydzielić stacji s_i jest uwarunkowana osiągnięciem kompatybilności w punktach testowych ε i γ. Dla danych wartości mocy $P_i^{(1)}$ i $P_i^{(2)}$ moc maksymalną wyznacza się ze wzoru:



Rys. 24. Wysokość maksymalna występowania sygnału inicjującego zakłócenia B1 nad stacją UKF FM w funkcji różnicy częstotliwości między sygnałem ILS lub VOR i produktem intermodulacji



Rys. 25. Wysokość maksymalna występowania zakłóceń B2 w funkcji odległości od stacji UKF FM dla odbiornika ICAO 1998

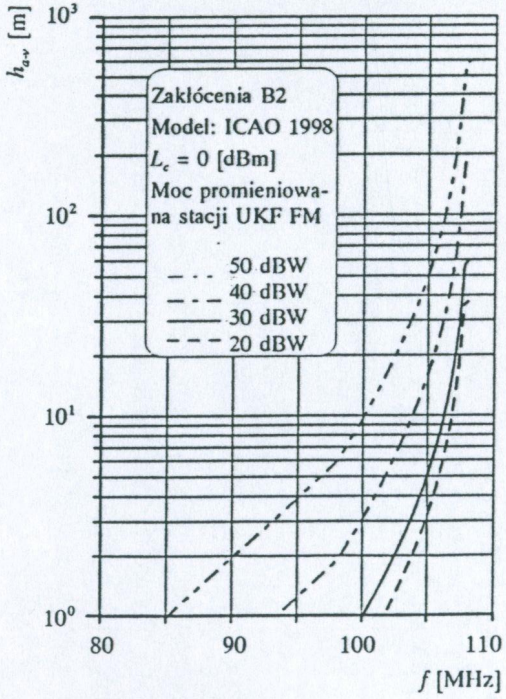
$$P_{i,\max} = \min\left(P_i^{(1)}, P_i^{(2)}\right). \tag{57}$$

W niektórych przypadkach uzyskanie zadowalającej wartości mocy maksymalnej $P_{i,\max}$ dla stacji s_i może okazać się bardzo trudne lub nawet niemożliwe. Wtedy należy poszukiwać nowych częstotliwości dla niektórych stacji uczestniczących w zakłóceniach. Odstrajając częstotliwość produktu intermodulacji od częstotliwości ILS lub VOR, można uzyskać niższą maksymalną wysokość występowania sygnału inicjującego nad anteną stacji UKF FM (rys. 24), a co się z tym wiąże mniejszą liczbę stacji uczestniczących w zakłóceniach, a tym samym mniejszą liczbę produktów intermodulacji.

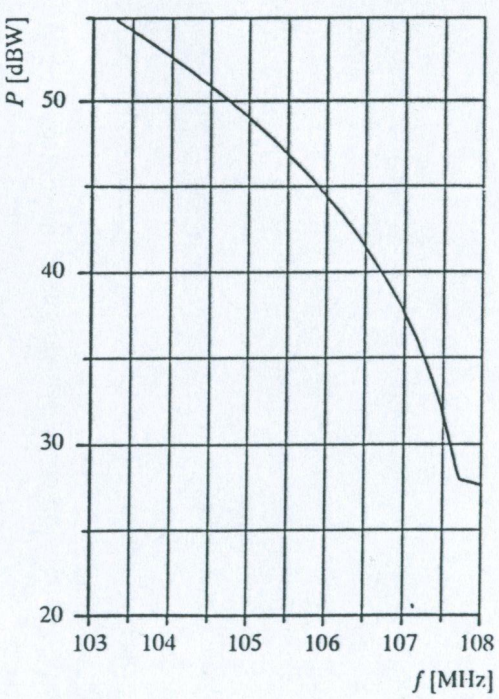
8.4. Zakłócenia B2

Silny sygnał pochodzący od stacji UKF FM i docierający do odbiornika lotniczego może powodować tzw. blokowanie. Zjawisko to wystąpi, jeżeli poziom sygnału N stacji UKF FM na wejściu odbiornika pokładowego samolotu przekroczy określony poziom $N_{\max}$ podany w zaleceniu ITU-R IS 1009-1. Na rys. 25 pokazano obszar występowania tego typu zakłóceń wokół stacji UKF FM przy różnych mocach dla modelu odbiornika ICAO 1998. Obszar ten w porównaniu z innymi zakłóceniami omówionymi poprzednio nie jest duży, a wysokość jego nad stacją nie przekracza 600 m. Rozważając dla VOR najgorszy przypadek występowania zakłóceń w punkcie testowym nad stacją UKF FM, tzn. 300 m nad jej anteną, blokowanie odbiornika pokładowego samolotu może mieć miejsce dla stacji o mocy $P > 44$ dBW i częstotliwości $f \geq 107{,}4$ MHz (rys. 26).

Korzystając ze wzorów (15) i (28), moc maksymalną, jaką można będzie przydzielić stacji radiofonicznej s_j, aby nie występowało blokowanie odbiornika pokładowego samolotu w punkcie testowym v znajdującym się w obszarze pokrycia operacyjnego ILS lub VOR, wyraża się zależnością:



Rys. 26. Wysokość maksymalna występowania zakłóceń B2 nad stacją UKF FM w funkcji częstotliwości



Rys. 27. Moc dopuszczalna stacji UKF FM w strefie ścieżki schodzenia samolotu do lądowania w funkcji częstotliwości przy L_c = 7 dB

$$P_{j,\max} = N_{\max} - H_j - V_j + L(f_j) + 20 \lg D_{a\text{-}v,j} + 53{,}6\,, \qquad (58)$$

gdzie:

$P_{j\max}$ - moc maksymalna, jaką można przydzielić stacji radiofonicznej s_j [dBW],

N_{max} - poziom maksymalny sygnału stacji UKF FM [dBm], po przekroczeniu którego występuje blokowanie odbiornika pokładowego samolotu,

H_j - współczynnik kierunkowości anteny w płaszczyźnie poziomej stacji s_j [dB],

V_j - współczynnik kierunkowości anteny w płaszczyźnie pionowej stacji s_j [dB],

$L(f_j)$ - straty systemu antenowego samolotu na częstotliwości f_j [dB],

$D_{a\text{-}v,j}$ - odległość punktu testowego v od anteny stacji radiofonicznej s_j [km].

Jeżeli stacja UKF FM będzie zlokalizowana w strefie ścieżki schodzenia samolotu w obszarze działania ILS, to ze wzoru (58) wynika, że blokowanie odbiornika pokładowego może już mieć miejsce na znacznie niższych częstotliwościach niż dla punktu testowego znajdującego się poza tą strefą. Dopuszczalną moc dla stacji lokalizowanych w strefie ścieżki schodzenia w zależności od częstotliwości pokazano na rys. 27.

9. ZAKOŃCZENIE

W niniejszym artykule poinformowano o zachodzących zjawiskach przy współistnieniu radiofonii UKF FM i radionawigacji lotniczej w sąsiednich pasmach oraz wskazano, jak dobierać moc stacji UKF FM, a także jak redukować występujące zakłócenia w obszarze działania ILS i VOR.

Zaproponowane w tym opracowaniu wzory na moc maksymalną stacji UKF FM umożliwiają przeanalizowanie jej wartości w zadanym zakresie częstotliwości. Takie podejście ma tę zaletę, że już na samym początku planowania stacji UKF FM wyklucza się wszystkie te częstotliwości, na których stacja ta mogłaby zakłócić pracę systemów radionawigacyjnych ILS i VOR. Umożliwia to bardziej racjonalną gospodarkę dostępnym widmem częstotliwości.

Stacje UKF FM o częstotliwościach znajdujących się w pobliżu górnej granicy zakresu stwarzają największe niebezpieczeństwo wystąpienia zakłóceń. Jeżeli stacje takie będą znajdować się nawet w znacznej odległości od obszarów działania ILS lub VOR na terenie naszego kraju, a nawet na terenie krajów ościennych w znacznej odległości od naszej granicy, to należy je uwzględniać w obliczeniach w przypadku zakłóceń A2 i B1. Ważne jest również, aby na tego typu stacje zwracać szczególną uwagę w trakcie uzgodnień międzynarodowych.

Wydaje się, że dla większości stacji UKF FM - planowanych w latach, kiedy obowiązywał model odbiornika lotniczego Montreal 1992 - warunki kompatybilności między radiofonią i radionawigacją lotniczą powinny być także spełnione dla modelu odbiornika lotniczego ICAO 1998.

WYKAZ LITERATURY

1. CCIR Doc. Task Group 12-1/TEMP/4(Rev.1)-E: Interference mechanisms, system parameters and compatibility assessment criteria. 11 June 1991.
2. CCIR Doc. 12-1/36-E: Calculation of VOR field strength at test points. 2 Jule 1992.
3. CCIR Rap. 946: Frequency-planning constrains on FM sound broadcasting in band 8 (VHF). Geneva 1982.

4. International standards, recommended practices and procedures for air navigation services: aeronautical telecommunications. Annex 10 to the Convention on I Civil Aviation, vol. I. International Civil Aviation Organization, Montreal (Canada) 1985.
5. ITU: Final acts of the Regional administrative conference for the planning of VHF sound broadcasting (region 1 and part of REGION 3). Geneva 1984.
6. ITU-R Rec. IS 1009-1: Compatibility between the sound-broadcasting service in the band of about 87-108 MHz and the aeronautical services in the band 108-137 MHz. 1996.

Збигнев Рымарович

ОГРАНИЧЕНИЕ МОЩНОСТИ РАДИОСТАНЦИИ УКВ-ЧМ ДЛЯ ЗАЩИТЫ СЛУЖБ АВИАЦИИ ОТ РАДИОПОМЕХ

Р е з ю м е

Рассмотрено вопросы радиопомех создаваемых УКВ-ЧМ радиостанциями работающих в диапазоне 87,5 - 108 МГц в приемных устройствах аэронавигации ILS и VOR. Дается в сокращении характеристика типов возникающих радиопомех и представлено способы их анализа с приведением соответствующих формул. Определено зоны возникновения потенциальных радиопомех вблизи УКВ-ЧМ радиостанций в зависимости от излучаемой мощности и частоты сигнала для модели бортового приемника ICAO, Приложение 10, 1998 г. Даются формулы для расчета максимально допустимой мощности радиостанции УКВ-ЧМ при которой выполняются условия электромагнитной совместимости этих двух служб в определенных измерительных точках в зоне действия ILS и VOR. Эти формулы позволяют сделать анализ мощности и частоты радиостанции УКВ-ЧМ позволяющий на исключение всех мешающих частот в самом начале процесса планирования этой радиостанции.

Zbigniew Rymarowicz

THE LIMITATION OF POWER OF UKF FM STATION FOR PROTECTION OF AVIATION SERVICES AGAINST THE PERTURBATIONS

Summary

The problem of existence of perturbation in reception equipment of the air radionavigation services ILS and VOR resulted from the signals of UKF FM station of frequency band of 87,5 - 108 MHz as well as the methods of protection of this services against the perturbations are presented. The types of perturbations are briefly characterized and the manner of their analyse is presented too with suitable relations between them. The areas of appearance of potential perturbations are specified for the environment of UKF FM station depending of power and frequency using a model of deck receiver of aircraft ICAO, according to the Annexe 10, 1998. The equations for maximal admissible power of UKF FM station which comply the conditions of compatibility between FM radiophony and radionawigation of aviation are proposed for the defined testing points on area of ILS and VOR. The equations are giving the possibility to analyse the value of power for UKF FM station in given band of frequency making possible an exclusion already just at the beginning of planning of the station - of all the frequencies are in collision.

Zbigniew Rymarowicz

LES LIMITATIONS DE LA PUISSANCE D'UNE STATION UKF FM POUR PROTEGER DES SERVICES D'AVIATION CONTRE LES PERTURBATIONS

Résumé

Il y a une présentation des problèmes d'existence des perturbations dans les équipements de réception exploités par les services de la radionavigation

de l'aviation ILS et VOR qui résultent des signaux de la station UKF FM de la bande de 87,5 au 108 MHz. Nous avons présenté aussi les méthodes de protection de ces services contre les perturbations. Les types de ces perturbations ainsi que la méthode qui serve pour les analyser sont brièvement caractérisés; les relations en question y sont citées. Les espaces d'existence potentielle des perturbations dans l'environment d'une station UKF FM en fonction de sa puissance et de sa fréquence pour un modele d'un récepteur de bord de l'avion; selon ICAO - annexe 10, 1998. Les équations de la puissance maximale admissible pour une station UKF FM sont proposées. Avec cette puissance les conditions de compatibilité seraient accomplis entre la radiophonie FM et celle de l'aviation pour les points d'essai définis dans l'espace de fonctionnement ILS et VOR. Les équations en question donnent la possibilité d'analyser la valeur de la puissance d'une station UKF FM pour une bande de fréquence donnée ce qui rends possible d'éliminer toutes les fréquences de colision - dés le début de la planification d'une station.

Zbigniew Rymarowicz

LEISTUNGSBEGRENZUNG DER UKW-FM-SENDER FÜR STÖRUNGSSCHUTZ DER LUFTFÄHRTDIENST

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

Vorgestellt wird die Problematik der in Empfangsanordnungen der Navigationfunkdienste im Band von 87,5 bis 108 MHz auftretenden Störungen. Schutzmethoden der Navigationfunkdienstes gegen diese Störungen werden vorgeschlagen. Es wird kürz auf die Störungstype und auf deren Analysenmethoden eingegangen wie auch entsprechende Relationen werden gegeben. Die Auftretenbereiche der Potentialstörungen sind für Environment der UKW-FM-Sender je nach der Leistung und der Frequenz unter Einsatz des Deckempfängers von ICAO-Flugzeug, des Annexes 10, 1998 gemäß, aufgeführt worden. Vorgeschlagen werden die Gleichungen für die maximale Strahlungleistung, die den Erfordernissen der Kompatibilität zwischen FM- und Navigationfunk in bestimmten Testpunkten des Wirkungsbereiches von ILS und VOR entspricht. Diese Gleichungen ermöglichen die Leistungswert

der UKW-FM-Sender im vorgegebenen Frequenzbereich zu analysieren, wieso schon zu Beginn der Plannung der Sender alle die Kolission verursachende Frequenzen zu exkludieren sind.

Andrzej Binkiewicz

657.47:621.31

KOSZT ENERGII ELEKTRYCZNEJ UZYSKIWANEJ W SYSTEMACH ZASILANIA, ZAWIERAJĄCYCH ALTERNATYWNE ŹRÓDŁA ENERGII

Przedstawiono oszacowanie i porównanie jednostkowych kosztów energii elektrycznej uzyskiwanej w konwencjonalnym systemie zasilania urządzeń łączności i w systemach zasilania, zawierających alternatywne źródła energii. Przeanalizowano następujące systemy zasilania ze źródłami alternatywnymi: autonomiczny system z baterią słoneczną, system z baterią słoneczną, współpracujący z siecią energetyczną oraz system hybrydowy z baterią słoneczną i generatorem wiatrowym, współpracujący z siecią energetyczną. Uwzględniono przy tym wszystkie składniki kosztów, m.in. koszt zakupu gruntu, budowy budynku siłowni, zakupu, montażu i uruchomienia urządzeń, koszty eksploatacji, a także koszty dodatkowe, np. wykonania projektu, wymaganych ekspertyz itd. Przy rozpatrywaniu systemów zasilania wyposażonych w alternatywne źródła energii wzięto pod uwagę dane, dotyczące podaży energii słonecznej i energii wiatrowej dla obszaru Polski.

1. WSTĘP

Celem tego artykułu jest podanie pewnych przesłanek i argumentów do dyskusji nad perspektywami zastosowania alternatywnych źródeł energii, nie jest zaś przesądzanie tych perspektyw. W wielu krajach świata, w tym także krajach Unii Europejskiej są tworzone programy rozwoju energetyki alternatywnej. Przykładowo przewiduje się dla obszaru UE, że w 2010 r. około 15% energii będzie uzy-

skiwane z tzw. czystych źródeł (głównie energii promieniowania słonecznego, wiatru i cieków wodnych). W związku z realną perspektywą przystąpienia Polski do UE trzeba brać te prognozy pod uwagę i przygotować się do - wprawdzie ograniczonej - lecz nieuchronnej transformacji naszej energetyki. Najważniejsze jest pytanie: ile to będzie kosztowało? W artykule podano odpowiedź. Wprawdzie przedstawione rozważania dotyczą telekomunikacyjnych systemów zasilania, jednak opisana metoda po pewnych modyfikacjach może być zastosowana w innych działach gospodarki.

W niniejszym opracowaniu rozpatrzono system zasilania z jednym alternatywnym źródłem energii (baterią słoneczną) oraz system mieszany z dwoma źródłami alternatywnymi (baterią słoneczną i generatorem wiatrowym). Przyjęto, że moc zainstalowana odbiorów dla rozpatrywanych systemów zasilania wynosi 10 kW. Koszt jednostkowy energii, zarówno w systemie tradycyjnym jak i w systemach z alternatywnymi źródłami zasilania, odnosi się do energii przetworzonej, tzn. mającej parametry odpowiednie do zasilania odbiorów komutacyjnych (napięcie stałe 48 V).

Bardzo istotnym zagadnieniem, warunkującym także poprawność przeprowadzonej w artykule analizy kosztów wytwarzania i przetwarzania energii, jest możliwość dokładnej oceny w warunkach polskich podaży odpowiednich rodzajów energii pierwotnej: energii promieniowania słonecznego i energii kinetycznej wiatru. W niniejszym opracowaniu zaprezentowano obszerne podejście do tego problemu.

2. KONFIGURACJE UKŁADU ZASILANIA

Właściwy dobór konfiguracji rozpatrywanych telekomunikacyjnych układów zasilania i parametrów urządzeń wchodzących w skład tych układów jest zadaniem zasadniczym. Prawidłowo dobrany układ

powinien zapewnić ciągłość zasilania oraz właściwe parametry zasilania.

Porównując tradycyjne systemy zasilania z systemami opartymi na zastosowaniu alternatywnych źródeł energii, trzeba zwrócić uwagę na fakt, że podstawowe źródło zasilania, którym jest w układach tradycyjnych sieć elektroenergetyczna, a ściślej elektrownie wchodzące w skład systemu energetycznego kraju, są zastąpione źródłami alternatywnymi. Celem analizy ekonomicznej może być więc w pierwszym rzędzie porównanie kosztów wytwarzania energii elektrycznej przez źródła podstawowe. Nie jest to jednak w pełni miarodajne, gdyż energia ta w systemie ulega dalszemu przetworzeniu z napięcia przemiennego 230/400 V do postaci wymaganej przez odbiory telekomunikacyjne (U_{ZN} = 48 V). Celowe jest zatem rozpatrzenie pełnego tradycyjnego układu zasilania odbiorów telekomunikacyjnych i kilku wariantów układów opartych na alternatywnych źródłach zasilania.

Tradycyjny układ zasilania składa się z siłowni telekomunikacyjnej, dwóch baterii akumulatorów i zespołu prądotwórczego. Przy czym każda z baterii powinna zapewnić rezerwę na ogół trzygodzinną. Moc zespołu prądotwórczego dobiera się z pewnym współczynnikiem w stosunku do mocy znamionowej odbiorów (1,5).

Układy, zawierające alternatywne źródła energii mogą mieć niżej podaną strukturę.

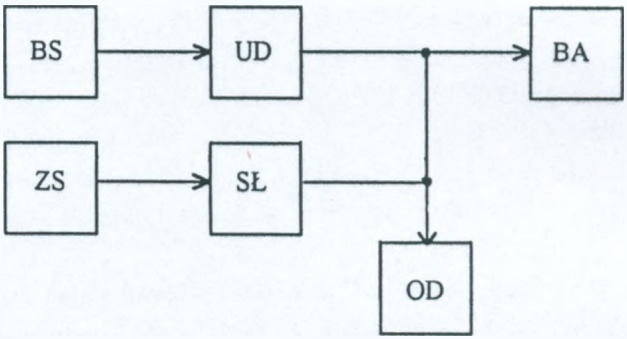
Układ autonomiczny jest złożony z następujących części zasadniczych:

- baterii słonecznej i/lub generatora wiatrowego,
- zespołu prądotwórczego,
- baterii akumulatorów,
- układu dopasowania (przetwornica DC/DC),
- siłowni.

Układ współpracujący z siecią składa się z następujących części zasadniczych:

- baterii słonecznej i/lub generatora wiatrowego,
- spalinowego zespołu prądotwórczego,
- układu dopasowania (przetwornica DC/DC),
- układu zwrotu nadwyżki energii elektrycznej do sieci (przetwornica DC/AC),
- siłowni.

Schematy blokowe tych układów zasilania przedstawiono na rysunku 1 i 2.

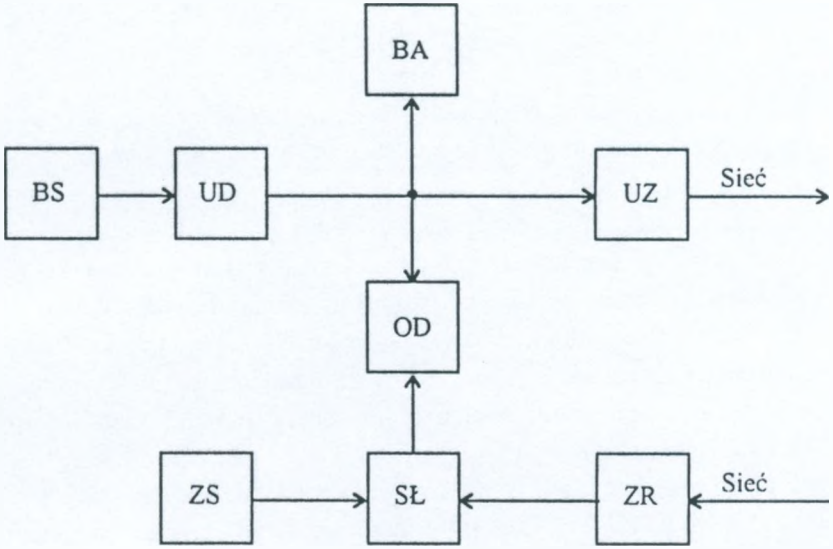


Rys. 1. Schemat blokowy autonomicznego układu zasilania

BS - bateria słoneczna, UD - układ dopasowania (przetwornica DC/DC), BA - bateria akumulatorów, ZS - zespół prądotwórczy, SŁ - siłownia, OD - odbiory

Analizując układ autonomiczny, można rozpatrywać dwa rozwiązania. W pierwszym rozwiązaniu zespół prądotwórczy jest traktowany jako podstawowe źródło rezerwowe, a rola baterii i jej parametry są takie same, jak w przypadku systemów tradycyjnych. W drugim rozwiązaniu bateria akumulatorów pełni rolę podstawowego źródła rezerwowego. W związku z tym rezerwa baterii jest zwiększona w stosunku do baterii w układach klasycznych (z 3 godzin do 12 godzin lub więcej). Zespół prądotwórczy zapewnia dostarcza-

nie energii w okresie wydłużonych okresów zmniejszonej podaży energii słonecznej lub wiatrowej (niekorzystne warunki meteorologiczne).



Rys. 2. Schemat blokowy systemu zasilania, współpracującego z siecią

UZ - układ zwrotu nadwyżki energii do sieci (falownik), pozostałe oznaczenia jak na rys. 1

W przypadku układu współpracującego z siecią analiza sprowadza się do porównania części kosztów wytwarzania energii elektrycznej, wnoszonych w układzie alternatywnym przez baterię słoneczną / generator wiatrowy i układ dopasowania (DC/AC), natomiast w układzie tradycyjnym koszt ten jest reprezentowany przez cenę energii elektrycznej pobieranej z sieci elektroenergetycznej. Pozostałe elementy układu tradycyjnego i układu opartego na źródłach alternatywnych są identyczne.

3. ANALIZA KOSZTÓW JEDNOSTKOWYCH ENERGII ELEKTRYCZNEJ ZUŻYWANEJ PRZEZ OBIEKTY TELEKOMUNIKACYJNE

Do analizy ekonomicznej powyższych wariantów systemów zasilania zostanie zastosowany wskaźnik *k* - jednostkowy koszt roczny energii. Pełną formułę tego wskaźnika i jej wyprowadzenie zamieszczono w załączniku.

Oszacowanie jednostkowych kosztów energii elektrycznej zużywanej przez odbiory telekomunikacyjne zasilane w systemie klasycznym, tj. opartym na używaniu jako źródła podstawowego energii pobieranej z sieci elektroenergetycznej 230/400 V 50 Hz, jest konieczne, aby można było porównać wynik tego oszacowania z analogicznym kosztem jednostkowym energii w przypadku zasilania odbiorów telekomunikacyjnych przez systemy, zawierające źródła alternatywne. Pełna analiza takich kosztów jest bardzo trudna i pracochłonna. Wymagałaby ona rozpatrzenia wszystkich typów obiektów telekomunikacyjnych, określenia stopnia partycypacji tego typu obiektów w krajowej sieci telekomunikacyjnej, a następnie na podstawie tych danych - określenia średnioważonego kosztu jednostkowego energii. Praca taka wymagałaby niemalże inwentaryzacji systemu telekomunikacyjnego kraju i jest niemożliwa do zrealizowania w zakresie niniejszego artykułu.

Należy więc wybrać inną drogę rozwiązania tego problemu. Ponieważ wynik oszacowania - z założenia - jest obarczony błędem, jest uprawnione zatem przyjęcie pewnych założeń upraszczających. Należy rozpatrzyć oszacowanie kosztu energii elektrycznej zużywanej w typowym obiekcie telekomunikacyjnym. Nie wnikając w charakter odbiorów należy rozważyć systemy zasilające o mocy nominalnej 10 kW i 50 kW i przyjąć upraszczające założenie, że koszt tego systemu jest liniowo zależny od mocy zainstalowanej (nie jest to prawdziwe, gdyż na ogół system o większej mocy zainstalowanej jest w przeliczeniu na jednostkę mocy tańszy).

4. OBLICZENIE JEDNOSTKOWEGO KOSZTU ENERGII DLA KONWENCJONALNEGO SYSTEMU ZASILANIA O MOCY 10 kW

4.1. Kalkulacja kosztów urządzeń

Przyjmując, że system dostarcza energię elektryczną o napięciu znamionowym 48 V, 200 A (moc 10 kW) i zakładając, że siłownia ma budowę modułową z odpowiednią liczbą modułów do zapewnienia redundancji wybiera się następujące typy siłowni, których ceny uwzględnia się w kalkulacji:

- SUH 240/240, firmy TELZAS;
- CS 300/240, firmy BPS;
- SBE 300/5, firmy BENNING.

Ceny tych siłowni, choć różne (od 46 200 zł do 65 000 zł), można szacować średnio na poziomie **50 000 zł** (I poł. 1998 r).

Bateria akumulatorów powinna zapewniać (zgodnie ze znowelizowanym zarządzeniem ministra łączności z 1987 r.) rezerwę bateryjną o czasie zasilania co najmniej 3 godziny. Wymaga się również istnienia baterii rezerwowej o takiej samej pojemności. Orientacyjna pojemność baterii wynosi zatem: Q_{10} = 800 Ah, 24 ogniwa. Zasadniczo bateria może być dwojakiego typu:

- bateria otwarta,
- bateria zamknięta (regulowana wentylami, określana też jako bezobsługowa).

Baterie otwarte są przeciętnie dwukrotnie tańsze od baterii bezobsługowych o tych samych parametrach.

Przykładowo mogą to być następujące typy baterii:

- 8OPzS800, firmy Warta, technologia „clasic", cena: 24 000 zł;
- 8OPzV800, firmy Warta, technologia żelowa, cena: 40 000 zł;
- 8OPzS800, firmy Bater, technologia „clasic", cena: 20 160 zł;
- ETG 960, firmy Bater, technologia żelowa, cena: 45 960 zł.

Jeśli zostanie użyta bateria klasyczna, to łączny koszt (dwie baterie o podanej pojemności) wyniesie ok. 50 000 zł. Natomiast jeśli zastosuje się **baterie żelowe, koszt** ten wyniesie ok. **90 000 zł.** Ponieważ obecnie obserwuje się tendencję do stosowania baterii bezobsługowych, należy przyjąć raczej tę drugą wartość, jako koszt baterii.

W przypadku zespołu prądotwórczego rozważono następujące typy zespołów:

- E22, firmy ENERCOM, cena: ok. 50 000 zł;
- ZG 1008-15 lub ZG 1008-20, firmy PZL-Mielec, cena: ok. 30 000 zł.

Łącznie koszt urządzeń wyniesie około: 50 000 + 90 000 + + 30 000 = 170 000 zł.

Do kosztów tych należy dodać:

- 3%: koszty instalacji i montażu;
- 5%: koszty projektu;
- 7%: koszty wyposażenia dodatkowego.

Łącznie koszty dodatkowe wynoszą ok. 15%: **25 000 zł. Sumaryczny koszt urządzeń** wchodzących w skład siłowni wyniesie zatem: 170 000 + 25 000 = **195 000 zł**. Trzeba zauważyć, że koszt urządzeń podano opierając się na danych katalogowych. Ceny katalogowe są na ogół wyższe od rzeczywistych oferowanych TP SA. Jednak preferencje te są objęte tajemnicą handlową, a ich uwzględnienie nie zniekształca w sposób wyraźny wyników przedstawionych szacunków.

4.2. Kalkulacja budynku siłowni i innych środków trwałych

Założono, że budynek, w którym będą zainstalowane urządzenia zasilające (siłownia, baterie akumulatorów, zespół prądotwórczy, moc nominalna odbiorów 10 kW), musi do tego celu mieć powierzchnię ok. 30 m^2. Grunt, na którym jest usytuowany budynek siłowni, musi być odpowiednio większy - zakłada się, że konieczna powierzchnia

działki powinna wynosić ok. 60 m^2. Według danych z cennika robót budowlanych (kwartalnika, wydawanego przez Ośrodek Wdrożeń Ekonomiczno-Organizacyjnych Budownictwa „Promocja" [3]), należy przyjąć dla tego typu budownictwa wskaźnik 1 400 zł/m^2 (maj 1998 r). Do kosztów tych należy dodać jeszcze następujące koszty:

- 15%: koszty przyłączy instalacji, 210 zł/m^2;
- 5%: koszty projektu, 70 zł/m^2;
- 5%: inne koszty bezpośrednie, 70 zł/m^2.

Koszt łączny 1 m^2 budynku (bez składnika wynikającego z kosztu działki) wynosi: 1 400 + 210 + 70 + 70 = 1 750 zł.

Ceny gruntu są bardzo zróżnicowane i w zależności od miejsca usytuowania mogą wynosić od 10 zł/m^2 do nawet 1 000 zł/m^2. Do analizy przyjęto wartość przeciętną 100 zł/m^2. Dla przyjętej **wielkości działki: 60 m^2 jej koszt** wyniesie **6 000 zł,** a w przeliczeniu na m^2 budynku koszt ten wyniesie: 200 zł/m^2. Łączny koszt 1 m^2 budynku wyniesie zatem średnio: 1 750 + 200 = 1 950 ≈ 2 000 zł/m^2, a **łączny koszt budynku siłowni**: 30 · 2 000 = **60 000 zł**.

4.3. Inne założenia niezbędne do analizy

Założono, że czas trwania inwestycji wyniesie dwa lata. Pierwszy rok obejmie koszty związane z budową budynku, natomiast drugi rok - koszty związane z zakupem i instalacją oraz uruchomieniem urządzeń, wchodzących w skład systemu zasilania odbiorów telekomunikacyjnych.

Zgodnie z rozporządzeniem ministra finansów z dnia 17 stycznia 1997 r., roczne stawki amortyzacyjne na poszczególne składniki majątkowe są następujące:

- budynek: 25 lat, 4%;
- baterie akumulatorów: 5 lat, 20%;
- siłownia: 10 lat, 10%;
- zespół prądotwórczy: 10 lat, 10%.

W rzeczywistości żywotność baterii, jak to wynika z praktyki, należy przyjąć 10 lat, a związaną z tym stawkę amortyzacyjną 10%. Przyjęto więc dla wszystkich urządzeń czas amortyzacji 10 lat i stawkę amortyzacyjną 10%, a dla budynku odpowiednio 25 lat i 4%. Ponadto należy przyjąć do obliczeń cenę energii elektrycznej pobieranej z sieci energetycznej - według taryfy C11 wynosi ona 0,27 zł/kWh.

Założyć należy również koszty eksploatacji. Składają się one z: kosztów stałych oraz kosztów zmiennych. Na koszty stałe eksploatacji składają się koszty zatrudnienia w dziale eksploatacji. Przyjęto, że dla rozpatrywanego obiektu potrzeby etatowe wynoszą ok. 1/4 etatu. Koszty zmienne eksploatacji obejmują m.in. koszt paliwa i olejów do zespołu prądotwórczego, koszt energii zużywanej w trakcie kontrolnego rozładowania i ładowania baterii, koszty konserwacji, remontów oraz ewentualnych napraw urządzeń itp. Przyjęto, że łączne koszty zmienne eksploatacji są równe kosztom stałym. **Sumaryczny koszt eksploatacji** odpowiada zatem 1/2 etatu, czyli 12 · 1 250 zł = = **15 000 zł/rok (brutto)**.

4.4. Obliczenia rocznych rat zwrotu kapitału dla poszczególnych składników majątkowych

Przyjęto następujące założenie: czas amortyzacji równa się czasowi użytkowania poszczególnych składników majątkowych. Założenie to jest rozsądne i znacznie upraszcza obliczenia. Założono również, że amortyzacji podlega 100% kosztu urządzenia. Wzór na roczną ratę zwrotu kapitału, przy tych założeniach, ma postać podaną w załączniku - por. wzór (10).

Przyjęto następujące dane do obliczeń:

k_n - nominalna stopa dyskontowa jest równa 13% (0,13);

D - roczna stawka amortyzacji jest równa 10% (0,1) dla urządzeń oraz 4% (0,04) dla budynku;

T - podatek dochodowy, przyjęto 35% (0,35);

n - liczba lat eksploatacji składników majątkowych: dla urządzeń 10, dla budynku 25.

Po podstawieniu tych danych dla urządzeń otrzymuje się następującą wartość rocznej raty zwrotu kapitału:

$$r_n = \frac{0{,}13\,(1{,}13)^{10}}{0{,}65\,((1{,}13)^{10} - 1)} - \frac{0{,}1 \cdot 0{,}35}{0{,}65} \approx 0{,}23 = 23\%\,.$$

Analogicznie dla budynku otrzyma się:

$$r_n = \frac{0{,}13\,(1{,}13)^{25}}{0{,}65\,((1{,}13)^{25} - 1)} - \frac{0{,}04 \cdot 0{,}35}{0{,}65} \approx 0{,}19 = 19\%\,.$$

W przypadku budynku trzeba zaznaczyć, że wynik ten jest przybliżony również z tego względu, że część składników obliczonego kosztu budynku jest związana z nabyciem środków trwałych (np. nabycie gruntu) i nie można ich uznać za koszt uzyskania przychodów. Fakt ten będzie wpływał na nieznaczne zwiększenie wartości r_n. Przyjęto, nie wdając się w szczegółową analizę, że **roczna rata zwrotu kapitału dla budynku** wyniesie $r_n = 0{,}2$, czyli 20%.

4.5. Modyfikacja kosztów inwestycyjnych przez zastosowanie rachunku dyskonta

Koszty inwestycyjne (I) dla rozpatrywanego przez nas przypadku można przedstawić w następującej postaci:

$$I = \sum_{t=-1}^{0} I_t \frac{1}{(1+k_n)^t} = I_{-1}(1+k_n) + I_o\,.$$

Inwestycja, jak już wspomniano, jest dwuletnia, gdzie:

I_{-1} - jest to koszt budynku oraz jego projektu, poniesiony w pierwszym roku inwestycji;

I_o - obejmuje koszt urządzeń, poniesiony w drugim roku inwestycji:

$$I_{-1d} = I_{-o}(1 + k_n) = 60\,000 \cdot (1 + 0{,}13) \approx 68\,000 \text{ zł},$$

$$I_{od} = I_o = 195\,000 \text{ zł};$$

I_{-1d} - zdyskontowany koszt I_{-1},
I_{od} - zdyskontowany koszt I_o.

Łącznie zmodyfikowane koszty inwestycyjne wyniosą: $I_{-1d} + I_o =$ **= 263 000 zł.**

4.6. Koszt jednostkowy 1 kWh

Łączny koszt roczny K_r związany z zasilaniem odbiorów na rozważanym obiekcie wynosi:

$$K_r = 195\,000 \cdot 0{,}23 + 68\,000 \cdot 0{,}2 + 15\,000 + A,$$

gdzie:
A - roczny koszt energii pobieranej z sieci elektroenergetycznej.

Przyjęto upraszczające założenie, że odbiory telekomunikacyjne pobierają w ciągu całego roku maksymalną energię odpowiadającą zainstalowanej mocy, czyli w ciągu roku jest 10 kWh · 8760 h = = 87 600 kWh. Założenie to jest maksymalistyczne i w efekcie zmniejsza - w stosunku do rzeczywistego koszt 1 kWh. Ponadto założono, że łączny współczynnik sprawności przedstawionego systemu zasilania wynosi 0,8, koszt A zatem będzie powiększony o czynnik 1,25. Przyjmując wcześniej przyjętą wartość dla taryfy C11 = = 0,27 zł/kWh otrzyma się po modyfikacji 1,25 · 0,27 = 0,34 zł/kWh, więc A = 87 600 kWh · 0,34 zł/kWh = 29 800 zł. **Koszt roczny** wyniesie więc K_r = 195 000 · 0,23 + 68 000 · 0,2 + 15 000 + 29 800 = **= 103 250 zł.**

Natomiast **jednostkowy koszt roczny energii** k (wzór (14) - zał.) wyniesie:

$$k = \frac{103250 \text{ zl}}{87600 \text{ kWh}} \approx 1{,}2 \text{ zł/kWh}.$$

5. OBLICZENIE JEDNOSTKOWEGO KOSZTU ENERGII DLA KONWENCJONALNEGO SYSTEMU ZASILANIA O MOCY 50 kW

Poniżej przedstawiono w sposób skrótowy analizę kosztu jednostkowego uzyskania energii w konwencjonalnym systemie zasilania o mocy znamionowej 50 kW. Analizę przeprowadzono w sposób analogiczny, jak w przypadku systemu o mocy 10 kW.

- Elementy systemu i ich koszt:
  - bateria akumulatorów: 1000 Ah · 3 = 3000 Ah + bateria rezerwowa o tej samej pojemności, 260 000 zł;
  - siłownia: 240 000 zł;
  - zespół prądotwórczy: 72 000 zł;
  - budynek siłowni 60 m^2: 60 · 1 400 zł/m^2 + 15% = 96 000 zł;
  - działka 120 m^2: 120 · 100 zł = 12 000 zł.
- Koszt inwestycyjny poniesiony w 1 roku inwestycji: 96 000 + + 12 000 = 108 000 zł.
- Koszt zmodyfikowany przez rachunek dyskonta: 108 000 · 1,13 = = 122 000 zł.
- Koszt urządzeń: 572 000 zł.
- Koszty dodatkowe: 10% kosztu urządzeń, czyli 57 200 zł.
- Koszt łączny dotyczący urządzeń: około 630 000 zł.
- Roczny koszt eksploatacji: 30 000 zł.
- Roczny koszt energii pobieranej z sieci elektroenergetycznej:
  - rocznie pobierana ilość energii przez odbiory (przy założeniu maksymalnego obciążenia): 8 760 h · 50 kW = 438 000 kWh;
  - koszt tej energii: 438 000 kWh · 0,34 zł/kWh ≈ 149 000 zł.

- Obliczenie kosztu rocznego związanego z zasilaniem obiektu:

$$K_r = 630\,000 \cdot 0{,}23 + 122\,000 \cdot 0{,}19 + 30\,000 + \\ + 149\,000 = 347\,080 \text{ zł}.$$

- Jednostkowy koszt roczny energii:

$$k = 347\,080 \text{ zł} / 438\,000 \text{ kWh} \approx 0{,}8 \text{ zł/kWh}.$$

Z tych obliczeń wynika, że koszt jednostkowy w tym systemie (50 kW mocy), zgodnie z przewidywaniami, jest niższy niż w systemie o mocy 10 kW (1,2 zł/kWh).

6. PODAŻ ENERGII PROMIENIOWANIA SŁONECZNEGO NA OBSZARZE POLSKI

Do przeprowadzenia analizy jednostkowych kosztów energii elektrycznej uzyskiwanej w systemach zasilania, zawierających alternatywne źródła energii, w tym przede wszystkim baterie słoneczne, jest konieczne podanie podstawowych informacji na temat podaży energii promieniowania słonecznego na obszarze Polski. Poniżej omówiono najważniejsze zagadnienia z tym związane.

Do Ziemi, a ściślej do granicy z atmosferą ziemską, dociera ze Słońca energia w postaci promieniowana o wartości powierzchniowej gęstości (na powierzchnię prostopadłą do kierunku promieniowania) równej 1353 W/m^2. Jest to tzw. stała słoneczna. Wprawdzie efektywne wykorzystanie tej energii jest możliwe na stosunkowo niewielkim obszarze, a sprawność instalacji, w których dokonuje się konwersja energii promieniowania na energię elektryczną, jest rzędu 10%, mimo to potencjał ten jest wyższy od obecnego światowego zapotrzebowania energetycznego. Jest to niewyczerpywalne źródło energii. Widmo promieniowania słonecznego odpowiada z dużą dokładnością promieniowaniu ciała doskonale czarnego w temperaturze

6 000°C. Najwięcej energii przypada na zakres długości fal światła widzialnego: 0,35 ÷ 0,75 μm.

Promieniowanie słoneczne przechodząc przez atmosferę ziemską ulega w niej osłabieniu wskutek procesów absorpcji, rozpraszania i odbicia. Absorpcja dotyczy zwłaszcza promieniowania nadfioletowego i podczerwonego. Promieniowanie nadfioletowe jest pochłaniane w warstwie atmosfery, zwanej ozonosferą, na wysokości około 35 km nad powierzchnią Ziemi. W procesie tym szczególną rolę odgrywa zjawisko syntezy i rozkładu ozonu - głównego składnika ozonosfery. Promieniowanie podczerwone jest pochłaniane przez zawarte w atmosferze: parę wodną i dwutlenek węgla.

Rozpraszanie promieniowania w atmosferze zachodzi zgodnie z modelem Rayleigha lub Miego [8]. Rozpraszanie Rayleigha dotyczy centrów rozpraszających w postaci cząstek mniejszych od 0,1 λ, gdzie λ jest długością fali światła. Odnosi się ono zatem m.in. do cząstek O_2 i N_2 - głównych składników atmosfery. Zgodnie z tą teorią, współczynnik rozpraszania światła jest odwrotnie proporcjonalny do czwartej potęgi długości fali światła. To tłumaczy m.in. błękitny kolor nieba (światło niebieskie ulega silniejszemu rozproszeniu niż światło czerwone, bo ma mniejszą długość fali). Rozproszenie Rayleigha wykazuje dużą równomierność we wszystkich kierunkach (prawie symetrię kulistą). To sprawia, że promieniowanie rozproszone, zwane także dyfuzyjnym, dociera ze wszystkich kierunków nieba i natężenie tego promieniowania z każdego kierunku jest w przybliżeniu takie samo. Rozproszenie Miego [8] dotyczy większych cząstek, np. pyłów, kropelek pary wodnej. Nie ma ono charakteru tak wyraźnie symetrycznego, jak rozpraszanie Rayleigha.

Odbicie całkowite promieniowania słonecznego od atmosfery i powierzchni ziemskiej określa się przez współczynnik odbicia (tzw. „albedo Ziemi") - jego wartość wynosi około 0,35.

Jak wspomniano wyżej, promieniowanie słoneczne docierające do powierzchni Ziemi składa się z dwóch składników: promieniowania

bezpośredniego i promieniowania rozproszonego. Promieniowanie bezpośrednie jest to ta część promieniowania słonecznego, która w postaci niezakłóconej dociera do powierzchni Ziemi, dlatego ta składowa promieniowania jest silnie związana z wyróżnionym kierunkiem, który jest wyznaczony przez pozycję Słońca nad horyzontem. Natomiast promieniowanie dyfuzyjne jest promieniowaniem wtórnym, wynikającym ze zjawiska rozproszenia (Rayleigha i Miego), a jego wartość jest w przybliżeniu jednakowa z każdego kierunku nieba.

Natężenie promieniowania słonecznego jest charakteryzowane przez powierzchniową gęstość energii promieniowania na jednostkę czasu - najczęściej godzinę lub dobę. Natężenie promieniowania słonecznego docierającego do powierzchni Ziemi zależy nie tylko od kąta Z - padania promieniowania na powierzchnię Ziemi, ale również od ilości i rodzaju naturalnych lub nienaturalnych absorbentów w atmosferze. Należą do nich opady, mgła, chmury, para wodna, jak również, będące skutkiem działalności przemysłowej człowieka: pyły, dwutlenek węgla oraz inne związki chemiczne. Przy dużym zachmurzeniu miejscowe natężenie promieniowania słonecznego docierającego do powierzchni Ziemi może spadać do 10% wartości właściwej dla optymalnych warunków meteorologicznych. Wymienione czynniki, wpływające na wartość miejscowego natężenia promieniowania słonecznego, mogą mieć charakter losowy, okresowy lub quasi-stały. Zjawiska meteorologiczne, np. stopień zachmurzenia, opady i poziom wilgotności atmosfery, mają charakter losowo-okresowy. Natomiast stan zapylenia i zawartość związków chemicznych w atmosferze nad danym terenem wiąże się z poziomem urbanizacji oraz uprzemysłowieniem tego terenu i ma charakter quasi-stały lub regularnie okresowy.

Do określenia lokalnych zasobów energetycznych promieniowania słonecznego, czyli średniej wieloletniej wartości gęstości energii promieniowania na jednostkę czasu, można zastosować dwie metody: empiryczną i obliczeniową.

6.1. Empiryczne metody określenia natężenia promieniowania

Metoda empiryczna jest bardziej wiarygodna i w dokładniejszy sposób umożliwia dokonanie oceny rzeczywistej wartości natężenia promieniowania. Polega ona na pomiarach promieniowania na danym obszarze przez sieć umiejscowionych na nim stacji aktynometrycznych.

Na obszarze Polski jest rozmieszczonych 21 takich stacji, należących do Instytutu Meteorologii i Gospodarki Wodnej (IMiGW). Choć nie jest to mało, to jednak rozkład tych stacji na obszarze kraju jest bardzo nierównomierny. Przykładowo, stacje Zakopane, Kasprowy Wierch i Hala Gąsiennicowa są umiejscowione tak blisko siebie, że dane uzyskane z tych stacji dotyczą praktycznie tego samego miejsca (po uwzględnieniu poprawki, wynikającej z różnic wysokości położenia). Również dość duża jest gęstość rozmieszczenia stacji w Polsce centralnej (Warszawa, Brwinów, Belsk, Sulejów), a jednocześnie są duże obszary, na których stacji prawie nie ma, np. Wielkopolska (tylko jedna stacja - Radzyń). Mimo tych zastrzeżeń, pomiary uzyskiwane na tych stacjach dały podstawę do wyznaczenia map zasobów energetycznych promieniowania słonecznego na obszarze Polski. Dane te są rejestrowane w sposób ciągły od wielu lat. Natężenie promieniowania jest uśredniane za okres 1 godziny.

Zgodnie z publikowanymi danymi, średnia roczna suma promieniowania na obszarze Polski wynosi 950 ÷ 1 250 kWh/m^2, co odpowiada średniemu natężeniu promieniowania: 110 ÷ 140 W/m^2 [6]. W [1] przedstawiono mapy obszaru Polski z naniesionymi izoliniami natężenia promieniowania słonecznego. Mapy te zostały sporządzone na podstawie danych z pomiarów wykonywanych przez IMiGW w latach 1956 ÷ 1975. Zgodnie z tymi mapami, średnie całkowite dzienne promieniowanie słoneczne na obszarze Polski wynosi 9,50 ÷ 10,25 MJ/m^2 na dobę, co odpowiada po przeliczeniu jednostek średniemu natężeniu promieniowania: 110 ÷ 120 W/m^2. Dane te do-

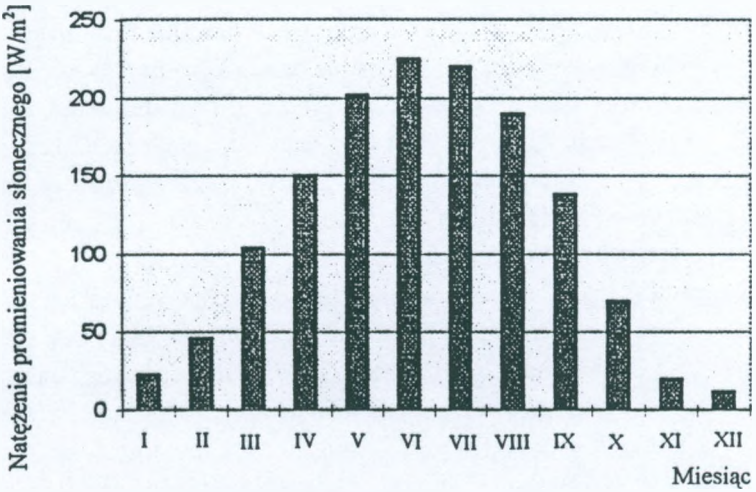
tyczą płaszczyzny odpowiadającej powierzchni ziemi. Jednostki podano zgodnie z oryginalnymi źródłami.

Największe natężenie promieniowania, czyli 120 W/m^2 (po przeliczeniu jednostek) występuje na Zamojszczyźnie i w Polsce centralnej (okolice Warszawy). Wielkopolska, Lubelszczyzna, Małopolska i Polska wschodnia charakteryzują się średnim natężeniem promieniowania o mocy wynoszącej 115 W/m^2. Najniższa wartość natężenia promieniowania występuje na obszarach Polski północnej, a także zachodniej i południowej (na południe od linii Wrocław - Kraków - - Przemyśl): 110 ÷ 113 W/m^2.

Przebieg krzywej natężenia promieniowania w ciągu roku wskazuje, że natężenie promieniowania ma na początku stycznia wartość około 25 W/m^2, następnie rośnie prawie równomiernie do początku czerwca, kiedy osiąga maksimum (na poziomie 230 W/m^2), przez kolejne dwa miesiące wolno się obniża, a następnie od połowy sierpnia szybko spada, osiągając na początku listopada wartość poniżej 35 W/m^2. Najniższą wartość natężenie promieniowania osiąga w drugiej połowie listopada i w grudniu, kiedy wynosi około 15 W/m^2. Na podstawie tych danych można stwierdzić dużą zależność natężenia promieniowania od pór roku. Natężenie to w czerwcu jest ok. 15 razy wyższe niż w grudniu. Na rys. 3 podano wartości średniego natężenia promieniowania słonecznego dla kolejnych miesięcy.

Poza tą długookresową, w miarę regularną zmiennością natężenia promieniowania w skali roku, występują również zmiany krótkookresowe w skali jednego miesiąca. Zmiany te są nieregularne, zależne od zjawisk meteorologicznych, takich jak: poziom zachmurzenia i opady. Na podstawie analizy danych z rocznika [12], przedstawiającego wyniki pomiarów natężenia promieniowania przez wszystkie 21 stacji aktynometrycznych, można stwierdzić, jak duża zmienność natężenia promieniowania występuje na danej stacji w tym samym okresie, np. w ciągu miesiąca o tej samej porze dnia (warunki astronomiczne wpływające na natężenie promieniowania, tj. pozycja Słońca na nie-

bie i kąt padania promieni słonecznych na powierzchnię ziemi - są dla danej stacji niezmienne). Wyjaśnieniem tej sytuacji może być tylko wpływ zmiennych warunków atmosferycznych. W tablicy 1 zamieszczono przykładowe dane dla Warszawy w lipcu 1978 r. w godz. 11.00 ÷ 13.00.



Rys. 3. Średnie natężenie promieniowania słonecznego w Polsce na płaszczyznę poziomą

Tablica 1

Przykładowe dane natężenia promieniowania słonecznego dla danego obszaru w ciągu miesiąca (Warszawa, lipiec 1978 r., godz. 11.00 ÷ 13.00)

Liczba godzin →	2	2	11	14	9	11	11	2
Przedział natężenia promieniowania słonecznego [W/m²]	< 116	116÷232	232÷348	348÷464	464÷580	580÷696	696÷812	> 812

W tabl. 1 uwzględniono liczbę godzin, w których wartość natężenia promieniowania słonecznego była zawarta w podanych prze-

działach dla płaszczyzny poziomej odpowiadającej powierzchni ziemi. Nietypowe granice przedziałów wynikają z przeliczenia jednostki oryginalnej, którą w źródle, z którego zaczerpnięto dane, była cal/cm^2 · h. Na podstawie tych danych można stwierdzić, że występuje znaczna liczba godzin z natężeniem promieniowania około 350 W/m^2 - 25 godzin oraz duża liczba godzin z natężeniem promieniowania ok. 700 W/m^2 - 22 godzin. Średnia obliczona moc promieniowania dla danych z tabl. 1 wynosi około 510 W/m^2. Jest to zatem znaczny rozrzut wartości natężenia promieniowania (blisko 50%). Wydaje się, że ten rozrzut jest spowodowany zachmurzeniem i zwiększoną wilgotnością atmosfery. Natężenie promieniowania o wartości poniżej 232 W/m^2 - 4 godziny jest związane prawdopodobnie z intensywnymi opadami w czasie tych godzin.

Dane na temat promieniowania dla szerokości geograficznej 52° podano również w normie [11]. W zasadzie odpowiadają one dobrze wartościom z rocznika [12]. Przykładowo maksymalne natężenie zmierzone w lipcu 1978 r. na stacji w Warszawie wynosiło 870 W/m^2 (w oryginalnych jednostkach: 75 cal/cm^2 · h), natomiast w normie dla płaszczyzny poziomej zmierzono wartość 912 W/m^2 (w jednostkach oryginalnych: 786 kcal/m^2 · h). Jednak dane w normie mają wartości maksymalne w stosunku do rzeczywiście występujących, gdyż nie uwzględniają one sytuacji gorszych warunków pogodowych, które zmniejszają przezroczystość atmosfery i w efekcie zmniejszają natężenie promieniowania słonecznego. Ocenia się, że zawyżenie to może być około 30%.

6.2. Teoretyczne metody wyznaczania natężenia promieniowania słonecznego

Metoda obliczeniowa polega na wyznaczaniu natężenia promieniowania na podstawie wskaźników teoretycznych lub uśrednionych danych empirycznych dla danej szerokości geograficznej. Według tej

metody podaje się przybliżone wartości promieniowania - jednakowe dla dużych obszarów - takich, jak np. obszar Polski, przy założeniu warunków normalnych i określonego stopnia przezroczystości atmosfery. Dane te są stabelaryzowane i podane dla płaszczyzn pionowych o odpowiednim kącie orientacji (względem kierunku północ-południe) i płaszczyzny poziomej.

Tego typu dane, jak już wspomniano, można znaleźć m.in. w normie [11]. Obejmują one miesiące: kwiecień ÷ wrzesień od godziny 5.00 do 19.00 dla powierzchni poziomej i pionowych zorientowanych od północy przez wschód (zachód) na południe co 30° kątowych. W wymienionej normie podano całkowite natężenie promieniowania oraz promieniowanie rozproszone dla trzech stopni przezroczystości atmosfery, związanych z charakterem obszaru i stopniem jego uprzemysłowienia. Są to następujące stopnie:

P3 - obszary nieuprzemysłowione,

P4 - obszary dużych miast,

P5 - obszary przemysłowe.

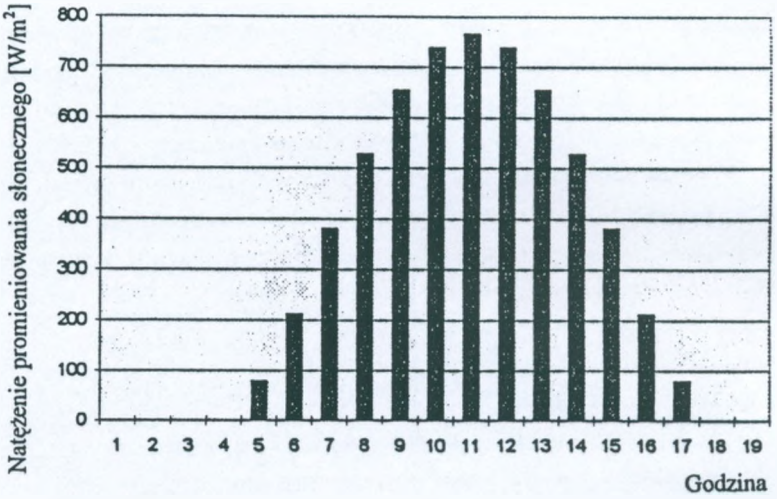
Na rys. 4 przedstawiono przykładowy wykres średniego natężenia promieniowania w kwietniu dla płaszczyzny baterii słonecznej skierowanej na południe i tworzącej z płaszczyzną poziomą kąt 35°.

Średnia dobowa wartość natężenia promieniowania w kwietniu dla szerokości geograficznej Warszawy (około 52°) na podstawie danych z wykresu na rys. 4 wynosi około 250 W/m^2. Jak już wspomniano, dane według normy są zawyżone. Korzystając z danych zawartych w wymienionej normie można dokonać syntezy wektora natężenia promieniowania dla dowolnie zorientowanej płaszczyzny baterii słonecznej.

Inną metodą oszacowania wartości natężenia promieniowania słonecznego jest metoda analityczna. Metoda ta polega na analitycznym rozwiązaniu takich zadań, jak:

1) wyznaczenie wektora natężenia promieniowania na płaszczyznę prostopadłą do kierunku padania promieni słonecznych;

2) rozkład otrzymanego wektora na składowe przez rzutowanie na wyróżnione płaszczyzny;
3) synteza wektora natężenia promieniowania słonecznego w dowolnym kierunku, wyznaczonym przez normalną do płaszczyzny baterii słonecznej.



Rys. 4. Średnie godzinowe natężenia promieniowania słonecznego w kwietniu dla szerokości geograficznej 52°

Do rozwiązania ww. zadań oprócz narzędzi matematycznych używa się metod cyfrowych. Metoda ta w artykule nie będzie szerzej omawiana.

7. PODAŻ ENERGII WIATROWEJ

W pkt. 7 podano niezbędne informacje do kontynuowania analizy kosztów uzyskiwania energii elektrycznej w systemach zasilania z generatorem wiatrowym. Najodpowiedniejszą metodę opisu wiatru

zawiera statystyka matematyczna. Szczególnie dobrze do tego celu nadaje się rozkład Weibulla. Za jego pomocą opisuje się średnie 10-minutowe prędkości wiatru v. Dystrubuanta tego rozkładu ma następującą postać:

$$F(v_z) = P(v \leq v_z) = 1 - e^{-\left(\frac{v_z}{\beta}\right)^{\gamma}},$$

gdzie:

β i γ - parametry, które należy wyznaczyć metodami statystycznymi;

v_z - założona prędkość wiatru.

Wartości parametrów β i γ dla stacji meteorologicznych w Polsce (na podstawie danych IMiGW) [10] przedstawiono w tablicy 2.

Tablica 2

Parametry rozkładu Weibulla dla różnych stacji meteorologicznych w Polsce

Stacja meteorologiczna	Parametry rozkładu Weibulla		h - wysokość wiatromierza	v_z dla prawdopodobieństwa przewyższenia P					
				P = 0,2 (20%)			P = 0,1 (10%)		
	β	γ		dla h	dla 10 m	dla 30 m	dla h	dla 10 m	dla 30 m
1	2	3	4	5	6	7	8	9	10
Białystok	3,989	1,698	12	5,3	5,5	6,5	6,5	6,7	7,9
Bielsko-Biała	4,766	1,440	20	6,6	6,3	7,4	8,5	8,1	9,5
Chojnice	4,734	1,653	13	6,3	6,0	7,1	7,8	7,5	8,8
Częstochowa	4,719	2,087	13	5,9	6,7	7,8	7,0	7,9	9,3
Elbląg	4,553	1,707	19	6,0	6,3	7,4	7,4	7,8	9,2
Gorzów Wlk.	3,773	1,504	13	5,2	5,9	7,0	6,6	7,4	8,7
Hel	5,929	2,108	23	7,4	8,3	9,8	8,8	9,9	11,7
Jelenia Góra	3,231	1,191	16	4,8	4,7	5,5	6,5	6,4	7,5
Kalisz	3,583	1,422	15	5,0	5,0	5,9	6,4	6,4	7,5
Katowice	3,925	1,666	20	5,2	5,0	5,8	6,5	6,2	7,3
Kętrzyn	4,243	1,579	13	5,7	5,5	6,5	7,2	6,9	8,1
Kielce	3,231	1,433	15	4,5	4,2	5,0	5,8	5,5	6,4

cd. tablicy 2

1	2	3	4	5	6	7	8	9	10
Kłodzko	5,085	2,104	14	6,4	6,1	7,2	7,6	7,2	8,5
Koło	3,385	1,398	14	4,8	4,8	5,7	6,2	6,3	7,4
Kołobrzeg	4,858	2,045	18	6,1	7,2	8,5	7,3	8,7	10,3
Koszalin	4,495	1,364	13	6,4	7,2	8,5	8,3	9,4	11,1
Kraków	3,990	1,600	11	5,4	5,3	6,2	6,7	6,6	7,8
Legnica	3,978	1,649	16	5,3	4,9	5,8	6,6	6,2	7,3
Lesko	4,356	1,623	14	5,8	5,5	6,5	7,3	6,9	8,1
Leszno	4,466	1,713	14	5,9	6,0	7,1	7,3	7,4	8,7
Lublin	4,065	1,834	12	5,3	5,2	6,1	6,4	6,2	7,3
Łeba	5,849	2,118	14	7,3	6,9	8,1	8,7	8,3	9,8
Łódź	4,829	1,801	12	6,3	6,5	7,7	7,7	8,0	9,4
Mikołajki	4,827	1,843	15	6,2	5,8	6,8	7,6	7,2	8,5
Mława	5,420	1,713	12	7,2	7,0	8,3	8,8	8,6	10,1
Nowy Sącz	2,116	1,126	16	3,2	3,9	4,6	4,4	5,4	6,4
Olsztyn	4,151	1,776	13	5,4	5,5	6,5	6,6	6,8	8,0
Opole	4,384	1,821	14	5,7	6,3	7,4	6,9	7,7	9,1
Ostrołęka	3,477	1,558	13	4,7	5,3	6,2	5,9	6,7	7,8
Poznań	5,101	1,842	10	6,6	7,0	8,3	8,0	8,5	10,0
Przemyśl	4,256	1,623	15	5,7	5,7	6,7	7,1	7,1	8,4
Racibórz	2,381	1,344	15	3,4	3,7	4,4	4,4	4,8	5,6
Rzeszów	4,605	1,621	16	6,2	6,7	7,9	7,7	8,3	9,8
Sandomierz	5,193	1,877	15	6,7	6,3	7,4	8,1	7,6	9,6
Siedlce	4,108	1,609	12	5,5	5,7	6,7	6,9	7,1	8,4
Słubice	3,290	1,518	17	4,5	5,4	6,4	5,7	6,8	8,0
Suwałki	5,616	1,759	10	7,4	7,4	8,7	9,0	9,0	10,6
Szczecin	5,213	2,086	24	6,6	6,6	7,8	7,8	7,8	9,2
Szczecinek	3,737	1,518	17	5,1	6,1	7,2	6,5	7,8	9,2
Świnoujście	5,145	1,747	11	6,8	7,1	8,4	8,3	8,7	10,3
Tarnów	3,070	1,513	14	4,2	5,3	6,2	5,3	6,6	7,8

cd. tablicy 2

1	2	3	4	5	6	7	8	9	10
Terespol	4,468	1,967	12	5,7	5,9	7,0	6,8	7,0	8,3
Toruń	4,061	1,776	12	5,3	6,9	8,1	6,5	8,4	9,9
Ustka	5,898	2,023	20	7,5	8,7	10,3	8,9	10,3	12,1
Warszawa	5,511	1,995	12	7,0	7,3	8,5	8,4	8,7	10,3
Wieluń	3,898	2,170	15	4,8	5,9	7,0	5,7	7,0	8,3
Włodawa	4,451	1,892	12	5,7	5,5	6,5	6,9	6,7	7,9
Wrocław	4,172	1,494	17	5,7	5,3	6,2	7,3	6,7	7,9
Zamość	4,101	1,700	12	5,4	5,6	6,6	6,7	6,9	8,1
Zielona Góra	4,690	2,057	13	5,9	7,5	8,8	7,0	8,9	10,5

W tabl. 2 podano także v_z dla dwóch założonych wartości prawdopodobieństw przewyższenia i trzech wartości wysokości nad powierzchnią ziemi: h (wysokości rzeczywistej pomiaru na stacji), 10 m i 30 m.

Do celów energetyki wiatrowej jest użyteczny wiatr w przedziale prędkości $4 \div 20$ m/s. Dolna granica jest to minimalna wymagana prędkość do rozruchu silnika wiatrowego (niekiedy jest to 5 m/s lub 6 m/s), a górna granica określa maksymalną prędkość bezpieczną dla instalacji wiatrowej, powyżej której następuje wyłączenie instalacji.

Aby oszacować użyteczną energię kinetyczną wiatru, trzeba kolejno rozwiązać następujące zagadnienia:

1) wyznaczyć prawdopodobieństwo wystąpienia wiatru o prędkości $v > 4$ m/s (tzw. wiatr użyteczny);
2) utożsamić to prawdopodobieństwo z czasem występowania w długim okresie wiatru użytecznego;
3) wyznaczyć prędkość średnią wiatru w zakresie wiatru użytecznego.

Pierwszy problem sprowadza się do obliczenia wyrażenia

$$P(v > v_z) = e^{-\left(\frac{v_z}{\beta}\right)^\gamma} = e^{-\left(\frac{4}{\beta}\right)^\gamma}.$$

Rozwiązanie drugiego zagadnienia wynika automatycznie z pierwszego:

$$t = 8760\, e^{-\left(\frac{v_z}{\beta}\right)^\gamma},$$

gdzie:

t - przeciętna liczba godzin w roku, podczas których występuje wiatr użyteczny.

Bardziej złożone jest zagadnienie trzecie. Wartość średnią wiatru $v_{śr}$ w zakresie wiatru użytecznego wyznacza się z następującego równania:

$$e^{-\left(\frac{v_{śr}}{\beta}\right)^\gamma} = 0{,}5\, e^{-\left(\frac{4}{\beta}\right)^\gamma}.$$

Po podwójnym zlogarytmowaniu i przekształceniach z równania tego można otrzymać:

$$v_{śr} = e^{\frac{\ln(4^\gamma + 0{,}69 \cdot \beta^\gamma)}{\gamma}}.$$

Przykładowo można obliczyć $v_{śr}$ dla Warszawy (i najbliższych jej okolic):

$\gamma \approx 2, \qquad \beta \approx 5{,}5$

$$P(v > v_z) = e^{-\left(\frac{4}{5{,}5}\right)^2} \approx 0{,}59$$ lub w procentach 59%.

$t = 8760 \cdot 0{,}59 \approx 5170$ h

$$v_{śr} = e^{\frac{\ln(36{,}9)}{2}} \approx e^{1{,}8} \approx 6{,}05 \text{ m/s}.$$

Jednostkowa energia użyteczna wiatru E jest energią kinetyczną wiatru użytecznego na jednostkową powierzchnię ustawioną prostopadle do kierunku strumienia powietrza:

$$E = \frac{\rho\, v_{śr}^3\, t}{2} \cdot 2{,}778 \cdot 10^{-7}\ [\mathrm{kWh/m^2}],$$

gdzie:

ρ - gęstość powietrza w temperaturze 15°C przy ciśnieniu 0,1 MPa wynosi 1,209 kg/m^3;

$v_{śr}$ - średnia prędkość wiatru;

t - czas występowania wiatru użytecznego;

czynnik $2{,}778 \cdot 10^{-7}$ wynika z dopasowania jednostek J do kWh.

Dla obliczonej dla okolic Warszawy wartości $v_{śr} = 6{,}05$ m/s energia użyteczna wiatru wynosi za czas 1 roku:

$$E = \frac{1{,}209 \cdot 6{,}05^3 \cdot 5170 \cdot 3600}{2} \cdot 2{,}778 \cdot 10^{-7}\ [\mathrm{kWh/m^2 \cdot rok}] \approx$$
$$\approx 692{,}7 \approx 700\ \mathrm{kWh/m^2 \cdot rok}$$

Znając powierzchnię zamiataną przez łopaty wirnika generatora wiatrowego, można przez pomnożenie jej przez obliczoną wartość E uzyskać szacunkową wartość energii przetwarzanej przez generator wiatrowy. Jednak energia ta nie jest w całości przetwarzana na energię elektryczną przez generator wiatrowy. Aby wyznaczyć ilość wytworzonej energii elektrycznej, trzeba posłużyć się krzywymi mocy generatorów wiatrowych.

Przykładowo dla generatora EW 160-22-30 (jedynego seryjnie produkowanego w Polsce) dla $v_{śr} = 6$ m/s odpowiadająca tej wartości moc tego generatora wynosi: 23 kW - co w roku odpowiada energii:

$$E = 23\ \mathrm{kW} \cdot 5170\ \mathrm{h} \approx 119\ \mathrm{MWh} \approx 120\ \mathrm{MWh}.$$

Do przybliżonych szacunków mocy generatora wiatrowego można także skorzystać z faktu, że energia, a zatem i moc wiatru, jest pro-

porcjonalna do trzeciej potęgi prędkości wiatru. Mając więc dla danego generatora wiatrowego moc znamionową dla określonej znamionowej prędkości wiatru, można oszacować moc generatora dla rzeczywistych warunków przez pomnożenie mocy znamionowej przez czynnik $(v_{śr}/v_{zn})^3$. Trzeba jednak pamiętać, że w ten sposób obliczona średnia moc generatora jest dostępna w roku tylko przez obliczony czas występowania w roku wiatru użytecznego.

8. ANALIZA CENY JEDNOSTKOWEJ ENERGII ELEKTRYCZNEJ DOSTARCZANEJ PRZEZ SYSTEMY OPARTE NA ZASTOSOWANIU ŹRÓDEŁ ALTERNATYWNYCH

Wyniki przeprowadzonej analizy bardzo mocno zależą od uczynionych założeń dotyczących sposobu działania poszczególnych systemów zasilania i roli, jaką mają spełniać poszczególne elementy tych systemów, a zwłaszcza alternatywne źródła energii. Proponuje się rozważyć niżej podane alternatywne systemy zasilania oparte na alternatywnych źródłach energii.

Najpierw omówiono **system autonomiczny,** w którym **źródłem alternatywnym jest bateria słoneczna**. Przeciętnie od kwietnia do września bateria słoneczna powinna dostarczać energii elektrycznej w takiej ilości, aby można było zasilać odbiory, nie korzystając z innych podstawowych źródeł energii. W ciągu dnia energia z baterii słonecznej powinna zasilać zatem odbiory technologiczne oraz służyć do ładowania baterii akumulatorów. Rezerwa bateryjna powinna wynosić co najmniej 13 godzin (wynika to z wykresu średniego natężenia promieniowania w kwietniu - rys. 4). W przypadkach losowych - wielodniowej, niekorzystnej pogody, jak również w okresie październik ÷ marzec niedobory energii byłyby uzupełniane przez użycie zespołu prądotwórczego. Średni poziom natężenia promieniowania słonecznego dla szerokości geograficznej Warszawy w kwietniu, jak

to wcześniej pokazano, wynosi ok. 250 W/m^2. Parametry modułów elektrowni słonecznej, takie jak maksymalne prądy obciążenia, a więc i moce, są zatem równe około 25% w stosunku do wymienionych przez producentów danych znamionowych (producenci podają dane dla natężenia promieniowania słonecznego równego 1 000 W/m^2).

W omawianym systemie autonomicznym problemem jest zarówno niedobór podaży energii słonecznej w okresie październik ÷ marzec, jak i zagospodarowanie nadwyżek tej energii, zwłaszcza w okresie czerwiec ÷ sierpień. Dlatego system autonomiczny jest niekorzystny i stosowanie jego należy ograniczyć tylko do przypadków, gdzie jest to konieczne.

Następnie przedstawiono **system nieautonomiczny (tzn. współpracujący z siecią elektroenergetyczną) z baterią słoneczną**, w którym **sieć elektroenergetyczna stanowi podstawowe źródło rezerwowe**. W systemie tym rezerwa bateryjna jest na ogół mniejsza, a niedobory energii w nocy mogą być w dużej części uzupełniane z sieci. Nadwyżki energii uzyskiwane w miesiącach letnich (duża podaż energii promieniowania słonecznego) są zwracane do sieci elektroenergetycznej dzięki odpowiedniemu układowi.

W systemie współpracującym z siecią można w zasadzie przyjąć dowolnie poziom, na jakim energia w systemie zasilania pochodzi ze źródła alternatywnego. W artykule przyjęto dla systemu współpracującego z siecią, na potrzeby przeprowadzanej analizy, takie same założenia, jakie wcześniej zrobiono dla systemu autonomicznego, tzn.: energia dostarczana ze źródeł alternatywnych jest na takim poziomie, że przy średnich warunkach podaży tej energii, jest ona praktycznie wystarczająca do pokrycia zapotrzebowania od kwietnia do września, bez konieczności zasilania z sieci elektroenergetycznej (poza przypadkami wymagającymi działania źródeł rezerwowych). Inne założenia, zmniejszające rolę alternatywnych źródeł energii, prowadziłyby do zatarcia charakteru systemów zasilania, jako systemów opartych na zastosowaniu źródeł alternatywnych. Oczywiście można zmienić

przedstawione założenia. Wpłynie to na zmianę wyników podanej w dalszym ciągu analizy. Wydaje się jednak, że uczynione założenia dotyczące systemów zasilania są sensowne.

Na zakończenie przeanalizowano **układ hybrydowy współpracujący z siecią**, złożony **z elektrowni słonecznej i generatora wiatrowego**. Dzięki temu można zmniejszyć moc zainstalowaną elektrowni słonecznej o moc przeciętną uzyskiwaną z elektrowni wiatrowej. Dodać należy, że w warunkach polskich największa podaż energii wiatrowej występuje w okresie jesienno-zimowym, a zatem w czasie, gdy podaż energii promieniowania słonecznego jest najniższa, więc **oba rodzaje energii w przeciągu roku dobrze się uzupełniają**.

8.1. Skompletowanie systemu zasilania opartego na bateriach słonecznych

8.1.1. Wybór modułów baterii słonecznych

Do celów analizy wybrano następujące typy modułów baterii słonecznych: MSX-50, MSX-60, MSX-120, firmy Solarex oraz SM-55, firmy Siemens. Podstawowe parametry rozpatrywanych modułów baterii ujęto w tablicy 3.

Tablica 3

Parametry modułów baterii słonecznej

Typ modułu	Napięcie jałowe [V]	Napięcie znamionowe [V]	Znamionowy prąd obciążenia [A]	Prąd zwarcia [A]	Powierzchnia [m^2]
MSX-50	21,1	17,1	2,9	3,17	0,47
MSX-60	21,1	17,1	3,5	3,8	0,556
MSX-120	21,1	17,1	7,0	7,6	1,1
SM-55	21,8	17,4	3,05	3,35	0,427

Moc znamionowa modułów baterii słonecznych jest łatwa do zidentyfikowania z oznaczenia ich typu - jest to część liczbowa oznaczenia.

Przyjęto, że łączna sprawność systemu zasilania, liczona jako stosunek mocy wyjściowej systemu do mocy energii elektrycznej uzyskiwanej na wyjściu z modułów baterii słonecznej, wynosi 0,8. Dla mocy odbiorów 10 kW należy przewidzieć zatem moc łączną modułów jako: 10 kW · 1,25 = 12,5 kW.

Jak wcześniej wspomniano, parametry modułów należy przeliczyć dla średniego natężenia promieniowania 250 W/m^2. Dla tych warunków moduły przy znamionowym prądzie obciążenia mają następujące moce:

- MSX-50: 12 W;
- MSX-60: 14,3 W;
- MSX-120: 28 W;
- SM-55: 12,6 W.

Do wytworzenia mocy 12,5 kW elektrownia powinna składać się z następującej liczby modułów:

- MSX-50: 1050;
- MSX-60: 825;
- MSX-120: 440;
- SM-55: 990.

Łączna powierzchnia modułów przy powyższych założeniach wynosi odpowiednio:

- MSX-50: 490 m^2;
- MSX-60: 486 m^2;
- MSX-120: 486 m^2;
- SM-55: 423 m^2.

Są to bardzo duże powierzchnie. Nie wdając się w szczegółowe rozwiązania należy przypuszczać, że cała bateria zostanie zrealizowana w formie kilkunastu równolegle połączonych sekcji o odpowiednio

mniejszych powierzchniach. Część modułów baterii będzie można umieścić na dachu budynku siłowni.

8.1.2. Dobór innych elementów systemu

Bateria akumulatorów powinna zapewnić w systemie autonomicznym rezerwę nie mniejszą niż 13 godzin, więc jej pojemność znamionowa powinna wynosić 13 · 200 Ah = 2 600 Ah. Przykładowo mogą być to następujące typy baterii: 20 OPzV 2 500, firmy Warta lub Sonnenschein albo ETG - 2 900, firmy Bater.

Jako falownik, czyli siłownię prądu przemiennego można przyjąć SPA 20/3 · 3,3 lub SPA 20/5 · 1,8, firmy Telzas.

Brak jest w dostępnych ofertach danych na temat przetwornicy prądu stałego o odpowiednich parametrach, jednak jej cenę uznać można za zbliżoną do siłowni rozpatrywanych dla systemu klasycznego.

8.2. Kalkulacja cenowa poszczególnych elementów systemu zasilania opartego na bateriach słonecznych

8.2.1. Obliczenie kosztu baterii słonecznej

Na podstawie cenników niemieckich i cennika firmy GTB-Solaris (filii w Polsce) ceny poszczególnych modułów można przyjąć następująco:

- MSX-50: 2 050 zł;
- MSX-60: 2 350 zł;
- MSX-120: 4 600 zł;
- SM-55: 2 160 zł.

Są to ceny przybliżone, lecz bardzo prawdopodobne, z lutego 1998 roku.

W związku z tym koszt całej baterii słonecznej o rozważanej mocy, złożonej z modułów poszczególnych typów, wyniesie:

- MSX-50: 2 152 500 zł;
- MSX-60: 2 056 250 zł;
- MSX-120: 2 024 000 zł;
- SM-55: 2 138 400 zł.

Jak widać, można przyjąć, że **koszt baterii** wyniesie **2 000 000 zł**. Koszt ten wynika także z działania pośredników, przy bezpośrednim imporcie koszt ten byłby niższy o około 50%.

Koszt instalacji modułów baterii łącznie z kosztami fundamentowania przyjęto jako 15% kosztu modułów, wyniesie on więc: **300 000 zł**.

8.2.2. Koszt pozostałych urządzeń

Koszt baterii akumulatorów, zawierającej ogniwa przedstawionych typów wyniesie około 125 000 zł. Biorąc pod uwagę, że bateria musi być rezerwowana, należy tę sumę pomnożyć przez 2, więc sumaryczny koszt baterii wyniesie około **250 000 zł**.

Koszt i typ **zespołu prądotwórczego** jest taki sam, jak dla rozważanego wcześniej klasycznego systemu zasilania i wynosi **30 000 zł**.

Koszt przetwornicy DC/DC, zgodnie z wcześniejszymi założeniami, przyjmuje się, że wyniesie **50 000 zł**.

W układzie nieautonomicznym występują także: falownik i siłownia.

Koszt falownika wymienionego wcześniej typu, zgodnie z cennikiem, wynosi **70 000 zł**.

Koszt i typ **siłowni** jest taki sam, jak w rozważanym wcześniej systemie klasycznym i wynosi **50 000 zł**.

Koszt wyposażenia dodatkowego (m.in. elektroniczny system sterowania) szacuje się na około **30 000 zł**.

Koszty projektu, koszty dodatkowe oraz koszty instalacji urządzeń (z wyłączeniem kosztów instalacji modułów baterii słonecznej) wyniosą około 10% sumarycznego kosztu urządzeń (bez baterii słonecznej): **50 000 zł**.

Łącznie koszt urządzeń bez baterii słonecznej dla układu autonomicznego wyniesie zatem:

- bateria akumulatorów:	250 000 zł
- przetwornica DC/DC:	50 000 zł
- zespół prądotwórczy:	30 000 zł
- siłownia:	50 000 zł
- wyposażenie dodatkowe:	30 000 zł
- koszty instalacji baterii z wyłączeniem kosztu fundamentowania:	150 000 zł
- koszty dodatkowe i instalacja pozostałych urządzeń:	50 000 zł
Razem:	610 000 zł
- bateria słoneczna:	2 000 000 zł

Łączny koszt urządzeń wyniesie więc: ≈ **2 610 000 zł**.

8.2.3. Koszt działki i budynku siłowni

Powierzchnia łączna modułów wchodzących w skład baterii wynosi około 500 m^2. Biorąc pod uwagę, że powierzchnia baterii (a ściślej sekcji, na jakie będzie podzielona bateria) będzie ustawiona pod kątem około 35° względem powierzchni ziemi, powierzchnia zajmowana przez baterię wyniesie: 500 $m^2 \cdot \cos(35°) \approx 400$ m^2. Pamiętając jednak o konieczności odstępów między poszczególnym sekcjami zakłada się, że **powierzchnia gruntu potrzebna do zainstalowania baterii słonecznej** o wymienionej powierzchni wyniesie **500 m^2**. Problemem niewątpliwie jest tak duża powierzchnia. Złagodzić go nieco może możliwość wykorzystania dachu budynku siłowni jako miejsca do instalacji pewnej liczby modułów baterii.

Przewiduje się także, że **powierzchnia budynku siłowni**, głównie ze względu na większe rozmiary baterii, powinna wynosić około **40 m^2**. Szacuje się, biorąc pod uwagę powyższe dane, że powierzchnia działki powinna wynosić nie mniej niż **600 m^2**, zatem

koszt działki, przy przyjętych uprzednio wskaźnikach, wyniesie 600 · 100 zł = **60 000 zł** lub 1 500 zł/m^2 - w przeliczeniu na 1 m^2 budynku.

Koszt budynku, przy przyjętych uprzednio wskaźnikach, wyniesie 40 · 1 750 zł = **70 000 zł**.

Łączny koszt budynku i działki wyniesie: 70 000 + 60 000 = = **130 000 zł**.

8.2.4. Inne założenia niezbędne do analizy

Czasy amortyzacji poszczególnych składników majątkowych są takie, jak wcześniej podano:

- urządzeń: 10 lat,
- budynku siłowni: 25 lat.

Inwestycja jest dwuletnia. **Pierwszy rok obejmie koszty** związane z budową budynku - **130 000 zł** oraz fundamentowaniem - część kosztów instalacji baterii około **150 000 zł**. W drugim roku natomiast należy uwzględnić koszty związane z zakupem i instalacją oraz uruchomieniem urządzeń wchodzących w skład systemu zasilania odbiorów.

Zakłada się również, że koszty eksploatacji wzrosną około dwukrotnie w stosunku do analogicznych rozpatrywanych dla klasycznego systemu zasilania. Spowodowane jest to wieloma czynnikami, m.in. tym, że bateria akumulatorów ma większą pojemność, co implikuje wyższe koszty eksploatacji, także rola zespołu prądotwórczego jest znacznie większa - przewiduje się większą liczbę godzin pracy zespołu, co zwiększa koszty eksploatacji. System zawiera większą liczbę urządzeń, w tym również urządzeń, z którymi eksploatacja nie miała dotychczas doświadczeń, wymaga to zwiększonych kosztów eksploatacji m.in. na szkolenia. Podsumowując, wydaje się w pełni uzasadnione przekonanie, że **koszty eksploatacji** wzrosną w przewidywanej skali i wyniosą w skali roku **30 000 zł**.

Łączny koszt inwestycyjny w pierwszym roku wyniesie: 130 000 + 150 000 = **280 000 zł.**

8.2.5. Obliczenia rocznych rat zwrotu kapitału dla poszczególnych składników majątkowych

Obliczenie rocznych rat zwrotu kapitału przeprowadza się tak, jak w pkt. 4.4., zgodnie z tym roczna rata zwrotu kapitału r_n wynosi:
- dla urządzeń: 0,23;
- dla budynku: 0,2.

Koszty poniesione w pierwszym roku inwestycji ulegają modyfikacji przez zastosowanie rachunku dyskonta zgodnie z pkt. 4.5. i wyniosą:

$$I = 280\,000 \cdot 1{,}13 = 316\,400 \text{ zł} \approx \mathbf{320\,000\ zł}.$$

8.2.6. Koszt jednostkowy 1 kWh dla autonomicznego systemu zasilania z baterią słoneczną

Koszt 1 kWh jest obliczany w sposób podany w pkt. 4.6. Po podstawieniu danych otrzyma się:

$$k = \frac{2\,610\,000 \cdot 0{,}23 + 320\,000 \cdot 0{,}2 + 30\,000}{87\,600} \approx \mathbf{7{,}9\ zł/kWh}\ .$$

Warto podkreślić, że koszty urządzeń stanowią około 90% całkowitych kosztów inwestycyjnych.

8.3. Analiza kosztu 1 kWh dla układu zasilania opartego na baterii słonecznej i współpracującego z siecią elektroenergetyczną

W analizie tego układu należy uwzględnić koszt dodatkowych urządzeń, takich jak falownik oraz siłownia, natomiast można rozważyć ewentualne zmniejszenie pojemności baterii, chociaż jeśli

system ma zachować charakter systemu alternatywnego, to w cyklu dobowym w normalnych warunkach nasłonecznienia nie powinna zachodzić konieczność pobierania energii z sieci elektroenergetycznej.

Dodatkowo należy uwzględnić wpływy uzyskiwane z nadwyżek energii zwracanych do sieci w miesiącach letnich oraz koszt niedoborów energii w miesiącach jesienno-zimowych.

Na podstawie danych IMiGW dla średniego natężenia promieniowania w poszczególnych miesiącach (patrz rys. 3) można, przy założeniu, że średnia dobowa moc natężenia promieniowania w kwietniu wynosi 250 W/m^2 (patrz pkt. 6.2), podać następujące wartości w jednostkach względnych (przy założeniu, że poziom ten jest równy 1 dla kwietnia): styczeń - 0,15, luty - 0,3, marzec - 0,7, kwiecień - 1, maj - 1,35, czerwiec - 1,5, lipiec - 1,46, sierpień - 1,25, wrzesień - 0,92, październik - 0,46, listopad - 0,13, grudzień - 0,09.

Należy przy tym zaznaczyć, że w okresie kwiecień ÷ wrzesień dane te są nieco zawyżone ze względu na to, że promieniowanie przed godz. 6.00 i po godz. 18.00 w rzeczywistości nie dociera do powierzchni aktywnej baterii słonecznej i nie powinno go się uwzględniać. Na podstawie normy PN-76/B-03420 wyznaczono, jaki jest udział energetyczny wymienionego promieniowania dla czerwca (w miesiącu tym udział tego promieniowania jest największy). Obliczony w ten sposób błąd względny dla czerwca okazał się mniejszy od 5%. Można uznać, że jest to błąd maksymalny - w przypadku pozostałych miesięcy jest niższy. Jak widać z powyższych danych, nadwyżki energii występują: w maju - 0,35, czerwcu - 0,5, lipcu - - 0,46, sierpniu - 0,25.

Łączna nadwyżka energii wynosi:

$$\approx (0{,}35 + 0{,}5 + 0{,}46 + 0{,}25) \cdot 10 \text{ kW} \cdot 30 \cdot 24 = 11\,232 \text{ kWh} \approx \mathbf{11\,000\ kWh}$$

(wynik zaokrąglono w dół ze względu na zawyżone wartości promieniowania w okresie kwiecień ÷ wrzesień - patrz wyżej). Przyjmując

cenę energii zgodnie z taryfą C11: 0,27 zł/kWh **wartość zwracanej energii** w ciągu roku wyniesie ≈ **3 000 zł**.

Niedobory energii w poszczególnych miesiącach są następujące: w styczniu - 0,85, lutym - 0,7, marcu - 0,3, wrześniu - 0,08, październiku - 0,54, listopadzie - 0,87, grudniu - 0,91.

Łącznie niedobór energii w ciągu roku wynosi:

$$\approx 4{,}25 \cdot 10 \text{ kW} \cdot 30 \cdot 24 \cdot 1{,}25 = 40\,050 \text{ kWh} \approx \mathbf{40\,000\ kWh}.$$

Koszt tej energii odpowiada około **10 800 zł.** Bilansując niedobór z nadwyżką - w skali roku wynikowy **koszt pobieranej energii** wyniesie około **7 800 zł**.

Łączny koszt urządzeń wchodzących w skład omawianego systemu zasilania wynosi: 2 610 000 + 70 000 = **2 680 000 zł** (do kosztu urządzeń dla systemu autonomicznego dodaje się koszt falownika). Dodając obliczony koszt energii elektrycznej z sieci otrzyma się łączny koszt roczny:

$$K_r = 2\,680\,000 \cdot 0{,}23 + 320\,000 \cdot 0{,}2 + 30\,000 + 7\,800 = 718\,200 \text{ zł}.$$

Liczba kWh zużywanych przez odbiory w roku (przy założeniu maksymalnego zapotrzebowania) wynosi: 8 760 h · 10 kW = = 87 600 kWh.

Koszt jednostkowy roczny energii elektrycznej wynosi:

$$k = 718\,200 \text{ zł} : 87\,600 \text{ kWh} \approx \mathbf{8{,}2\ zł/kWh}.$$

8.4. Analiza kosztu jednostkowego energii dla hybrydowego układu zasilania, współpracującego z siecią elektroenergetyczną

Układ mieszany (hybrydowy) cechuje się tym, że zastosowano w nim dwa typy źródeł alternatywnych (w jednym systemie zasilania). Najczęściej stosuje się generatory wiatrowe i baterie słoneczne.

Na początku analizy należy przyjąć założenia na temat układu hybrydowego. Używanie generatora wiatrowego wraz z baterią słoneczną jest w pewnej mierze uzasadnione wzajemnym uzupełnianiem się podaży poszczególnych rodzajów energii. Podaż energii wiatrowej w warunkach polskich jest najniższa w okresie letnim, lecz wtedy jest najwyższa podaż energii promieniowania słonecznego. Z kolei wyższa podaż energii wiatrowej w pozostałych okresach (głównie jesień-zima) trafia na okres niskiej podaży promieniowania słonecznego (zgodnie z danymi IMiGW w Polsce najbardziej wietrzną porą jest zima). W związku z tym łączna podaż obu składników energii jest bardziej równomierna i zwiększa pewność zasilania. W efekcie można zmniejszyć czas rezerwy bateryjnej, a więc i pojemność baterii. Wydaje się rozsądne założenie, aby udział poszczególnych rodzajów źródeł alternatywnych w uzyskiwaniu energii w systemie był jednakowy, czyli po około 50% potrzebnej energii powinien dostarczać generator wiatrowy i tyleż samo bateria słoneczna.

Generator wiatrowy powinien zatem dostarczać energię elektryczną o przeciętnej mocy 5 kW, a moc baterii słonecznej (i wszystkie jej pochodne od mocy parametry) przy tych założeniach może być dwukrotnie zmniejszona (też do wartości 5 kW). Moc znamionową generatorów wiatrowych z reguły podaje się dla prędkości wiatru $12 \div 14$ m/s. Natomiast przeciętna prędkość wiatru na obszarze Polski jest niższa, np. dla okolic Warszawy wynosi ona około 6 m/s, jak podano w pkt. 7. Energia kinetyczna wiatru (por. pkt 7) jest w przybliżeniu proporcjonalna do prędkości wiatru w trzeciej potędze, zatem jeśli prędkość wiatru jest dwukrotnie wyższa, to moc wiatru jest aż ośmiokrotnie wyższa. Moc znamionowa generatora wiatrowego, przy podanych założeniach, powinna więc wynosić około $2^3 \cdot 5$ kW = 40 kW. W tablicy 4 zamieszczono przykładowe dane generatorów wiatrowych firmy Bay Winds.

Cena wszystkich podanych modeli jest bardzo zbliżona i wynosi (bezpośrednio u producenta) około 30 000 USD (ok. 105 000 zł).

Ze względu na zbliżony koszt modeli najkorzystniej jest zastosować model 29-20. Aby pokryć podaną w założeniach moc (5 kW), musimy zastosować dwa generatory. **Koszt generatorów wiatrowych** wyniósłby zatem 210 000 zł. Należy do tego dodać koszty pośrednie związane z pośrednikami na rynku i podatek VAT, łącznie co najmniej 40%, tj. 84 000 zł. Koszt samych urządzeń wyniósłby więc około **300 000 zł**.

Tablica 4

Parametry generatorów wiatrowych firmy Bay Winds

Parametry	Oznaczenie typu generatorów				
	23-10	23-12	24-15	26-17	29-20
Moc znamionowa [kW]	10	12,5	15	17,5	20
Minimalna prędkość wiatru [m/s]	4	4	4	4	4
Nominalna prędkość wiatru*) [m/s]	12,5	13,5	14	13,5	13
Liczba łopat	3	3	3	3	3
Średnica wirnika [m]	6,9	6,9	7,2	7,8	8,7
Wysokość wieży [m] / masa wieży [kg]	opcjonalnie: 24/1980, 30/2880, 36/3730				

*) Jest to prędkość wiatru, przy której generator uzyskuje moc znamionową.

W Polsce jest produkowany seryjnie jeden typ generatora wiatrowego, a mianowicie EW 160-22-30 (Zakład Nowomag). Moc znamionowa generatora wynosi 160 kW, jest ona osiągana przy prędkości wiatru 13 - 14 m/s. Dla średniej prędkości wiatru użytecznego w okolicach Warszawy, a wynoszącego ~ 6 m/s, moc generatora EW 160-22-30, wyznaczona z krzywej mocy generatora, wynosi 23 kW.

Następnie przeanalizowano koszty wytwarzania energii w przedstawionym wcześniej układzie (współpracującym z siecią), wyposażo-

nym w generator wiatrowy EW 160-22-30 lub dwa generatory typu 29-20 firmy Bay Winds. Zakłada się, że rezerwa bateryjna baterii akumulatorów w rozpatrywanych układach wynosi 3 godziny.

W kosztach należy uwzględnić następujące dodatkowe koszty związane z wyposażeniem systemu w generator wiatrowy:

- zakup generatora z pełnym wyposażeniem;
- jego montaż i uruchomienie;
- fundamentowanie wieży generatora;
- podłączenie systemu do sieci energetycznej;
- koszty dodatkowe, obejmujące projekt, konieczne ekspertyzy i dokumentacje;
- układ sterowania nadzorujący i integrujący działanie systemu oraz kierujący współpracą poszczególnych elementów systemu.

Na podstawie oferty Nowomagu (I poł. 1998 r.) **koszt** zakupu **generatora typu EW 160-22-30** wraz z transportem, montażem i uruchomieniem wynosił 421 000 zł + 22% ≈ **514 000 zł.**

Pozostałe koszty szacuje się następująco:

- koszt fundamentowania ok. 50 000 zł,
- koszty związane z podłączeniem do sieci ok. 30 000 zł,
- koszty inne ok. 25 000 zł,
- układ sterowania 30 000 zł.

Łącznie koszty dodatkowe poniesione w pierwszym roku inwestycji wyniosą: 50 000 + 25 000 = **75 000 zł. Uwzględniając rachunek dyskonta** otrzyma się wartość kosztu w pierwszym roku 1,13 · 75 000 zł ≈ **85 000 zł. Koszt inwestycji w pierwszym roku** wynosi 320 000 + 85 000 = **405 000 zł.**

Natomiast koszty dodatkowe poniesione w drugim roku wynoszą: 514 000 + 30 000 + 30 000 = **574 000 zł.**

Koszty urządzeń wchodzących w skład rozpatrywanego systemu zasilania wyniosą **1 894 000 zł.**

Składają się na nie:

- bateria słoneczna: 1 000 000 zł
- generator wiatrowy: 574 000 zł
- bateria akumulatorów: 90 000 zł
- siłownia: 50 000 zł
- falownik: 70 000 zł
- przetwornica DC/DC: 50 000 zł
- zespół prądotwórczy: 30 000 zł
- układ sterowania: 30 000 zł

Należy także uwzględnić koszt nadwyżek energii odprowadzanych do sieci. Średnia wydajność baterii słonecznej w roku (bateria o podanych parametrach) wynosi 2,9 kW.

Jak wcześniej podano, średnia wydajność generatora wiatrowego w roku wynosi 23 kW. W odniesieniu do napięcia stałego odpowiada to mocy 18,4 kW. Łącznie daje to moc systemu 21,3 kW. Zapotrzebowanie na moc w rozpatrywanym systemie wynosi 10 kW. Nadwyżka mocy wynosi zatem 11,3 kW w odniesieniu do napięcia stałego, co odpowiada mocy ~ 9 kW w odniesieniu do napięcia sieci elektroenergetycznej. Wielkość nadwyżek energii w roku odpowiadających tej mocy wynosi: 8 760 h · 9 kW = 78 840 kWh.

Wartość tej energii według taryfy C11 wynosi:

$$78\ 840\ \text{kWh} \cdot 0{,}27\ \text{zł/kWh} \approx \mathbf{21\ 300\ zł}.$$

Po uwzględnieniu powyższych składników można wyznaczyć **koszt roczny**. Wynosi on:

$$K_r = 1\ 894\ 000 \cdot 0{,}23 + 405\ 000 \cdot 0{,}2 + 30\ 000 - 21\ 300 = \mathbf{= 526\ 320\ zł}.$$

Jednostkowy koszt roczny energii w systemie wyposażonym w generator EW 160-22-30 wynosi:

$$k = \frac{526\ 320\ \text{zł}}{87\ 600\ \text{kWh}} \approx \mathbf{6{,}0\ zł/kWh}\ .$$

Należy rozpatrzyć teraz wariant dla systemu wyposażonego w dwa generatory typu 29-20 firmy Bay Winds. Kalkulacje przeprowadzono analogicznie, jak dla poprzedniego wariantu systemu. Trzeba jednak uwzględnić dodatkowe koszty montażu i uruchomienia generatorów wiatrowych (w przypadku generatora EW 160-22-30 koszt ten był wliczony w cenę urządzenia). Szacuje się wysokość tego kosztu na 15% kosztu generatorów, czyli 45 000 zł.

Łączny koszt urządzeń wyniesie zatem: **1 665 000 zł**.

Należy uwzględnić także **koszt niedoboru energii**, który trzeba uzupełnić z sieci energetycznej. Jak podano wyżej, średnia wydajność baterii słonecznej w odniesieniu do napięcia stałego wynosi: 2,9 kW. Wydajność generatora wiatrowego 0,8 · 5 kW = 4 kW. Łącznie wydajność źródeł alternatywnych wynosi więc 6,9 kW. Niedobór mocy wynosi zatem: 10 - 6,9 = 3,1 kW (w odniesieniu do napięcia stałego). Odpowiada to około 3,8 kW w odniesieniu do napięcia sieci elektroenergetycznej. Wielkość energii odpowiadająca tej mocy w ciągu roku wynosi: 8 760 h · 3,8 kW = 33 290 kWh. Koszt tej energii według taryfy C11 wynosi: 33 290 kWh · 0,27 zł/kWh = = 7 990 zł ≈ **9 000 zł.**

Po uwzględnieniu powyższych składników można wyznaczyć **koszt roczny**. Wynosi on:

$$K_r = 1\,665\,000 \cdot 0{,}23 + 405\,000 \cdot 0{,}2 + 30\,000 + 9\,000 = \\ = \mathbf{502\,950\ zł}.$$

Jednostkowy koszt roczny energii w systemie wyposażonym w dwa generatory wiatrowe typu 29-20 firmy Bay Winds wynosi:

$$k = \frac{502\,950\ \text{zł}}{87\,600\ \text{kWh}} \approx \mathbf{5{,}7\ zł/kWh}.$$

Warto podkreślić, że koszt urządzeń stanowi około 85% całkowitego kosztu inwestycji.

9. PODSUMOWANIE

W tablicy 5 podano zestawienie kosztu rocznego energii dla wszystkich rozpatrywanych wariantów.

Tablica 5

Roczny koszt jednostkowy energii dla różnych wariantów systemów zasilania

Wariant systemu zasilania	Łączny koszt roczny [zł]	Koszt jednostkowy [zł/kWh]	Koszt względny
Tradycyjny 10 kW	103 250	1,2	1,0
Alternatywny, autonomiczny	694 300	7,9	6,6
Alternatywny, współpracujący z siecią	718 200	8,2	6,8
Alternatywny, hybrydowy	526 320 / 502 950	6 / 5,7	5 / 4,8

Z przeprowadzonej analizy wynika, że energia uzyskiwana i przetwarzana w systemie, zawierającym alternatywne źródła energii jest około 5 ÷ 7 razy droższa od energii przetwarzanej w układzie konwencjonalnym. Analiza została wykonana dla typowego układu zasilania o przeciętnych parametrach (10 kW). Ze względu na ograniczoną objętość artykułu jest to analiza jednopunktowa. Nie umożliwiło to przeprowadzenia w sposób pewny ekstrapolacji wyników na obiekty o parametrach znacznie różniących się od rozpatrywanych, zwłaszcza różniących się mocą.

Wyniki obliczeń ceny energii dla konwencjonalnego systemu zasilania o mocy 50 kW wykazały, że koszt 1 kWh w tym systemie jest, zgodnie z przewidywaniami, niższy niż dla systemu 10 kW. Również, jak należy przewidywać, dla alternatywnego systemu zasilania o mocy 50 kW koszt jednostkowy energii będzie niższy, niż dla tego typu systemów o mocy 10 kW. Należy też oczekiwać, że dla

systemów alternatywnych o mocy mniejszej niż 10 kW koszt jednostkowy energii będzie wyższy. Najbardziej ekonomiczne wydają się systemy mieszane, składające się z dwóch typów źródeł alternatywnych: baterii słonecznej i generatora wiatrowego.

Trzeba zwrócić uwagę na to, że w przeprowadzonej analizie przyjęto wartości cen aktualne w połowie 1998 r. Zmiana cen, związana z inflacją (ok. 10% w skali roku), wpłynie niewątpliwie na zmianę bezwzględnych wartości obliczonych wskaźników, jednak wartości względne pozostaną w przybliżeniu takie same. Jednostkowe koszty energii uzyskiwanej w układach, zawierających źródła alternatywne będą w przyszłości niższe ze względu na to, że inwestycje ekologiczne, do których należy zaliczyć również inwestycje w energetykę alternatywną, zostaną objęte preferencjami, które wpłyną na obniżkę tych kosztów. Na początku 1999 roku zostały wprowadzone następujące preferencje:

- umożliwiono uzyskanie preferencyjnych kredytów w Banku Ochrony Środowiska (oprocentowanie 7% w skali roku na 7 lat);
- wprowadzono obowiązek zakupu energii ze źródeł odnawialnych po preferencyjnych cenach przez przedsiębiorstwa zajmujące się obrotem i sprzedażą energii (na podstawie rozporządzenia ministra gospodarki, wydanego 4. lutego 1999 r.).

Na obniżenie tych kosztów wpłynie także fakt, że koszt podstawowych urządzeń, takich jak moduły baterii słonecznych, w przeliczeniu na jednostkę mocy sukcesywnie zmniejsza się, a jak wynika z artykułu, dla układów alternatywnych koszt urządzeń stanowi 80 ÷ 90% kosztów całkowitych.

WYKAZ LITERATURY

1. Atlas zasobów, walorów i zagrożeń środowiska geograficznego Polski. PWN, Warszawa 1994.

2. Binkiewicz A.: Analiza możliwości zastosowania alternatywnych źródeł energii w systemie zasilania urządzeń i obiektów łączności. Instytut Łączności, Warszawa 1997.
3. Cennik Robót Budowlanych. Ośrodek Wdrożeń Budownictwa „Promocja", Warszawa 1998.
4. Dmowski A.: Ogólne właściwości i sposób eksploatacji baterii fotowoltaicznych. Mat. z seminarium PW, Warszawa 1998.
5. Elementy rachunku ekonomicznego. Praca zbiorowa. PWN, Warszawa 1985.
6. Fotowoltaika - ogniwa słoneczne i detektory podczerwieni. Wykłady i komunikaty XII Szkoły Optoelektroniki. Kazimierz Dolny 1997.
7. International Energy Agency: Renevable energy technology application. OECD/IAE, Paris 1991.
8. Jastrzębski Z.M.: Energia słoneczna. PWN, Warszawa 1990.
9. Katalogi firm: Sonnenschein, Varta, Bater, Telzas, Enercom, BPS, Benning, PZL-Mielec Solarex, Simens, Webasco, Nowomag Bay Wind.
10. Lorenc H.: Struktura i zasoby energetyczne wiatru w Polsce. Mat. Bad. IMiGW, Warszawa 1996.
11. PN-76/B-03420: Parametry obliczeniowe powietrza zewnętrznego.
12. Promieniowanie słoneczne. Wyniki pomiarów na stacjach aktynometrycznych w 1978 r. WKŁ, Warszawa 1983.

ZAŁĄCZNIK

METODY PODEJMOWANIA DECYZJI EKONOMICZNYCH

Ocena kosztów wytwarzania energii elektrycznej, czy szerzej opłacalności inwestowania w określony wariant - typ instalacji wytwarzania energii, wiąże się z ogólnym zagadnieniem, jakim jest wybór i zastosowanie właściwych wskaźników ekonomicznej efektywności inwestycji.

W gospodarce wolnorynkowej najbardziej są rozpowszechnione trzy metody podejmowania decyzji inwestycyjnych:

1) metoda zaktualizowanej wartości netto inwestycji,
2) metoda równych rat rocznych,
3) metoda wewnętrznej stopy procentowej.

Metoda zaktualizowanej wartości netto inwestycji jest znana w literaturze anglosaskiej jako NPV (*Net Present Value Method*).

W metodzie tej podaje się zdyskontowaną różnicę wszystkich wpływów i wydatków rocznych w kolejnych latach przez cały okres budowy oraz eksploatacji inwestycji. Sumy te dyskontuje się na rok zerowy, którym umownie jest rok zakończenia budowy inwestycji.

$$\mathrm{NPV} = \sum_{t=1}^{n} P_t \frac{1}{(1+k_n)} - \sum_{t=1-p}^{0} I_t \frac{1}{(1+k_n)^t}, \qquad (1)$$

gdzie:

P_t - wszystkie roczne wpływy i wydatki (ze znakiem minus) w kolejnych latach eksploatacji,

I_t - wszystkie roczne wydatki w kolejnych latach budowy inwestycji,

t - wskaźnik kolejnego roku,

k_n - nominalna stopa dyskontowa,

p - liczba lat budowy,

n - liczba lat eksploatacji.

Korzystne są inwestycje, dla których NPV ma wartość dodatnią. Z dwóch różnych wariantów inwestycyjnych, korzystniejszy jest ten, dla którego NPV jest większe.

W **metodzie równych rat rocznych**, która jest pewnym przypadkiem szczególnym metody 1, oblicza się przeciętne wydatki i dochody roczne, przyjmując, że są one stałe w kolejnych latach. Przy tym uwzględnia się także nakłady inwestycyjne rozłożone na cały okres eksploatacji.

$$I = \sum_{t=1}^{n} I_t \frac{1}{(1+k_n)^t}, \tag{2}$$

stąd ze wzoru na sumę postępu geometrycznego otrzymuje się:

$$I = I_t \frac{(1+k_n)^n - 1}{k_n(1+k_n)^n}, \tag{3}$$

a więc:

$$I_t = I \frac{k(1+k)^n}{(1+k_n)^n - 1}. \tag{4}$$

Stosując podobne obliczenia otrzyma się dla rocznych wydatków i wpływów (z pominięciem nakładów inwestycyjnych):

$$P_t = P \frac{k_n(1+k_n)^n}{(1+k_n)^n - 1}. \tag{5}$$

W **metodzie wewnętrznej stopy procentowej** (*Internal Rate Method*) zamiast stopy dyskontowej używa się tzw. wewnętrznej stopy procentowej. NPV przyrównuje się do zera i oblicza się stopę procentową. Jest to graniczna stopa zwrotu r poniesionych nakładów. Korzystniejszy jest ten wariant inwestycyjny, który cechuje się wyższą wewnętrzną stopą inwestycji. Stopa ta nie powinna być niższa niż

nominalna stopa dyskontowa. Jeśli wartość produkcji i koszty w poszczególnych latach są stałe, to ze wzoru (1), po przekształceniach, otrzyma się równanie, z którego wyznacza się r:

$$P \frac{r(1+r)^n}{(1+r)^n - 1} - I = 0 . \tag{6}$$

Dodatkowo wyróżnia się jeszcze co najmniej dwa wskaźniki ekonomiczne, które są bardzo przydatne w ocenie efektywności inwestycji, a mianowicie:

A) wymagany wyrównany dochód,
B) okres zwrotu.

Wskaźnik A, czyli wymagany wyrównany dochód (*levelised required revenues*) wyraża średni roczny wymagany przychód przy założeniu, że jest on równy średnim rocznym kosztom inwestycji. Warto poświęcić mu najwięcej uwagi ze względu na jego podstawowe znaczenie dla dalszej analizy.

Wskaźnik ten oblicza się przez przyrównanie równania (1) do zera (NPV = 0) i wyznaczenie przychodu. Aby to uczynić, należy najpierw podać bardziej rozwiniętą formułę na NPV, wyróżniając koszty i dochody. W miejsce P_t we wzorze (1) wstawia się wyrażenie:

$$P_t = V_e - L_e - M ,$$

gdzie:

V_e - przychód wynikający z wartości uzyskanej, wytworzonej w ciągu roku z danej inwestycji (w szczególnym, interesującym przypadku jest to roczna wartość energii wytworzona przez instalację energetyczną);

L_e - roczny zmienny koszt eksploatacji: koszty energii na potrzeby własne, opłaty środowiskowe;

M - stały koszt eksploatacji: koszty utrzymania - w tym koszty remontów i konserwacji urządzeń, koszty osobowe oraz koszty ogólne.

W równaniu (1) należy uwzględnić także wpływ opodatkowania. Dochód roczny P_t jest zmniejszony po opodatkowaniu. Przyjmując, że stawka opodatkowania T (*tax*), dochód roczny wyniesie $(1 - T) \cdot P_t$. W formule na NPV należy wziąć pod uwagę również odpisy amortyzacyjne. Wchodzą one w skład kosztów uzyskania dochodów, a więc zmniejszają podstawę opodatkowania o wartość $T \cdot D_t$, gdzie D_t jest rocznym odpisem amortyzacyjnym w roku t. W roku t dochody są zatem wyższe o $T \cdot D_t$ z tytułu amortyzacji.

D_t można wyrazić jako:

$$D_t = \frac{Ib}{d},$$

gdzie:

b - podstawa amortyzacji (podlegająca amortyzacji część kosztu inwestycyjnego);

d - okres amortyzacji - liczba lat.

Ostatecznie rozwinięta formuła na NPV przyjmuje następującą postać:

$$\mathrm{NPV} = (1-T)\sum_{t=1}^{n}(V_e - L_e - M)\frac{1}{(1+k_n)^t} + \frac{bTI}{d}\sum_{t=1}^{d}\frac{1}{(1+k_n)^t} - I. \tag{7}$$

Po przyrównaniu NPV do zera oblicza się V_e:

$$V_e = r_n I + M + L_e, \tag{8}$$

gdzie: r_n – roczna rata zwrotu kapitału.

Z równania (7) dla NPV = 0 otrzyma się:

$$r_n = \frac{1 - \frac{bT}{d}\sum_{t=1}^{d}\frac{1}{(1+k_n)^t}}{(1-T)\sum_{t=1}^{n}\frac{1}{(1+k_n)^t}}. \tag{9}$$

Gdy $b = 1$ (cały koszt inwestycyjny podlega amortyzacji), a także uwzględniając, że $\frac{1}{d} = D$, wzór (9) po przekształceniach przyjmuje postać:

$$r_n = \frac{k_n (1+k_n)^n}{(T-1)\left((1+k_n)^n - 1\right)} - \frac{DT}{1-T} . \tag{10}$$

Wzór ten uzupełnia się czasem o roczny koszt ubezpieczenia p_1 oraz koszt innych opłat, np. podatek od własności p_2.

Ostatecznie wzór przyjmuje następującą postać:

$$r_n = \frac{k_n (1+k_n)^n}{(T-1)\left((1+k_n)^n - 1\right)} - \frac{DT}{1-T} + p_1 + p_2 . \tag{11}$$

Nominalna stopa dyskontowa k_n obrazuje średnią ważoną stopę oprocentowania kredytów. Rozwinięta formuła dla k_n ma następującą postać:

$$k_n = \frac{k_e E + k_p P_r + (1-T)\, k_b B}{K_c} , \tag{12}$$

gdzie:

E - środki finansowe ze sprzedaży akcji publicznych;
k_e - nominalna stopa zwrotu dla tych akcji;
P_r - środki finansowe ze sprzedaży akcji preferencyjnych;
k_p - nominalna stopa zwrotu dla akcji preferencyjnych;
A - środki finansowe uzyskane przez kredyt;
k_b - nominalna stopa oprocentowania kredytów;
$K_c = \mathrm{E} + P_r + B$ - nakłady inwestycyjne ogółem.

Ze względu na to, że w rozpatrywanej sytuacji $K_c = B$ (wszystkie nakłady są finansowane z kredytu), więc $k_n = (1 - T) \cdot k_b$. Czynnik $(1 - T)$ w tym wzorze wynika z faktu, że roczne raty spłaty kredytu stanowią koszt uzyskania i są odejmowane od podstawy opodatkowa-

nia. Opodatkowanie zmniejsza zatem obciążenia z tytułu spłaty kredytu.

Wymagany roczny dochód obliczony według formuły (8) jest równy rocznemu kosztowi (ponieważ NPV = 0). Koszt roczny wyniesie więc:

$$K_r = r_n I + M + L_e . \tag{13}$$

W dalszy ciągu rozważań będzie wprowadzony termin kosztu rocznego, gdyż jest on bardziej rozpowszechniony w rozpatrywanej problematyce od innych wielkości.

Właściwym wskaźnikiem porównawczym jest roczny koszt jednostkowy *k*, czyli koszt roczny wytworzenia jednej kilowatogodziny energii elektrycznej:

$$k = \frac{K_r}{A_n} , \tag{14}$$

gdzie:

A_n - roczna produkcja energii elektrycznej netto (cała wyprodukowana w roku energia pomniejszona o wielkość energii na potrzeby własne).

Wskaźnik B, czyli okres zwrotu (*payback period*) ma następującą postać:

$$PP = \frac{I}{V_e - L_e - M} . \tag{15}$$

Zgodnie z dotychczasowymi oznaczeniami, równa się on ilorazowi całkowitych kosztów nakładów inwestycyjnych przez jednoroczny dochód (w pierwszym roku eksploatacji). Im mniejszy jest *PP* - okres zwrotu jest krótszy, tym korzystniejsza jest inwestycja. Metoda oceny inwestycji oparta na tym wskaźniku jest szeroko rozpowszechniona, lecz w przedstawionej, nierozwiniętej postaci, znajduje ona jedynie

zastosowanie do oceny projektów inwestycyjnych o szacowanym okresie zwrotu co najwyżej 5-letnim. Dla dłuższych okresów zwrotu należy uwzględnić efekt dyskontowania sum i opodatkowania.

Niniejszy załącznik opracowano na podstawie [5] i [7]. Umożliwia on lepsze zrozumienie tych partii części głównej artykułu, które dotyczą bezpośrednio analizy ekonomicznej. W części głównej opracowania skorzystano z rozwiniętej formuły wskaźnika A - wzór (14) - z zastosowaniem metody równych rat rocznych i metody zaktualizowanej wartości netto inwestycji. W powyższym załączniku przedstawiono sposób dojścia do ostatecznej użytecznej formuły wskaźnika A. Ponadto w części głównej artykułu przytoczono także wzory (2) i (10).

Анджей Бинкевич

СТОИМОСТЬ ЭЛЕКТРОЭНЕРГИИ В СИСТЕМАХ ЭЛЕКТРОПИТАНИЯ С АЛЬТЕРНАТИВНЫМИ ИСТЫНИКАМИ ЭЛЕКТРОЭНЕРГИИ

Резюме

Представлена оценка и сравнение удельной стоимости электроэнергии получаемой в обычных системах электропитания устройств связи и в системах с альтернативными источниками электроэнергии. Дается анализ следующих систем электропитания: автономная система с солнечной батерей, система с солнечной батерей взаимодействующая с энергетической сетью, гибридная система с солнечной батереей и ветровым генератором взаимодействующая с энергетической сетью. Учитываются все компоненты затрат: стоимость земли, строительство здания станции, приобретение, монтаж и запуск устройств станции, эксплуратационные затраты, а также дополнительные затраты на разработку проекта, выполнение необходимых экспертных работ итд. При

анализе систем электропитания с альтернативными источниками энергии использовано данные касающиеся стоимости электроэнергии и ветровых условий в Польше на ее территории.

Andrzej Binkiewicz

THE COST OF ELECTRICAL ENERGY OF SUPPLYING SYSTEMS WITH THE ALTERNATIVES SOURCES OF ENERGY

S u m m a r y

The evoluation and comparison of the unit price of electrical energy obtained in conventional supplying system for telecommunication equipment as well as for supplying systems containing the sources alternatives of energy are presented. The following supplying systems with alternatives sources of energy are analysed: autonomons system with solar battery, system with solar battery interworking with main power network as well as the hybrid system with solar battery and wind generator interworking with main power network. It is taken in consideration all the components of cost, among other the cost of buying of terrain, the cost of constructing of supplying buildings, the cost of buing, of assemblage and putting in motion of equipments, the cost of operation as well as supplementary costs, for instance of design execution, of required expertises etc. There was taken into consideration for the supplying systems equipped with alternative sources of energy the data of offer for solar energy and wind energy for whole surface of Poland.

Andrzej Binkiewicz

LE COUT D'ENERGIE ELECTRIQUE OBTENUE DES SYSTEMES D'ALIMENTATION CONTENANT LES SOURCES ALTERNATIVES DE L'ENERGIE

R é s u m é

Il y a une présentation de l'évaluation et de la comparaison du coût unitaire d'énergie électrique obtenue à partir d'un système conventionnel

d'alimentation des équipements de télécommunication ainsi que de seux qui contiennent de sources alternatives d'énergie. Nous avons fait l'analyse des systèmes suivants d'alimentation comprenant les sources alternatives: un système autonome avec une batterie solaire, un système avec la batterie solaire qui coopére avec le réseau électrique et un système hybride composé d'une batterie solaire et d'un générateur de vent coopérant avec le réseau électrique. Nous avons pris en compte toutes les composants de coûts, entre autres: le coût d'achat d'un terrain, le coût de la construction de batiment d'une centrale, et pour les équipements - coût d'achat, d'assemblage et de mise en marche, ensuite les coûts d'exploitation ainsi que les coûts supplementaires, par exemple d'exécution d'un projet, les coûts des expertises necessaires, etc. Pour exécuter des examens des systèms équipés d'alternatives sources d'énérgie nous avons pris en compte les données qui concernent l'offre de l'énérgie solaire et de l'énérgie de vent par raport à toute la surface de Pologne.

Andrzej Binkiewicz

KOSTEN DER IN STROMVERSORGUNGSSYSTEMEN MIT ALTERNATIVEN STROMQUELLEN GEWONNENEN ELEKTROENERGIE

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

Einzelkosten der Elektroenergie, die in üblichen Stromversorgungssystemen wie auch in denen mit alternativen Stromquellen gewonnen wird, wurden abgeschätzt und verglichen. Folgende Systeme wurden analysiert: das abgesonderte Solarzellensystem, das mit Netzanschluß verbundene Solarzellensystem, das Solarzellen- und Windgenerator-Hybridsystem. Gezogen wurden in Betracht folgende Kostenbestandteile: Einkauf der Gründstücks, Bau der Kraftwerkgebäude, Ankauf, Montage und Inbetriebsetzung der Anlagen und auch Mehrkosten, wie: Design, Begutachtung u.a. Für die Stromversorgungssysteme mit alternativen Stromquellen wurden Daten über Angebot in ganz Polen von Sonnen- und Windenergie in Erwägung gezogen.

Roman Nierebiński

621.39„313".0058

KRZYWE LOGISTYCZNE W PROGNOZOWANIU ROZWOJU TELEKOMUNIKACJI

Przedstawiono krzywe logistyczne, ich właściwości oraz metody szacowania ich parametrów. Omówiono wykorzystanie krzywych logistycznych do prognozowania rozwoju telekomunikacji na przykładzie telefonii w krajach Unii Europejskiej, w Demokratycznej Republice Kongo (dawny Zair) oraz w Polsce.

1. KRZYWA LOGISTYCZNA I JEJ WARIANTY

1.1. Wprowadzenie

W Oddziale Gdańskim Instytutu Łączności od 1977 r. prowadzi się badania związane z prognozowaniem rozwoju usług telekomunikacyjnych w Polsce. Wykorzystuje się do tego celu krzywą logistyczną, której właściwości dobrze opisują rozwój usług telekomunikacyjnych.

Przedmiotem artykułu będzie krzywa logistyczna, a właściwie grupa krzywych logistycznych. Na podstawie literatury [8, 11] i przykładów z dziedziny telekomunikacji [4, 9] wyróżniono trzy typy równań krzywych logistycznych:

- równania podstawowe;
- równania uwzględniające wielkość Produktu Krajowego Brutto (PKB) na głowę mieszkańca;
- równania loglogistyczne (logarytmiczno-logistyczne).

Poszczególne rodzaje równań mogą występować w różnych wariantach. Niektóre z nich opisano w dalszej części artykułu.

Celem niniejszego artykułu jest przedstawienie możliwości zastosowania krzywych logistycznych do prognozowania rozwoju telefonii oraz innych usług telekomunikacyjnych. Pojawić się może więc pytanie: co to jest usługa telekomunikacyjna? Według [5, s. 83]: *„Usługą telekomunikacyjną można nazwać dowolny zasób lub czynność operatora telekomunikacyjnego oferowaną swoim abonentom"*. Istnieje wiele klasyfikacji usług telekomunikacyjnych, ale nie one są przedmiotem tego opracowania.

W dalszej części artykułu przyjęto, że omawiając rozwój usługi telekomunikacyjnej uwzględnia się jedynie aspekt ilościowy, czyli: liczbę abonentów, gęstość abonentów, ilościowe zapotrzebowanie na usługę, liczbę łączy i liczbę terminali. Warto podkreślić, że w literaturze i statystykach telekomunikacyjnych pisząc o liczbie abonentów telefonicznych podaje się zamiennie liczbę linii głównych lub liczbę terminali telefonicznych. W przypadku gęstości abonentów telefonicznych (gęstości telefonicznej) oblicza się ją w przeliczeniu na 1, 100 lub 1000 mieszkańców. W niniejszym artykule będzie stosować się przeliczenie na 100 mieszkańców. Natomiast analizując zapotrzebowanie na usługę telefoniczną bierze się pod uwagę zarówno abonentów (zapotrzebowanie zrealizowane), jak również wszystkich zainteresowanych otrzymaniem telefonu (zapotrzebowanie niezrealizowane).

1.2. Równanie podstawowe

Punktem wyjścia będzie krzywa wykładnicza o równaniu:

$$y = y_0 e^{ct}, \tag{1}$$

gdzie:

y - zmienna zależna (liczba abonentów, gęstość abonentów, zapotrzebowanie),

y_0 - wartość początkowa, np. liczba abonentów w momencie $t = 0$,

t - zmienna niezależna (czas, rok),

c - parametr.

Współczynnik przyrostu funkcji jest stały i wynosi:

$$\frac{dy}{ydt} = c = const . \tag{2}$$

Model ten jest nierealistyczny w dłuższym przedziale czasu, ponieważ liczba abonentów nie może rosnąć nieograniczenie, lecz przeciwnie musi zmierzać do wartości asymptotycznej, która odpowiada nasyceniu. Jako przykład mogą posłużyć najbardziej rozwinięte kraje świata, w których np. liczba abonentów telefonicznych wzrasta w ostatnich latach nieznacznie.

Krzywa logistyczna opiera się, zgodnie z [11], na założeniu, że współczynnik przyrostu funkcji nie jest stały, ale proporcjonalny do różnicy między y i jej wartością asymptotyczną a:

$$\frac{dy}{ydt} = \frac{c}{a}(a - y) . \tag{3}$$

Rozwiązaniem powyższego równania różniczkowego jest funkcja logistyczna o postaci:

$$y(t) = \frac{a}{1 + e^{b - ct}} , \tag{4}$$

spełniająca warunek początkowy:

$$y(0) = \frac{a}{1 + e^{b}} . \tag{5}$$

Parametry a, b i c przyjmują wartości dodatnie.

1.3. Warianty równania podstawowego

W literaturze wymienia się różne postaci równania krzywej logistycznej. Oprócz równania (4) podaje się równania:

$$y(t) = \frac{y_\infty}{1 + \left(\frac{y_\infty}{y_0} - 1\right) e^{-\frac{t}{\tau}}}, \tag{6}$$

gdzie:

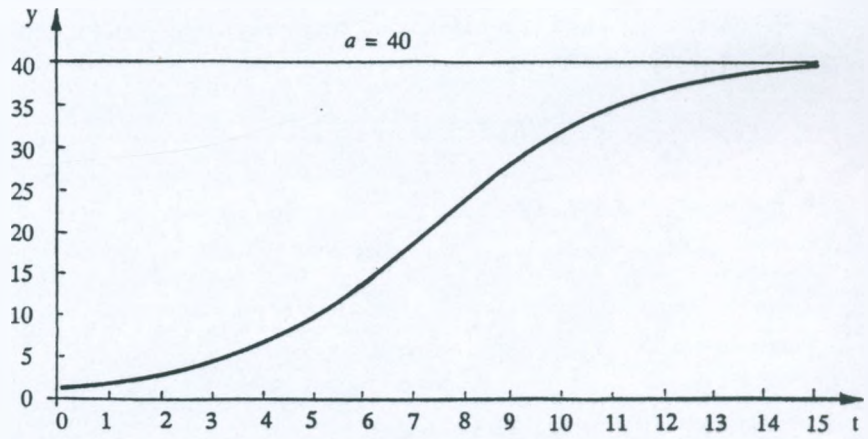
y_∞ - wartość asymptotyczna funkcji dla $t \to \infty$,

τ - stała czasowa

$$y(t) = \frac{a}{1 + Be^{-ct}}, \tag{7}$$

$$y(t) = \frac{a}{1 + e^{-c(t-t_0)}}. \tag{8}$$

Z pobieżnej analizy widać, że równania (4), (6), (7) i (8) tylko nieznacznie różnią się i bardzo łatwo przejść od jednej postaci do drugiej.



Rys. 1. Krzywa logistyczna o równaniu $y = \frac{40}{1 + e^{3,66 - 0,5t}}$

Na rys. 1 przedstawiono wykres przykładowej krzywej logistycznej (wg wzoru 4).

1.4. Równania uwzględniające wartość Produktu Krajowego Brutto

1.4.1. Równanie ogólne

Realizując w latach 1993-1994 projekt RACE R2091 [3, 4], sformułowano prognozy rozwoju usług telekomunikacyjnych do 2010 r. dla 12 krajów Unii Europejskiej. Przedmiotem zainteresowania były następujące usługi: telefonia, multimedia, szybki faks, wideofonia, średnioszybka transmisja danych, telefonia komórkowa, szybka transmisja danych i wideokonferencja. W badaniach wykorzystano różne metody, między innymi zastosowano krzywą logistyczną, w nieco rozbudowanej postaci. Przyjęto, że zapotrzebowanie na usługi telekomunikacyjne zależy od PKB na głowę mieszkańca oraz od czasu. PKB odzwierciedla bowiem stan ekonomiczny państwa, a jego przyrost może być uważany za podstawową siłę napędową zapotrzebowania na usługi telekomunikacyjne. Czas natomiast może być postrzegany jako czynnik, umożliwiający postęp techniczny i zwiększanie wiedzy użytkownika o dostępnych usługach.

Gęstość abonentów telefonicznych wyrażono następującym wzorem:

$$y_g(t) = \frac{a\left(\frac{P_t}{P_{2010}}\right)^d}{1 + e^{b - c(t - 1960)}}, \tag{9}$$

gdzie:

y_g - gęstość abonentów telefonicznych,
P_t - PKB na głowę mieszkańca w roku t,
P_{2010} - PKB na głowę mieszkańca w 2010 r.
a, b, c, d - parametry.

1.4.2. Inne równania

W czasie prac nad projektem RACE R2091 przeanalizowano także inne modele dla gęstości telefonicznej. Rozważano przedstawione poniżej równania.

- **Równanie 1**

$$y_g(t) = \frac{a\left(\frac{P_t}{P_{1975}}\right)^d}{1 + e^{b - c\,(t - 1960) + f \cdot produkcja}}, \tag{10}$$

gdzie:

P_{1975} - PKB na głowę mieszkańca w 1975 r.,

produkcja - udział produkcji przemysłowej (w procentach) w tworzeniu PKB,

f - parametr.

Udział produkcji przemysłowej w tworzeniu PKB odzwierciedla strukturę ekonomii danego kraju. W krajach najbardziej rozwiniętych maleje udział produkcji przemysłowej w tworzeniu PKB, wzrasta natomiast udział usług. Przyrost udziału usług znajduje również odzwierciedlenie w szybszym rozwoju usług telekomunikacyjnych. Istnieje zatem negatywne oddziaływanie między parametrem *produkcja* i gęstością telefoniczną.

- **Równanie 2**

$$y_g(t) = \frac{a\left(\frac{P_t}{P_{1975}}\right)^d}{1 + e^{b - c\,(t - 1960) + f \cdot cyfryzacja}}, \tag{11}$$

gdzie:

cyfryzacja - cyfryzacja sieci telefonicznej w procentach.

Cyfryzacja sieci telekomunikacyjnych czyni je bardziej nowoczesnymi i wydajnymi. Obserwuje się więc pozytywne oddziaływanie między wartością parametru *cyfryzacja* i gęstością telefoniczną (parametr *f* przyjmuje wartości ujemne).

- **Równanie 3**

$$y_g(t) = \frac{a\left(\frac{P_t}{P_{1975}}\right)^d}{1 + e^{b - c(t - 1960)}} . \tag{12}$$

W wyniku przeprowadzonej analizy zdecydowano, że równanie (9) jest najlepszym modelem dla gęstości telefonicznej w krajach Unii Europejskiej.

1.5. Funkcja loglogistyczna (logarytmiczno-logistyczna)

Założenie o nieprzekraczaniu przez badaną funkcję poziomu nasycenia nie zawsze okazuje się prawdziwe. Do opisu i prognozowania rozwoju zjawisk charakteryzujących się stałym, nieograniczonym wzrostem, z malejącym do zera tempem wzrostu, zgodnie z [8, 12], można wykorzystać funkcję loglogistyczną, mającą postać:

$$y(t) = \frac{a \ln t}{1 + e^{b - ct}} . \tag{13}$$

Funkcja ta, w odróżnieniu od funkcji logistycznej, nie ma asymptoty nasycenia. Warto podkreślić, że w dobrze funkcjonującej gospodarce procesy rozwojowe nigdy nie ustają, w związku z czym wydaje się, że funkcja loglogistyczna może być dobrym narzędziem do opisu takich zjawisk. Modele zbudowane na podstawie funkcji loglogistycznej mogą służyć także do prognozowania rozwoju usług telekomunikacyjnych.

2. SZACOWANIE PARAMETRÓW KRZYWEJ LOGISTYCZNEJ

Bardzo istotną sprawą jest określenie wartości parametrów występujących w przedstawionych w poprzednim punkcie równaniach krzywych logistycznych. Korzysta się w tym celu z danych historycznych, najczęściej rocznych, obrazujących ilościowy rozwój usługi telekomunikacyjnej do chwili obecnej. Na podstawie tych danych szacuje się wartości parametrów odpowiednich krzywych, stosując jedną z poniżej omówionych metod.

2.1. Interpretacja parametrów równania podstawowego

W równaniu podstawowym krzywej logistycznej $y(t) = \frac{a}{1 + e^{b-ct}}$ występują trzy parametry: a, b i c. Parametr a określa nasycenie funkcji logistycznej, co w języku matematyki można opisać następującą zależnością:

$$\lim_{t \to \infty} \frac{a}{1 + e^{b-ct}} = a \ . \tag{14}$$

Powyższy zapis oznacza, że prosta o równaniu $y = a$ jest asymptotą poziomą krzywej logistycznej. W celu znalezienia interpretacji dla pozostałych parametrów oblicza się pierwszą i drugą pochodną krzywej logistycznej. Wynoszą one:

$$y' = \frac{ace^{b-ct}}{(1 + e^{b-ct})^2} \ , \tag{15}$$

$$y'' = \frac{-ac^2 e^{b-ct}(1 + e^{b-ct})(1 - e^{b-ct})}{(1 + e^{b-ct})^4} \ .$$

Wiadomo, że druga pochodna określa wypukłość funkcji oraz punkt przegięcia (jeżeli występuje). Warunkiem koniecznym istnienia punktu przegięcia jest $y''(t) = 0$. Dla krzywej logistycznej punkt przegięcia występuje dla

$$t = \frac{b}{c} . \tag{16}$$

W punkcie przegięcia następuje największy przyrost wartości funkcji logistycznej. Wynosi on:

$$y'_{max} = \frac{ac}{4} . \tag{17}$$

Z powyższych równań wynika, że parametry b i c mają związek z punktem przegięcia krzywej logistycznej.

W celu zilustrowania metody wyznaczania wartości parametrów krzywej logistycznej należy rozpatrzyć wykres funkcji logistycznej z rys. 1. Parametry występujące w równaniu krzywej przyjmują wartości: $a = 40$, $b = 3{,}66$, $c = 0{,}5$. Można założyć, że nie jest znane równanie krzywej, a krzywa ta odzwierciedla rzeczywisty rozwój wybranej usługi telekomunikacyjnej, na przykład w Polsce. Ponieważ parametr a określa poziom nasycenia dla danej funkcji, to z wykresu funkcji można przyjąć $a = 40$. Można także zaobserwować występowanie punktu przegięcia krzywej dla $t \approx 7$. Wiadomo, że punkt przegięcia występuje dla $t = b/c$, a ponadto, że w punkcie przegięcia jest największy przyrost wartości funkcji. Ten maksymalny przyrost równa się $ac/4$ (na rys. 1 wartość tego przyrostu wynosi ≈ 5). Znając wartość parametru a wystarczy teraz rozwiązać układ równań:

$$\begin{cases} \dfrac{b}{c} = 7 \\ \dfrac{40c}{4} = 5 \end{cases} . \tag{18}$$

Łatwo obliczyć, że $c = 0{,}5$, $b = 3{,}5$. Uwzględniając $a = 40$, można uzyskać następujące równanie omawianej krzywej logistycznej:

$$y = \frac{40}{1 + e^{3{,}5 - 0{,}5t}} . \tag{19}$$

Należy podkreślić, że wyżej obliczone i występujące na rys. 1 wartości parametrów a i c są identyczne. Różnią się nieco wartości parametru b (w art. $b = 3{,}5$; na rys. $b = 3{,}66$). Można zatem przyjąć, że równanie (19) odpowiada w przybliżeniu równaniu krzywej z rys. 1.

2.2. Metoda trzech punktów

Do przedstawienia metody wyliczenia parametrów krzywej logistycznej zostanie wykorzystana funkcja logistyczna określona równaniem (6). Zawiera ona trzy parametry: y_0, y_∞ i τ. Aby je wyznaczyć, wystarczy znać wartość y dla trzech momentów czasowych t_0, t_1 i t_2. Przyjmując, że $t_0 = 0$, wyznacza się $y(t_0) = y_0$. W celu wyznaczenia wartości parametrów y_∞ i τ należy rozwiązać układ dwóch równań z dwiema niewiadomymi:

$$\begin{cases} y_1 = \dfrac{y_\infty}{1 + \left(\dfrac{y_\infty}{y_0} - 1\right) e^{-\frac{t_1}{\tau}}} & \text{(20a)} \\ y_2 = \dfrac{y_\infty}{1 + \left(\dfrac{y_\infty}{y_0} - 1\right) e^{-\frac{t_2}{\tau}}} & \text{(20b)} \end{cases}$$

Z równania (20a) wyznacza się:

$$1 + \left(\frac{y_\infty}{y_0} - 1\right) e^{-\frac{t_1}{\tau}} = \frac{y_\infty}{y_1} . \tag{21}$$

Po kolejnych przekształceniach uzyskuje się:

$$-\frac{t_1}{\tau} = \ln \frac{\frac{y_\infty}{y_1} - 1}{\frac{y_\infty}{y_0} - 1} \tag{22}$$

oraz

$$-\frac{1}{\tau} = \frac{1}{t_1} \ln \frac{\frac{y_\infty}{y_1} - 1}{\frac{y_\infty}{y_0} - 1} . \tag{23}$$

Analogicznie można przekształcić równanie (20b). Otrzymuje się:

$$-\frac{1}{\tau} = \frac{1}{t_2} \ln \frac{\frac{y_\infty}{y_2} - 1}{\frac{y_\infty}{y_0} - 1} . \tag{24}$$

Porównując prawe strony obu równań uzyskuje się równanie:

$$\frac{1}{t_1} \ln \frac{\frac{y_\infty}{y_1} - 1}{\frac{y_\infty}{y_0} - 1} = \frac{1}{t_2} \ln \frac{\frac{y_\infty}{y_2} - 1}{\frac{y_\infty}{y_0} - 1} . \tag{25}$$

Podstawiając $t_1 = 1$ i $t_2 = 2$ otrzymuje się równanie:

$$\ln \frac{\frac{y_\infty}{y_1} - 1}{\frac{y_\infty}{y_0} - 1} = \frac{1}{2} \ln \frac{\frac{y_\infty}{y_2} - 1}{\frac{y_\infty}{y_0} - 1} . \tag{26}$$

Po prostych przekształceniach uzyskuje się równanie kwadratowe:

$$\left(\frac{\frac{y_\infty}{y_1} - 1}{\frac{y_\infty}{y_0} - 1}\right)^2 = \frac{\frac{y_\infty}{y_2} - 1}{\frac{y_\infty}{y_0} - 1} . \tag{27}$$

Na podstawie znanych wzorów na pierwiastki równania kwadratowego oblicza się wartość y_∞:

$$y_\infty = \frac{y_1\left(y_1y_0 + y_1y_2 - 2y_0y_2\right)}{y_1^2 - y_0y_2} . \tag{28}$$

Podstawiając $t_2 = 2$ oraz obliczoną wartość y_∞ do wzoru (24) wyznacza się wartość $-\frac{1}{\tau}$:

$$-\frac{1}{\tau} = \frac{1}{2}\ln\frac{y_0\left[y_1\left(y_1y_0 + y_1y_2 - 2y_0y_2\right) - y_2\left(y_1^2 - y_0y_2\right)\right]}{y_2\left[y_1\left(y_1y_0 + y_1y_2 - 2y_0y_2\right) - y_0\left(y_1^2 - y_0y_2\right)\right]} . \tag{29}$$

Wyznaczone wartości parametrów y_0, y_∞ oraz $-\frac{1}{\tau}$ podstawia się do wzoru (6) i uzyskuje równanie krzywej logistycznej.

2.3. Metoda najmniejszych kwadratów

W dalszej części artykułu (pkt. 2.4 ÷ 2.6) do obliczania wartości parametrów (szacowania parametrów) krzywej logistycznej zastosowano metodę najmniejszych kwadratów. Dla jasności obrazu opisano ją zgodnie z [11].

Niech będzie dany liniowy model ekonometryczny o równaniu:

$$Y = a_0 + a_1 X + \varepsilon \ , \tag{30}$$

gdzie:

Y - zmienna objaśniana,
X - zmienna objaśniająca,
ε - błąd modelu,
a_0, a_1 - parametry modelu.

W celu obliczenia wartości parametrów a_0 i a_1 zakłada się, że funkcja

$$S = \sum_{t=1}^{n} (y_t - a_0 - a_1 x_t)^2 \tag{31}$$

osiąga wartość najmniejszą. Po obliczeniu pochodnych cząstkowych względem a_0 oraz a_1 otrzymuje się następujący układ równań:

$$\begin{cases} a_0 n + a_1 \sum_{t=1}^{n} x_t = \sum_{t=1}^{n} y_t \\ a_0 \sum_{t=1}^{n} x_t + a_1 \sum_{t=1}^{n} x_t^2 = \sum_{t=1}^{n} x_t y_t \end{cases} \tag{32}$$

Korzystając z wzorów Cramera oblicza się wartości parametrów a_0 i a_1:

$$\begin{cases} a_0 = \dfrac{\sum_{t=1}^{n} y_t \sum_{t=1}^{n} x_t^2 - \sum_{t=1}^{n} x_t \sum_{t=1}^{n} x_t y_t}{n \sum_{t=1}^{n} x_t^2 - \left(\sum_{t=1}^{n} x_t \right)^2} \\ a_1 = \dfrac{n \sum_{t=1}^{n} x_t y_t - \sum_{t=1}^{n} x_t \sum_{t=1}^{n} y_t}{n \sum_{t=1}^{n} x_t^2 - \left(\sum_{t=1}^{n} x_t \right)^2} \end{cases} \tag{33}$$

2.4. Metoda Hotellinga

Do rozważań w pkt. 2.4 i 2.5 przyjęto, zgodnie z [11], krzywą logistyczną opisaną równaniem (7), tj. $y(t) = \dfrac{a}{1 + Be^{-ct}}$.

Funkcja logistyczna jest jedynym rozwiązaniem równania różniczkowego

$$\frac{y'}{y} = \frac{c}{a}(a - y) , \tag{34}$$

spełniającym warunek początkowy

$$y(0) = \frac{a}{1 + B} . \tag{35}$$

Hotelling zastąpił równanie różniczkowe (34) następującym równaniem różnicowym

$$\frac{y_{t+1} - y_t}{y_t} = c - \frac{c}{a} y_t \tag{36}$$

z warunkiem początkowym (35).

Obliczenie wartości parametrów a, B, c jest dwuetapowe. Pierwszy etap polega na wyznaczeniu wartości parametrów a i c. W drugim etapie na podstawie znajomości wartości parametrów a i c wyznacza się wartość parametru B.

Punktem wyjścia jest szereg czasowy

$$(1, y_1), ..., (n, y_n) , \tag{37}$$

zawierający wartości funkcji y dla kolejnych momentów czasowych (lat) $t = 1, ..., n$.

Obliczając względne przyrosty

$$u_t = \frac{y_{t+1} - y_t}{y_t} \quad (t = 1, ..., n - 1) , \tag{38}$$

otrzymuje się nowy szereg czasowy

$$(1, u_1), ..., (n-1, u_{n-1}) . \tag{39}$$

Równanie różnicowe przyjmuje postać liniową

$$u_t = c - \frac{c}{a} y_t \quad (t = 1, ..., n-1) \tag{40}$$

lub też ogólnie

$$u = a_0 + a_1 y , \tag{41}$$

gdzie:

$$\begin{aligned} a_0 &= c , \\ a_1 &= -\frac{c}{a} . \end{aligned} \tag{42}$$

Korzystając z metody najmniejszych kwadratów zastosowanej do równania i szeregu empirycznego

$$(y_1, u_1), ..., (y_{n-1}, u_{n-1}) , \tag{43}$$

otrzymuje się wartości parametrów a_0 i a_1

$$\begin{aligned} a_0 &= \frac{W_0}{W} , \\ a_1 &= \frac{W_1}{W} , \end{aligned} \tag{44}$$

gdzie:

$$\begin{aligned} W &= (n-1) \sum_{t=1}^{n-1} y_t^2 - \left(\sum_{t=1}^{n-1} y_t \right)^2 , \\ W_0 &= \sum_{t=1}^{n-1} y_t^2 \sum_{t=1}^{n-1} u_t - \sum_{t=1}^{n-1} y_t u_t \sum_{t=1}^{n-1} y_t , \\ W_1 &= (n-1) \sum_{t=1}^{n-1} y_t u_t - \sum_{t=1}^{n-1} y_t \sum_{t=1}^{n-1} u_t . \end{aligned} \tag{45}$$

Następnie korzystając z zależności (42) oblicza się wartości parametrów a i c:

$$a = -\frac{a_0}{a_1}, \qquad c = a_0 . \tag{46}$$

W drugim etapie metody Hotellinga przekształca się wzór (7) do postaci:

$$B = \frac{a - y}{y} e^{ct} . \tag{47}$$

Następnie stosuje się ponownie metodę najmniejszych kwadratów w najprostszej postaci, tzn. oblicza się:

$$B_t = \frac{a - y_t}{y_t} e^{ct} \quad (t = 1, ..., n) . \tag{48}$$

Szuka się takiego B, przy którym $\sum_{t=1}^{n} (B - B_t)^2$ jest najmniejsza. Prowadzi to do wzoru na wartość parametru B:

$$B = \frac{1}{n} \sum_{t=1}^{n} B_t = \frac{1}{n} \sum_{t=1}^{n} \left(\frac{a}{y_t} - 1 \right) e^{ct} . \tag{49}$$

Obliczone wartości parametrów a, B i c podstawia się do równania (7) krzywej logistycznej.

2.5. Metoda Tintnera

Idea metody Tintnera, zgodnie z [11], polega na znalezieniu równania różnicowego pierwszego rzędu o stałych współczynnikach, które spełnia odwrotność funkcji logistycznej dla każdego $t \in N$. Wprowadza się zmienne:

$$z_t = \frac{1}{y_t} = \frac{1 + Be^{-ct}}{a}, \qquad z_{t+1} = \frac{1}{y_{t+1}} = \frac{1 + Be^{-c(t+1)}}{a}. \tag{50}$$

Po przekształceniu otrzymuje się równanie:

$$z_{t+1} = dz_t + g, \tag{51}$$

gdzie:

$$d = e^{-c}, \qquad g = \frac{1 - e^{-c}}{a}. \tag{52}$$

Równanie to jest odpowiednikiem równania różnicowego dla metody Hotellinga. Jest ono punktem wyjścia dwuetapowej metody Tintnera.

Mając do dyspozycji szereg czasowy

$$(1, y_1), ..., (n, y_n) \tag{53}$$

tworzy się nowy szereg empiryczny, składający się z kolejnych odwrotności y_t, tzn. szereg

$$(z_t, z_{t+1}) = \left(\frac{1}{y_t}, \frac{1}{y_{t+1}}\right) \quad (t = 1, ..., n - 1), \tag{54}$$

czyli szereg

$$\left(\frac{1}{y_1}, \frac{1}{y_2}\right), ..., \left(\frac{1}{y_{n-1}}, \frac{1}{y_n}\right). \tag{55}$$

Korzystając z metody najmniejszych kwadratów, zastosowanej do równania (51) otrzymuje się wartości parametrów g i d:

$$g = \frac{U_0}{U}, \qquad d = \frac{U_1}{U}, \tag{56}$$

gdzie:

$$U = (n-1)\sum_{t=1}^{n-1} z_t^2 - \left(\sum_{t=1}^{n-1} z_t\right)^2,$$

$$U_0 = \sum_{t=1}^{n-1} z_{t+1} \sum_{t=1}^{n-1} z_t^2 - \sum_{t=1}^{n-1} z_t \sum_{t=1}^{n-1} z_t z_{t+1}, \tag{57}$$

$$U_1 = (n-1)\sum_{t=1}^{n-1} z_t z_{t+1} - \sum_{t=1}^{n-1} z_{t+1} \sum_{t=1}^{n-1} z_t .$$

Następnie wyznacza się wartości parametrów a i c:

$$a = \frac{1-d}{g}, \qquad c = -\ln d . \tag{58}$$

Drugi etap metody Tintnera jest drugim etapem metody Hotellinga. Znając wartości parametrów a i c ze wzoru

$$B = \frac{1}{n}\sum_{t=1}^{n}\left(\frac{a}{y_t} - 1\right)e^{ct} \tag{59}$$

wyznacza się wartość parametru B. Obliczone wartości parametrów a, B i c podstawia się do równania (7) krzywej logistycznej.

2.6. Metoda dwuetapowa

W pierwszym etapie należy oszacować wartość parametru a. W drugim etapie oblicza się wartości parametrów b i c. W tym celu

przekształca się równanie krzywej logistycznej (4), tj. $y(t) = \frac{a}{1 + e^{b-ct}}$ do postaci:

$$b - ct = \ln\left(\frac{a}{y} - 1\right). \tag{60}$$

Po podstawieniu $w = \ln\left(\frac{a}{y} - 1\right)$ otrzymuje się równanie

$$w = b - ct. \tag{61}$$

Jest to równanie liniowe. Do obliczenia wartości parametrów b i c można skorzystać z metody najmniejszych kwadratów. Uzyskuje się następujące wzory:

$$\begin{cases} b = \dfrac{\sum_{t=1}^{n} w_t \sum_{t=1}^{n} t^2 - \sum_{t=1}^{n} t \sum_{t=1}^{n} t w_t}{n\sum_{t=1}^{n} t^2 - \left(\sum_{t=1}^{n} t\right)^2} \\ c = -\dfrac{n\sum_{t=1}^{n} t w_t - \sum_{t=1}^{n} t \sum_{t=1}^{n} w_t}{n\sum_{t=1}^{n} t^2 - \left(\sum_{t=1}^{n} t\right)^2} \end{cases} \tag{62}$$

Obliczone wartości parametrów a, b i c podstawia się do równania (4) krzywej logistycznej.

2.7. Programy komputerowe

Obecnie trudno wyobrazić sobie jakiekolwiek prace prognostyczne bez wykorzystania programów komputerowych. Proste metody prognostyczne można przetestować za pomocą kalkulatora, ale inne są

bardzo rozbudowane obliczeniowo i praktycznie nie dają się zrealizować bez pomocy komputera.

Współczesny prognosta ma do wyboru trzy rodzaje programów komputerowych:

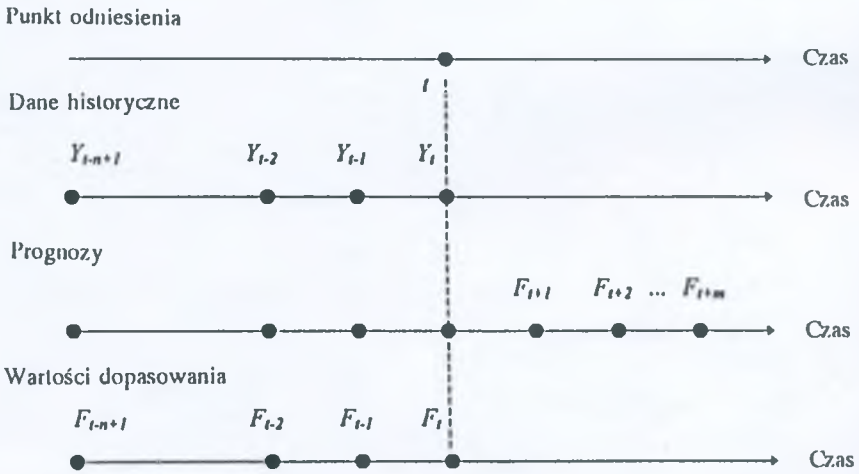
- arkusze kalkulacyjne (np. Excel, Lotus, Quattro Pro),
- pakiety statystyczne (np. Statgraphics, Statistica, SPSS, SAS),
- pakiety prognostyczne (np. Forecast Pro, EViews, Autobox, SCA).

W przypadku szacowania parametrów można skorzystać z wymienionych pakietów komputerowych.

3. PROGNOZOWANIE NA PODSTAWIE KRZYWEJ LOGISTYCZNEJ

3.1. Scenariusz prognozowania

Na rys. 2 zaprezentowano, zgodnie z [7], scenariusz prognozowania, który daje się zastosować w większości przypadków. Na



Rys. 2. Scenariusz prognozowania

podstawie danych historycznych Y dla momentów czasowych t, t - 1, t - 2, ..., $t - n + 1$ (najczęściej lat) buduje się model ekonometryczny, który jest najbardziej dopasowany do tych danych. Wykorzystując ten model tworzy się prognozy F dla kolejnych momentów czasowych $t + 1$, $t + 2$, ..., $t + m$. Dla uzyskanego modelu można określić zarówno błędy dopasowania $(Y_{t-n+1} - F_{t-n+1})$, ... , $(Y_{t-1} - F_{t-1})$, $(Y_t - F_t)$, jak i błędy prognozowania $(Y_{t+1} - F_{t+1})$, $(Y_{t+2} - F_{t+2})$, ..., które dadzą się obliczyć z chwilą uzyskania danych dla prognozowanych momentów czasu.

Przedstawiony scenariusz daje się także zastosować dla modeli opartych na krzywej logistycznej. W pkt. 3.2 ÷ 3.4 opisano modele rozwoju telefonii dla Demokratycznej Republiki Kongo, Unii Europejskiej i Polski, na podstawie których opracowano prognozy.

3.2. Demokratyczna Republika Kongo

W czasie programu ONZ [9] realizowanego w 1998 r. badano zapotrzebowanie na usługę telefoniczną dla Konga. Do prognozowania zapotrzebowania dla użytkowników mieszkaniowych wykorzystano krzywą logistyczną o równaniu (8), tj. $y(t) = \dfrac{a}{1 + e^{-c(t - t_0)}}$.

W przypadku regionu Kinszasa przyjęto, że wartość nasycenia liczby abonentów telefonicznych stanowić będzie 20% liczby mieszkańców regionu w 2038 roku. Prognozowana liczba mieszkańców w 2038 r. będzie wynosiła: 51 561 000. Wartość parametru nasycenia określono zatem następująco:

$$a = 20\% \cdot 51\,561\,000 = 10\,312\,200 \,. \tag{63}$$

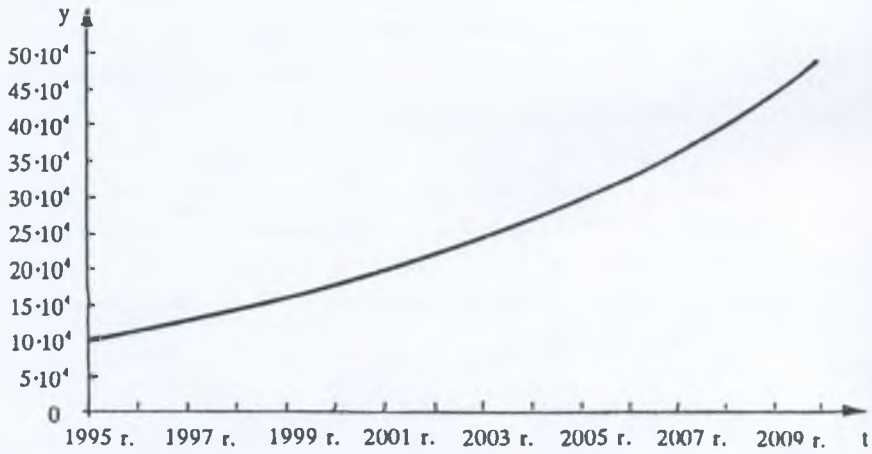
W celu wyznaczenia pozostałych parametrów, występujących w równaniu (8), tj. parametrów c i t_0 rozwiązano układ dwóch równań z dwiema niewiadomymi. Skorzystano przy tym z danych doty-

czących zapotrzebowania na usługę telefoniczną w latach 1988 i 1998. Uzyskano następujące zależności:

$$c = \frac{\ln\left(\frac{\frac{a}{y_1} - 1}{\frac{a}{y_2} - 1}\right)}{t_2 - t_1}, \qquad (64)$$

$$t_0 = t_1 + \frac{\ln\left(\frac{a}{y_1} - 1\right)}{c}.$$

Występujące w równaniu wartości t_1 i t_2 oznaczają odpowiednio lata 1988 oraz 1998, natomiast y_1 i y_2 - wartości zapotrzebowania na usługę telefoniczną w latach 1988 oraz 1998.



Rys. 3. Prognoza zapotrzebowania na usługę telefoniczną w prowincji Kinszasa w Kongo

W wyniku obliczeń uzyskano następujący model zapotrzebowania na usługę telefoniczną w prowincji Kinszasa w Kongo:

$$y = \frac{10\ 312\ 200}{1 + e^{-0{,}1068679\,(t - 2038)}} \quad (65)$$

Na podstawie modelu zbudowano prognozy rozwoju zapotrzebowania na usługę telefoniczną w prowincji Kinszasa do 2010 roku. Wyniki przedstawiono na rys. 3.

3.3. Unia Europejska

Podczas realizacji projektu RACE R2091 [3, 4] zbudowano prognozy rozwoju usługi telefonicznej dla 12 krajów Unii Europejskiej. Wykorzystano model dla gęstości telefonicznej opisany równaniem (9):

$$y_g(t) = \frac{a\left(\frac{P_t}{P_{2010}}\right)^d}{1 + e^{b - c\,(t - 1960)}}$$

W tym równaniu a jest parametrem nasycenia, który nie może być przekroczony do 2010 roku. Zmienną y_g określono jako prognozowaną gęstość telefoniczną. Przyjęto, że parametr a ma tę samą wartość dla każdego badanego kraju, zakładając, że w 2010 roku wszystkie kraje Unii Europejskiej osiągną zbliżony poziom rozwoju technologii i usług telekomunikacyjnych. Przyjęto także, że relacja między zmianami PKB na mieszkańca w poszczególnych latach jest analogiczna do zmiany gęstości telefonicznej. Założono stały, dla wszystkich krajów Unii Europejskiej, parametr d. Różnice między krajami uwidaczniają się w parametrach b i c.

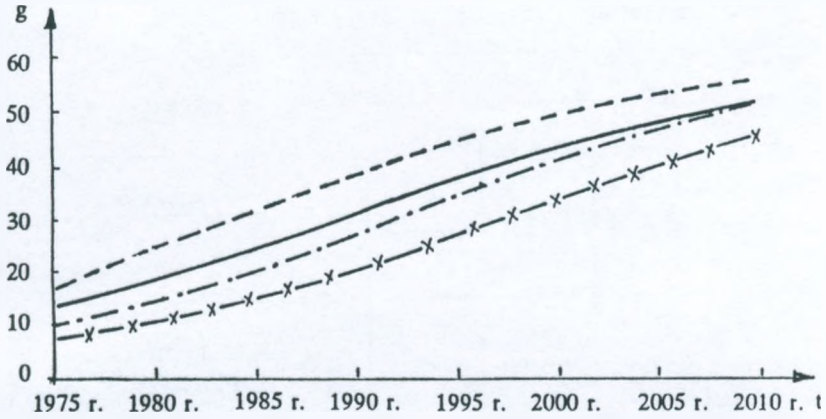
W tablicy 1 podano wartości parametrów dla gęstości telefonicznej dla 12 krajów Unii Europejskiej. Parametry obliczono korzystając ze specjalizowanych programów komputerowych.

Tablica 1

Wartości parametrów dla gęstości telefonicznej dla państw Unii Europejskiej

Kraj	Parametry				Punkt przegięcia [rok]	Maksymalny przyrost [%]	Gęstość telefoniczna na 100 mieszkańców	
	a	*b*	*c*	*d*			1991 r.	2010 r.
Belgia	59,1	2,188	-0,097	0,077	1983	2,42	40,9	55,2
Dania	59,1	2,174	-0,169	0,077	1973	4,22	57,7	59,0
Francja	59,1	3,903	-0,193	0,077	1980	4,81	51,0	58,9
Grecja	59,1	2,369	-0,101	0,077	1983	2,53	41,2	55,3
Hiszpania	59,1	2,459	-0,088	0,077	1988	2,19	34,0	51,5
Holandia	59,1	1,841	-0,108	0,077	1977	2,71	47,6	57,5
Irlandia	59,1	2,997	-0,096	0,077	1991	2,41	29,1	50,8
Luksemburg	59,1	1,168	-0,085	0,077	1974	2,12	50,1	56,5
Niemcy	59,1	2,550	-0,141	0,077	1978	3,52	48,7	58,4
Portugalia	59,1	3,280	-0,089	0,077	1997	2,23	25,5	45,2
Wielka Brytania	59,1	1,768	-0,101	0,077	1978	2,51	46,1	56,9
Włochy	59,1	2,397	-0,102	0,077	1984	2,54	40,0	55,3

Na rys. 4 przedstawiono prognozy gęstości telefonicznej do 2010 roku dla Grecji, Hiszpanii, Irlandii i Portugalii.



Rys. 4. Prognoza gęstości telefonicznej

Grecja Hiszpania Irlandia Portugalia

3.4. Polska

Poniżej przedstawiono modele rozwoju usługi telefonicznej w Polsce, zawarte w [11]. Do rozważań wzięto równanie (7) krzywej logistycznej, tj. $y(t) = \frac{a}{1 + Be^{-ct}}$. Na podstawie danych statystycznych z lat 1965 ÷ 1976 obliczono wartości parametrów *a*, *b* i *c*, za pomocą metod Hotellinga i Tintnera. W tablicy 2 podano uzyskane wartości parametrów oraz równania uzyskanych modeli.

Wartości parametrów obliczone za pomocą obu metod różnią się między sobą. Metoda Tintnera, jako bardziej dokładna, daje na ogół lepsze rezultaty niż metoda Hotellinga. Na podstawie tych modeli

można było sporządzać prognozy gęstości telefonicznej w kolejnych latach (1977 ÷ 1980).

Tablica 2

Modele ekonometryczne gęstości telefonicznej
na 100 mieszkańców Polski na podstawie danych z lat 1965 ÷ 1976

Metoda	Wartości parametrów			Model
	a	*b*	*c*	
Hotellinga	4,94634	3,9541	0,3033	$y_g = \frac{4{,}94634}{1 + 3{,}9541\,e^{-0{,}3033t}}$
Tintnera	4,33923	2,8299	0,3703	$y_g = \frac{4{,}33923}{1 + 2{,}8299\,e^{-0{,}3703t}}$

Prezentowane modele mają jedynie historyczną wartość i w obecnych warunkach nie można ich zastosować. Po 1989 roku nastąpiły w Polsce głębokie zmiany we wszystkich dziedzinach życia, także w telekomunikacji. Obecne modele należy zatem budować na podstawie danych statystycznych z lat 1990 ÷ 1997 i późniejszych. W tablicy 3 zebrano dane dotyczące liczby ludności, liczby abonentów telefonicznych i obliczone na tej podstawie gęstości telefoniczne w poszczególnych latach. W celu sporządzenia prognoz, opierając się na równaniu (4), tj. $y(t) = \frac{a}{1 + e^{b - ct}}$ zbudowano model dla gęstości telefonicznej. W celu oszacowania parametrów wykorzystano metodę dwupunktową. Zaproponowano wariantowe oszacowanie wartości parametru *a* (nasycenia). Punktem odniesienia była wartość parametru *a* przyjęta dla krajów Unii Europejskiej w programie RACE R2091. Rozpatrzono trzy warianty, a mianowicie:

- wariant 1 (pesymistyczny): a = 50, tj. mniej niż w programie RACE R2091;
- wariant 2 (unijny): a = 59,1, tj. tyle samo co w programie RACE R2091;
- wariant 3 (optymistyczny): a = 60, tj. więcej niż w programie RACE R2091.

Tablica 3

Gęstość telefoniczna w Polsce w latach 1990 ÷ 1997

Rok	Liczba ludności [tys.]	Liczba abonentów [tys.]	Gęstość telefoniczna na 100 mieszkańców
1990	38183	3293	8,62
1991	38309	3565	9,31
1992	38418	3938	10,25
1993	38505	4416	11,47
1994	38581	5006	12,98
1995	38609	5728	14,84
1996	38639	6532	16,91
1997	38660	7619	19,71

W tablicy 4 przedstawiono prognozy gęstości telefonicznej i liczby abonentów telefonicznych. W celu obliczenia prognoz liczby abonentów telefonicznych w latach 1998 ÷ 2000 wykonano dodatkowe obliczenie:

$$Liczba\ abonentów(t) = \frac{Gęstość\ telefoniczna\ (t)}{100} \cdot Liczba\ mieszkańców\ (t)\,. \quad (66)$$

Liczbę mieszkańców w latach 1998 ÷ 2000 oszacowano, zakładając, że przyrost liczby ludności w tych latach w stosunku do lat poprzednich będzie wynosił 20 tys.

Tablica 4

Prognozy gęstości telefonicznej (na 100 mieszkańców) i liczby abonentów telefonicznych (tys.) w Polsce w latach 1998 - 2000

Wariant	Model ekonometryczny (dla gęstości telefonicznej)	Prognoza 1998		Prognoza 1999		Prognoza 2000	
		Gęstość telefoniczna	Liczba abonentów	Gęstość telefoniczna	Liczba abonentów	Gęstość telefoniczna	Liczba abonentów
1	$y_g = \frac{50}{1 + e^{1,807958 - 0,162217t}}$	20,69	8004	22,68	8779	24,71	9566
2	$y_g = \frac{59,1}{1 + e^{1,990506 - 0,153498t}}$	20,82	8053	22,93	8875	25,12	9727
3	$y_g = \frac{70}{1 + e^{2,173773 - 0,146799t}}$	20,92	8093	23,14	8954	25,46	9860

4. ZAKOŃCZENIE

Krzywa logistyczna „zadomowiła się" w dziedzinie prognozowania rozwoju telefonii oraz innych usług telekomunikacyjnych. Burzliwy rozwój telekomunikacji w ostatnich dziesięcioleciach spowodował gwałtowny wzrost liczby usług telekomunikacyjnych oferowanych przez operatorów telekomunikacyjnych. Wśród tych usług telefonia odgrywa szczególną rolę z kilku względów:

- jest usługą najstarszą i najbardziej rozpowszechnioną, a więc dostarczającą najwięcej danych historycznych, które można wykorzystać do prognozowania;
- tworzona na potrzeby telefonii infrastruktura (zwłaszcza sieć cyfrowa) stanowi podstawę do rozwoju innych usług telekomunika-

cyjnych, często bardzo wyspecjalizowanych, takich jak: usługi ISDN, usługi sieci inteligentnej i wiele innych;

- w krajach zaniedbanych pod względem rozwoju infrastruktury telekomunikacyjnej (a do takich ciągle zalicza się Polska) zaspokojenie zapotrzebowania na usługę telefoniczną jest niezwykle ważne z punktu widzenia społecznego i gospodarczego.

Z wyżej wymienionych przyczyn w wielu krajach przywiązuje się wielką wagę do prognozowania rozwoju właśnie telefonii, co wykazują przykłady przytoczone w tym artykule. Stosuje się przy tym różne postaci krzywych logistycznych; zarówno jej postać podstawowa, jak i ta uwzględniająca wielkość Produktu Krajowego Brutto na mieszkańca znajdują zastosowanie w różnych krajach.

Krzywą logistyczną wykorzystuje się także do prognozowania rozwoju innych usług telekomunikacyjnych, np. telefonii komórkowej, dla których dysponuje się danymi historycznymi. Dane takie, choć mniej liczne niż w przypadku usługi telefonicznej, są wystarczające do sporządzenia wiarygodnych prognoz. Przykłady zastosowania można znaleźć w opracowaniach Unii Europejskiej [3, 4]. W przypadku krajów słabiej rozwiniętych pod względem infrastruktury telekomunikacyjnej, dla których brakuje danych historycznych dla konkretnej nowej usługi telekomunikacyjnej, można metodą analogii wykorzystać odpowiednie dane dla bardziej rozwiniętych krajów.

Najtrudniej zastosować krzywą logistyczną do prognozowania rozwoju nowych usług, dla których brakuje danych historycznych. W tym przypadku można założyć hipotetyczny rozwój nowej usługi, przyjmując typowy dla krzywej logistycznej charakter przebiegu funkcji. Można na przykład określić warunek początkowy, hipotetyczny punkt przegięcia krzywej logistycznej, poziom nasycenia dla danej usługi i na podstawie tych założeń zbudować model jej rozwoju.

Wydaje się zatem celowe dalsze podejmowanie badań w zakresie wykorzystania krzywej logistycznej do prognozowania rozwoju usług

telekomunikacyjnych zarówno tych, dla których dysponuje się wystarczającą liczbą danych historycznych, jak też usług zupełnie nowych.

WYKAZ LITERATURY

1. Analizy oraz prognozowanie ruchu z uwzględnieniem usług, zarówno konwencjonalnych jak i nowych, realizowanych aktualnie i w przyszłości w polskich sieciach telekomunikacyjnych. Etap 1 - Badania w zakresie usług konwencjonalnych. Oddział Gdański Instytutu Łączności, Gdańsk 1997.
2. Analizy oraz prognozowanie ruchu z uwzględnieniem usług, zarówno konwencjonalnych jak i nowych, realizowanych aktualnie i w przyszłości w polskich sieciach telekomunikacyjnych. Etap 2 - Badania w zakresie usług nowych. Oddział Gdański Instytutu Łączności, Gdańsk 1998.
3. Demand Scenarios for AC at the level of the Economy. R2091 URSA, 1994.
4. EC Demand Scenarios: First Set. R2091 URSA, 1993.
5. Jajszczyk A., Wachowski M.: Klasyfikacja nowoczesnych usług telekomunikacyjnych. KST'97. T. D, Bydgoszcz 1997.
6. Łączność w 1997 roku. Główny Urząd Statystyczny, Warszawa 1998.
7. Makridakis S., Wheelwright S.C., Hyndman R.J.: Forecasting. Methods and Applications. Third Edition. John Wiley & Sons, 1998.
8. Prognozowanie gospodarcze. Metody i zastosowania. Red. M. Cieślak. PWN, Warszawa 1997.
9. Republique Democratique du Congo, Plan Directeur National des Telecommunications 2001 - 2020, Prevision de la Demande, Programme des Nations Unies pour le Developpement. Union Internationale des Telecommunications, Version Provisoire, Juillet 1998.
10. Rocznik statystyczny 1997. Główny Urząd Statystyczny, Warszawa 1997.
11. Stanisz T.: Funkcje jednej zmiennej w badaniach ekonomicznych. PWN, Warszawa 1993.
12. Zeliaś A.: Teoria prognozy. PWE, Warszawa 1997.

Роман Неребиньски

ЛОГИСТИЧЕСКИЕ КРИВЫЕ В ПРОГНОЗИРОВАНИИ РАЗВИТИЯ ТЕЛЕКОММУНИКАЦИИ

Резюме

Представлено логистические кривые, их особенности и методы оценки их параметров. Рассмотрено использование логистических кривых для прогнозирования развития телекоммуникации на примере телефонных сетей в странах Европейского Сообщества, в Демократической Республике Конго (б. Заир) и в Польше.

Roman Nierebiński

LOGISTIC CURVES IN TELECOMMUNICATIONS DEVELOPMENT FORECASTING

Summary

The logistic curves, their properties as well as the methods of evaluation of their parameters are presented. The utilisation of logistic curves for forecasting the development of telecommunications exemplified by telephony services in CE countries, in Democratic Republic of Congo and Poland are described, too.

Roman Nierebiński

LES COURBES LOGISTIQUES EN PREVISION DE DEVELOPPEMENT DE TELECOMMUNICATION

Résumé

On a présenté les courbes logistiques, leurs propriétés ainsi que les méthodes d'évaluation des leurs paramètres. La discussion est présentée sur

l'utilisation des courbes logistiques pour faire les prévisions de développement de télécommunication en prenant comme exemples la téléphonie dans les pays de l'Union Européenne, en République Démocratique du Congo et en Pologne.

Roman Nierebiński

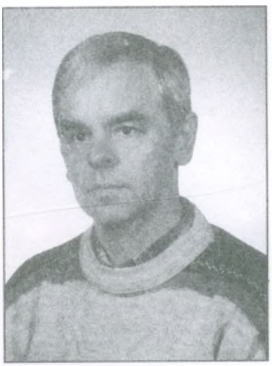
LOGISTIKKURVEN IN TELEKOMMUNIKATIONENTWICKLUNGSVORHERSAGEN

Zusammenfassung

Dargestellt werden Logistikkurven, ihre Eigenschaften und Schätzungsverfahren ihren Parameter. Am Beispiel der Telefonie in UE-Ländern, in der Demokratischen Kongo Republik (früher Zair) und in Polen ist es gezeigt worden, wie Logistikkurven für Telekommunikationentwicklungsvorhersagen zunutze machen kann.

AUTORZY

Mgr inż. Andrzej Binkiewicz urodził się w 1953 r. w Grzmiącej. W 1978 r. ukończył studia na Wydziale Elektrycznym Politechniki Warszawskiej. Przez niemal cały okres działalności zawodowej zajmuje się zagadnieniami zasilania urządzeń elektronicznych. Od 1987 r. do chwili obecnej pracuje w Zakładzie Energetyki Łączności, gdzie projektuje urządzenia zasilające dla telekomunikacji, prowadzi prace analityczne w tym zakresie oraz opracowuje różne dokumenty normatywne dotyczące budowy, eksploatacji i badania systemów zasilających łączności. Jest autorem oraz współautorem kilku publikacji i patentów.



Mgr inż. Roman Nierebiński urodził się w 1953 r. w Śliwicach. W 1977 r. ukończył studia na Wydziale Elektroniki Politechniki Gdańskiej, uzyskując tytuł magistra inżyniera elektronika. Od 1977 r. pracuje w Oddziale Gdańskim Instytutu Łączności, obecnie na stanowisku starszego specjalisty badawczo-technicznego. W latach 1977÷1996 zajmował się między innymi projektowaniem i tworzeniem oprogramowania dla central telegraficznych, problematyką sieci LAN oraz ich współpracy z sieciami publicznymi, sieciami komputerowymi, systemami zarządzania i utrzymania systemów, zagadnieniami ochrony informacji. Od 1997 r. prowadzi badania związane z prognozowaniem

rozwoju usług telekomunikacyjnych. Jest autorem kilkunastu publikacji naukowych.

Dr inż. Elżbieta Andrukiewicz - notkę biograficzną wydrukowano w *Pracach Instytutu Łączności*, nr 108, 1997.

Dr inż. Zbigniew Rymarowicz - notkę biograficzną wydrukowano w *Pracach Instytutu Łączności*, nr 106, 1996.