TELEKOMUNIKACJA I TECHNIKI INFORMACYJNE

3-4/2010

Redakcja

Rada Programowa

ISSN 1640-1549 on-line: ISSN 1899-8933

Nakład: 300 egz.
Sowa - Druk na życzenie, www.sowadruk.pl, tel. 22 431-81-40

Andrzej Hildebrandt

Od Redaktora Naczelnego

Witamy Państwa przy lekturze kolejnego numeru naszego kwartalnika. Zamieściliśmy w nim pięć artykułów. Dwa z nich dotyczą zagrożeń towarzyszących rozwojowi telekomunikacji, dwa dalsze sieci dostępowych, ostatni zaś oszacowania błędów przetwarzania sygnału. Na końcu numeru znajdą Państwo jak zwykle wykaz ważniejszych konferencji planowanych na I półrocze 2011 r.

Burzliwy rozwój telekomunikacji przynosi nie tylko nowe możliwości i różnorodne korzyści. Pojawiają się również związane z nim zagrożenia zarówno dla samych sieci, jak i dla środowiska. Ochronie sieci poświęcony jest artykuł Ryszarda Strużaka „Problemy ochrony sieci teleinformatycznych przed narażeniami i terroryzmem elektromagnetycznym". Ten obszerny artykuł jest ilustrowany przykładami zagrożeń przypadkowych i ich efektami oraz zagrożeń mających postać celowych ataków. Autor przedstawił także wyniki prac prowadzonych w Instytucie Łączności w opisywanym obszarze.

Na zagrożenia dla środowiska, a w szczególności dla człowieka, pochodzące głównie od urządzeń radiokomunikacyjnych zwrócili uwagę Marta Macher, Marek Kałuski i Karolina Skrzypek w artykule „Ochrona środowiska przed elektromagnetycznym promieniowaniem niejonizującym". Autorzy opisali charakter, źródła i efekty zagrożeń oraz wskazali na przepisy krajowe i międzynarodowe służące zabezpieczeniu ludności przed skutkami takich zagrożeń.

Rozwój telekomunikacji to w dużym stopniu rozwój sieci dostępowych, kosztownych i różnorodnych technicznie. Pojawienie się sieci dostępowych nowej generacji na konkurencyjnym rynku wymaga starannie dostosowanych regulacji. W artykule „Polityka regulacyjna dotycząca sieci dostępowych nowej generacji" Stanisław Piątek przedstawił proces formułowania nowej polityki regulacyjnej UE w tym obszarze. Celem tej polityki jest sprzyjanie inwestowaniu w taki sposób, aby nie wytwarzać nowych barier.

Jednym z rozwiązań sieci dostępowych wykorzystujących sieć energetyczną jako medium transmisyjne jest system InHousePLC, przedstawiony przez Henryka Guta-Mostowego w artykule „Systemy InHousePLC – charakterystyka ogólna, kierunki rozwoju i zastosowań". Oprócz szczegółowego opisu systemu autor porównał go z innymi rozwiązaniami dostępu i wykazał jego konkurencyjność cenową.

Przetworniki cyfrowo-analogowe są niezbędnymi elementami radiowych urządzeń nadawczych. Właściwy dobór ich parametrów jest szczególnie ważny w przypadku stosowania modulacji OFDM. Adam Rudziński i Sebastian Kozłowski w artykule „Wymagania na rozdzielczość i nieliniowość przetwornika C/A dla sygnału OFDM" opisali opracowany przez nich model analityczny, który umożliwia oszacowanie parametrów przetwornika gwarantujących utrzymanie zniekształceń poniżej założonego poziomu. Autorzy przeprowadzili także weryfikację numeryczną modelu.

Życzymy Państwu miłego spędzenia Świąt i docenienia również uroków zimy.

Redaktor Naczelny
Andrzej Hildebrandt

Problemy ochrony sieci teleinformatycznych przed narażeniami i terroryzmem elektromagnetycznym

Ryszard Strużak

Omówiono zagadnienia ochrony systemów i sieci teleinformatycznych przed przypadkowymi i celowymi narażeniami elektromagnetycznymi w aspekcie potencjalnych ataków terrorystycznych i rozwoju społeczeństwa informacyjnego. W artykule wykorzystano częściowo wyniki prac prowadzonych w Zakładzie Kompatybilności Elektromagnetycznej Instytutu Łączności we Wrocławiu.

atak elektromagnetyczny, terroryzm elektromagnetyczny, zakłócenia elektromagnetyczne, zagłuszanie, cyberatak, kompatybilność elektromagnetyczna, teleinformatyka, ochrona sieci telekomunikacyjnych

Wprowadzenie

W miarę postępów techniki rośnie liczba urządzeń elektronicznych, zwłaszcza komputerów i bezprzewodowych urządzeń teleinformatycznych. W prognozach *Wireless World Research Forum* podano, że do 2017 r. przypadać będzie średnio tysiąc urządzeń bezprzewodowych na każdego mieszkańca Ziemi [7]. Według wizji społeczeństwa informacyjnego bez granic, będą one współpracować w rozmaitych sieciach połączonych ze sobą; od sieci globalnej do sieci makro, mikro, piko, lub jeszcze mniejszych. Lista takich sieci jest długa i obejmuje, oprócz klasycznych naziemnych i satelitarnych sieci radiowych, telewizyjnych i telefonii ruchowej, bezprzewodowe sieci komputerowe, sieci kontroli i zbierania danych SCADA (*Supervisory Control and Data Acquisition*), bezprzewodowe sieci sensorowe WSN (*Wireless Sensor Networks*), sieci identyfikacji radiowej RFID (*Radio Frequency Identification Device*), bezprzewodowe sieci personalne WPAN (*Wireless Personal Area Networks*), sieci radionawigacyjne i inne. Przyszłość z pewnością przyniesie nowe zastosowania, nowe systemy i nowe sieci. Grupa ekspertów Międzynarodowego Związku Telekomunikacyjnego (ITU – *International Telecommunication Union*) w raporcie przygotowanym dla światowej konferencji „World Summit on Information Society 2005" stwierdza m.in. (w swobodnym przekładzie):

"Postęp technologiczny w teleinformatyce obiecuje świat połączony siecią urządzeń dostarczających użytkownikom potrzebną im informację gdziekolwiek mogą się oni znajdować. Komunikacja człowiek – człowiek i komunikacja człowiek – maszyna zostanie rozszerzona i obejmie komunikację miedzy rzeczami, od przedmiotów gospodarstwa domowego do czujników monitorujących ruchy mostu Golden Gate albo drgania skorupy ziemskiej. Wszystko, od opon samochodowych do szczoteczki do zębów będzie w zasięgu tej sieci, zwiastując świt nowej ery, ery, w której dzisiejszy "internet ludzi" ustąpi miejsca jutrzejszemu "internetowi rzeczy" [11].

Sieć powiązań infrastruktury państwa

Rozwój światowej sieci telekomunikacyjnej ułatwia rozwój powiązań gospodarczych i kulturalnych, nazywanych krótko „globalizacją". Globalizacja z kolei jest motorem napędowym dalszego rozwoju

sieci teleinformatycznych. Sieciowe systemy teleinformatyczne NIS (*Networked Information Systems*) integrują działania ludzi z systemami komputerowymi i telekomunikacyjnymi wypełniając różne funkcje, często na wielkich obszarach geograficznych. Ma to dobre i złe strony. Do dobrych można zaliczyć ułatwienie życia i działalności gospodarczej, kulturalnej, itd. Do złych - uzależnienie od sprawnego działania tych sieci. Funkcjonowanie społeczeństwa, zwłaszcza społeczeństwa informacyjnego, przypomina pracę żywego organizmu, w którym zakłócenie normalnej pracy jednego tylko organu może prowadzić do bardzo poważnych następstw. Na przykład, uszkodzenie jednego nerwu może spowodować ślepotę lub paraliż.

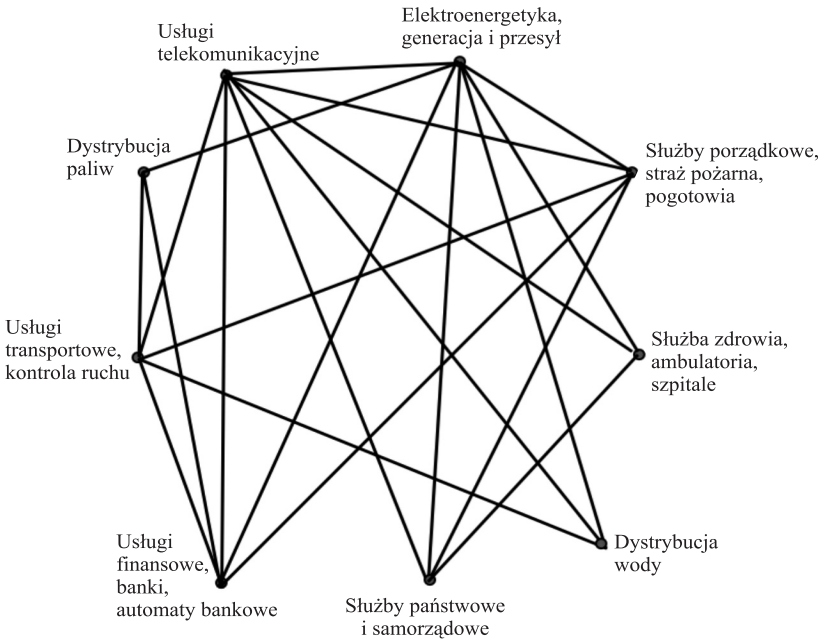
Już obecnie obserwuje się wzrastające uzależnienie od różnych urządzeń i systemów kontrolujących nasze życie. Poranny komunikat meteorologiczny w radiu decyduje o tym jak się ubierzemy. Sprawna winda w domu, w którym mieszkamy i sprawne światła regulujące ruch na skrzyżowaniu ulicy, którą idziemy decydują, czy zdążymy na samolot, na który wykupiliśmy wcześniej bilet korzystając z internetu. Autopilot i inne urządzenia pokładowe decydują o tym, czy dolecimy i wylądujemy na lotnisku docelowym.

Usługi transportowe, energetyczne, finansowe i inne są uzależnione od sprawnego działania wielu innych sieci i systemów, coraz częściej zdalnie sterowanych komputerami. Elektroniczne bazy danych przechowują niezbędne informacje począwszy od metryki urodzenia aż do aktu zgonu, dokumenty finansowe, akta sądowe, itd. w skali lokalnej, regionalnej, krajowej i międzynarodowej. Sieci powiązań funkcjonalnych w skali państwa badała niedawno Komisja Kongresu Stanów Zjednoczonych (nazywana dalej Komisją Grahama, od nazwiska przewodniczącego). W swoim raporcie [8], wyróżniła ona dziesięć głównych obszarów funkcjonalnych infrastruktury państwa:

- elektroenergetyka,
- telekomunikacja,
- banki i usługi finansowe,
- paliwa,
- transport,
- żywność,
- woda,
- służby pogotowia,
- satelity,
- administracja rządowa i samorządowa.

Rysunek 1 ilustruje ważniejsze powiązania wybranych elementów infrastruktury państwa. Punkty reprezentują usługi (lub funkcje), a linie - wzajemne powiązania. Na przykład, dystrybucja paliw płynnych wymaga działających pomp elektrycznych, dlatego wierzchołek *Elektroenergetyka* jest połączony linią z *Dystrybucja paliw*. Podobnie działanie automatów bankowych jest uzależnione od funkcjonowania sieci telekomunikacyjnej, stąd linia łącząca usługi telekomunikacyjne i finansowe.

Życie jednostki oraz funkcjonowanie przedsiębiorstw i całego społeczeństwa zależy od bezbłędnego i niezawodnego działania licznych sieci urządzeń i systemów. Funkcjonowanie wielu służb państwowych, przedsiębiorstw, zakładów przemysłowych, systemów energetycznych itp., jest uzależnione od działania urządzeń elektronicznych, sensorów, komputerów, łączności, urządzeń automatyki, układów



Rys. 1. Wybrane funkcje infrastruktury państwa, i ich ważniejsze powiązania [8]

scalonych, pamięci itp., zwłaszcza w sytuacjach kryzysowych. Nie wszystkie współzależności są pokazane na rysunku – rzeczywiste powiązania i zależności funkcjonalne ujawniają się najwyraźniej w sytuacjach krytycznych. Dla przykładu, powódź w Dolinie Odry w 1997 r., która doprowadziła w trzech krajach (Czechy, Polska i Niemcy) do śmierci 114 osób i szkód materialnych ocenianych na około 4,5 miliarda euro[①], w różnych fazach katastrofy ujawniła różne elementy krytyczne. W raporcie Komisji Sejmowej, powołanej do oceny działalności służb państwowych i samorządowych w czasie powodzi stwierdzono:

”*System ostrzeżeń, informowania i ewakuowania zagrożonej ludności okazał się niesprawny, działał z opóźnieniem, a w pierwszych dniach powodzi - chaotycznie. Szczególnie dotkliwy był brak łączności na terenach zalanych, ponieważ łączność opierała się głównie na sieci telefonów przewodowych, zaś jak wiadomo z doświadczeń poprzednich powodzi, przewody telefoniczne i linie energetyczne, jako pierwsze ulegają awarii już na początku wezbrania. W protokołach komisji badających przyczyny i skutki powodzi 1970, 1972, 1977, 1979, 1980 r. i innych, zawsze, jako najistotniejsze utrudnienie w akcji przeciwpowodziowej wymieniano brak łączności. […] brakowało istotnej informacji z powodu zerwanej łączności lub zalania bądź niedostępności na skutek powodzi. Zalana także została siedziba oddziału wrocławskiego IMGW - głównego źródła komunikatów, prognoz i ostrzeżeń, łączność z tym ośrodkiem była zerwana przez kilka dni. […] Ostatnia powódź przekonała […] o wielkiej roli niezawodnej i trafnej informacji na temat aktualnych i prognozowanych zagrożeń. Konieczność rozwoju nowoczesnych, niezawodnych systemów informacji i prognoz dostrzegają wszyscy, rzecz w tym, aby to priorytetowe zadanie zostało szybko zrealizowane* [3] .

① *Źródło: http://pl.wikipedia.org/wiki/Specjalna:Szukaj/Powodz_tysiaclecia*

Doświadczenia innych krajów są podobne. Huragan Katrina, (sierpień 2005 r.) jeden z największych w Stanach Zjednoczonych, może służyć za przykład. Na skutek uszkodzenia sieci telekomunikacyjnej we wczesnej fazie huraganu, powstała seria kolejnych, powiązanych ze sobą zdarzeń, które doprowadziły do śmierci 1464 osób i do wielkich strat materialnych. Policja, pogotowie ratunkowe zostały sparaliżowane natychmiast. Skutki uszkodzenia sieci elektroenergetycznej ujawniły się później. Nieczynne elektryczne pompy stacji paliw unieruchomiły transport, co z kolei uniemożliwiło ewakuację ludzi, dostawy wody, żywności i sprzętu. Trwało to tygodniami i miesiącami. Nawet po trzech latach po huraganie Nowy Orlean (i okolice) nie doszedł w pełni do normalnego stanu, co można przeczytać w raporcie Komisji Grahama. Należy podkreślić, że miało to miejsce w jednym z najbogatszych i najlepiej zorganizowanych krajów świata. Jakie skutki byłyby w kraju biedniejszym i gorzej zorganizowanym?

Dysfunkcja jednego systemu może prowadzić do uszkodzenia pozostałych powiązanych z nim systemów, tak jak pojedyncza śnieżka może spowodować całą lawinę. Jednoczesna zaś dysfunkcja większej liczby systemów może spowodować ogólną katastrofę. Komisja Grahama podkreśla, że rozdzielanie powiązanych ze sobą systemów i rozpatrywanie ich w oderwaniu od pozostałych utrudnia lub uniemożliwia ocenę rzeczywistej ich współzależności i jej skutków. Niektóre związki są ukryte i trudne do zidentyfikowania. Charles Perrow scharakteryzował ten fakt następująco (w swobodnym przekładzie):

„Stworzyliśmy tak skomplikowane systemy, że nie jesteśmy już w stanie przewidzieć możliwych wzajemnych powiązań i nieuniknionych katastrof: dodajemy urządzenia zabezpieczające, których działanie jest błędne, albo zgoła zbędne, albo też neutralizowane przez ukryte powiązania w systemie”①

Wśród wszystkich systemów, system teleinformatyczny, system energetyczny i system bankowy mają, zdaniem Komisji, podstawowe znaczenie. Krytyczną rolę sieci teleinformatycznej ujmuje najlepiej motto raportu dla Biura Koordynacji Akcji Humanitarnych Organizacji Narodów Zjednoczonych: *„W terenie, niezawodna łączność jest często sprawą życia lub śmierci*” [29]. Z tego też powodu może być ona uprzywilejowanym celem ataków terrorystycznych.

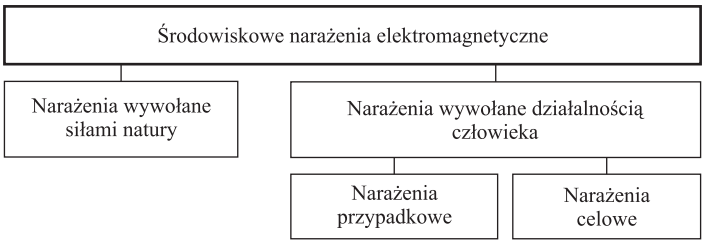
Zagrożenia i narażenia elektromagnetyczne

Większość publikacji na temat przyszłych sieci koncentruje się na fascynujących możliwościach doskonalszych lub całkowicie nowych usług, jakie oferują nowe „inteligentne” technologie sieciowe. Znacznie mniej publikacji omawia ich podatność (wrażliwość) na elektromagnetyczne narażenia środowiskowe②. W miarę jak wzrasta liczba urządzeń wykorzystujących energię elektromagnetyczną i rośnie sieć wzajemnych powiązań, sprawa narażeń i zagrożeń elektromagnetycznych staje się krytyczna. Nowe, lepsze właściwości urządzeń (np. mniejsze rozmiary i koszt) i systemów uzyskiwane są z reguły kosztem większej złożoności i większej podatności na narażenia środowiskowe.

Narażenia elektromagnetyczne mogą być naturalne, wywołane silami natury (np. wyładowaniami atmosferycznymi), albo też mogą być spowodowane działaniem urządzeń wytworzonych przez człowieka. Te ostatnie mogą być przypadkowe albo celowe, jak pokazano na rys. 2. W idealnym świecie (gdyby taki istniał) nie byłoby narażeń celowych (ludzie żyliby bez konfliktów) ani przypadkowych (wszystkie urządzenia byłyby kompatybilne elektromagnetycznie). Byłyby tam jedynie naturalne narażenia elektromagnetyczne.

① *Perrow C: Normal Accidents: Living with High-Risk Technologies Basic Books, NY, 1984 (cytowane za [8]).*

② *Zagrażać znaczy «stać się dla kogoś lub czegoś realnym niebezpieczeństwem» a narażać - «wystawić kogoś albo coś na niebezpieczeństwo, na działanie czegoś szkodliwego» Słownik Języka Polskiego PWN; http://sjp.pwn.pl/.*



Rys. 2. Narażenia elektromagnetyczne mogą być spowodowane siłami natury lub działalnością człowieka

Trzeba pamiętać, że kompatybilność elektromagnetyczna odnosi się do stanu, w którym systemy i urządzenia elektromagnetyczne ani nie zaburzają nadmiernie środowiska (tj. działania innych systemów), ani nie odczuwają zakłóceń środowiskowych w sposób istotny, tj. funkcjonują w nim prawidłowo [5], [19], [23]. Definicje „prawidłowe funkcjonowanie", oraz „środowisko" (otoczenie) odnoszą się do konkretnego przypadku i tak jak „nadmierne zaburzenia" – do określonego ryzyka (prawdopodobieństwa). Zakłócenie elektromagnetyczne (EMI – *Electromagnetic Interference*) jest definiowane jako przeciwieństwo kompatybilności: jest to dowolne zjawisko elektromagnetyczne, które przerywa, blokuje, niszczy, lub w inny sposób obniża wydajność albo bezpieczeństwo urządzeń i procesów. Bezpieczeństwo z kolei jest rozumiane jako stan wolny od nadmiernego ryzyka, nieakceptowanego przez osobę, grupę, lub społeczeństwo. Dalej będą rozpatrywane wyłącznie oddziaływania elektromagnetyczne między urządzeniami; pominięte zaś będą narażenia naturalne i oddziaływania na organizmy żywe.

W świecie realnym ani ludzie, ani urządzenia nie są idealne. Urządzenia często są niekompatybilne elektromagnetycznie. Wiele z nich wytwarza zbędną energię elektromagnetyczną, inne zaś niepotrzebnie reagują na nią. Konkurencja w skrajnych przypadkach prowadzi do konfliktów między ludźmi, które mogą przejawiać się w formie ataków terrorystycznych przy użyciu środków elektromagnetycznych. Takie ataki mogą blokować działanie teleinformatycznej infrastruktury państwa, lub w skrajnym przypadku prowadzić do jej trwałego uszkodzenia. Infrastruktura informatyczna, jej elementy „twarde" (hardware) i „miękkie" (software) mogą same być celem ataku terrorystycznego lub mogą służyć jako narzędzie do ataku na inne cele (np. system elektroenergetyczny). Olbrzymia większość elementów cywilnej sieci telekomunikacyjnej jest celem względnie łatwym. Przy braku rozległych uszkodzeń fizycznych usługi sieciowe mogą być często przywrócone w ciągu godzin lub dni. W tym czasie jednak powstać może chaos i ogólna panika, której skutki mogą trwać dłużej i przynieść nieobliczalne straty. Nieodwracalna utrata lub zafałszowanie krytycznych danych przechowywanych w formie elektronicznej może mieć trwałe skutki dla społeczeństwa.

Sprawy te są omawiane w rozdziale „Atak elektromagnetyczny i terroryzm". Wcześniej, w rozdziale „Narażenia przypadkowe" pokazano, że nawet niezamierzone, przypadkowe oddziaływania elektromagnetyczne mogą powodować poważne skutki. Obserwowany w ostatnich latach trend w kierunku liberalizacji i prywatyzacji zaostrza konkurencję i zwiększa presję na obniżanie kosztów, co odbija się niekorzystnie zarówno na odporności sieci na takie ataki i narażenia, jak i na ograniczanie niepożądanych emisji. Obniżanie kosztów uzyskuje się zwykle przez stosowanie rozwiązań najtańszych, eliminowanie funkcji rzadko używanych, redukcję rezerw itd. Zapobieganie skutkom narażeń elektromagnetycznych z reguły powiększa koszt urządzeń i wydłuża czas ich opracowania. Dla zagwarantowania sobie rynku, firmy stosują celowo rozwiązania niestandardowe i niekompatybilne z innymi, nadużywając często prawa do ochrony interesów tzw. *Trade Secret* i *Intellectual Property Rights*.

W sytuacjach kryzysowych, powoduje to dodatkowe trudności w zapewnieniu niezawodnej i bezpiecznej współpracy urządzeń i systemów oferowanych przez różnych dostawców. W rozdziale „Ochrona przed narażeniami" omawiane są przedsięwzięcia i zalecenia zmierzające do zmniejszenia negatywnych skutków narażeń elektromagnetycznych.

Narażenia przypadkowe

Zdarza się, że urządzenia emitują fale elektromagnetyczne zbędne z punktu widzenia ich normalnego działania lub reagują na przypadkowe bodźce elektromagnetyczne, bez potrzeby. Wskutek tych niezamierzonych emisji i niezamierzonych reakcji powstają szkodliwe oddziaływania i powiązania elektromagnetyczne, które w idealnym świecie nie występują. Takie przypadkowe narażenia elektromagnetyczne mogą powodować zakłócenia w normalnym działaniu urządzeń, a skutki tych zakłóceń mogą być poważne. Richard Haitch pisał (w czasie tworzenia centrum analiz kompatybilności elektromagnetycznej w Annapolis, USA), że diaboliczny aspekt zakłóceń elektromagnetycznych (nazywanych wówczas RFI – *Radio Frequency Interference*) polega na tym, że dowolne urządzenie elektryczne lub jego część może być ich źródłem, zagrażając życiu i mieniu. Mogą to być urządzenia zarówno bardzo skomplikowane, jak i bardzo proste, duże lub małe, działające w pobliżu lub na innym kontynencie.

W Polsce nie zbiera się i nie publikuje systematycznie informacji o takich incydentach, również nie analizuje się ich. Nie istnieją publiczne statystyki dotyczące narażeń elektromagnetycznych i ich skutków. Można je oszacować jedynie na podstawie analizy konkretnych przypadków. Przypadki takie są znane ekspertom, lecz informacje o nich, z różnych powodów, nie są rozgłaszane, z wyjątkiem katastrof, których nie można ukryć przed niezależna prasą. Przedstawione dalej krótko przykłady ilustrują tę różnorodność.

Sieć telekomunikacyjna

Sieć telekomunikacyjna jest jedną z najważniejszych (por. rys. 1) i jednocześnie jedną z najbardziej wrażliwych na narażenia elektromagnetyczne. W czasie pracy w CCIR/ITU① w Genewie, autorowi powierzono rozwiązanie problemu powtarzających się sporadycznie uszkodzeń jedynej linii radiowej łączącej wschodnią i zachodnią część jednego z krajów Ameryki Środkowej. Linia ta prowadziła przez rejony górskie, słabo zaludnione i trudno dostępne. Wymiana (lub naprawa) uszkodzonych urządzeń wymagała dużych nakładów sił, środków i czasu, co prowadziło do znacznych kosztów i długotrwałych przerw łączności. Przeprowadzone badania potwierdziły elektromagnetyczny charakter narażeń. Jednocześnie wykluczyły one możliwość, że źródła tych narażeń podlegają jurysdykcji tego kraju. Przyczyny należało szukać poza granicami kraju, stąd oficjalna prośba rządowa do ITU o wszczęcie międzynarodowej procedury, zgodnie z Konwencją i Regulaminem Radiokomunikacyjnym ITU. Prawdopodobną bezpośrednią przyczyną uszkodzeń było napromieniowanie przez stacje radarowe (pracujące niezgodnie z Regulaminem) na okrętach, które zmierzały w kierunku Kanału Panamskiego. "Prawdopodobną", ponieważ nie udało się zidentyfikować źródła narażeń po rozpoczęciu formalnej procedury mającej na celu wykrycie sprawcy. Zakłócenia bowiem zniknęły – sprawca usunął przyczynę bez rozgłosu. W ten sposób uniknął sporów, roszczeń i konieczności zwrotu kosztów naprawy uszkodzeń i ich skutków. (Według nieoficjalnych informacji radary okrętowe zostały wyposażone w dodatkowe filtry.)

Wcześniej, w Instytucie Łączności, autor spotkał się z problemem zakłóceń po zainstalowaniu stacji bazowej radiokomunikacji ruchomej na budynku jednego z ministerstw. Po uruchomieniu tej stacji wszystkie telefony (przewodowe) w tym budynku i w budynkach sąsiednich przestały prawidłowo

① *Comité Consultatif International des Radio Communications, CCIR – Międzynarodowy Doradczy Komitet Radiokomunikacyjny, obecnie Radiocommunication Bureau, BR-ITU*

działać: w każdym słychać było rozmowy prowadzone w sieci radiowej (która według projektu miała być całkowicie odizolowana od sieci przewodowej). Przyczyną były procesy nieliniowe spowodowane energią wielkiej częstotliwości, przenikającą do przewodów sieci telefonicznej w wyniku jej przypadkowego (silnego) sprzężenia z anteną stacji bazowej.

Inny przykład niezamierzonych zakłóceń w wyniku przypadkowych narażeń elektromagnetycznych dotyczy radiofonii. W centrum jednego z miast uruchomiono nową lokalną stację nadawczą UKF FM. Po jej uruchomieniu okazało się, że odbiór innych stacji w centrum miasta został silnie zakłócony. Przyczyną były procesy nieliniowe w obwodach wejściowych radioodbiorników FM spowodowane zbyt silnym sygnałem nowej stacji i powstawanie niekorzystnej kombinacji częstotliwości odbieranych stacji (intermodulacja).

Richard Haitch opisuje przypadek zakłócania komunikatów straży pożarnej, w stanie Ohio, USA, promieniowaniem radiolatarni, usytuowanej w pobliżu Bristolu, po drugiej stronie Oceanu Atlantyckiego①. Przykłady te ilustrują znaczenie odpowiedniego planowania lokalizacji, częstotliwości, mocy, polaryzacji itp. w sieciach radiowych. Bardziej szczegółowa dyskusja tych zagadnień wykracza poza ramy niniejszego opracowania; są one omawiane m.in. w pracach [15], [23], [25], [30], [31], [32]. W Instytucie Łączności, pod kierunkiem autora, były również badane zakłócenia powodowane urządzeniami grzejnymi. Przy stosowaniu ferromagnetycznego materiału grzejnika i niekorzystnym doborze temperatury punktu Curie, indukcyjność grzejnika zmienia się z częstotliwością 100 Hz (przy zasilaniu siecią 50 Hz). Przy odbiorze lokalnej stacji radiofonicznej i dużych prądach wielkiej częstotliwości wyidukowanych w przewodach sieci zasilającej, na oryginalną modulację sygnału radiowego nakładała się dodatkowa modulacja 100 Hz (wywołana zmienną indukcyjnością grzejnika), zakłócając poważnie odbiór radiowy w najbliższym sąsiedztwie.

Sieci transportowe

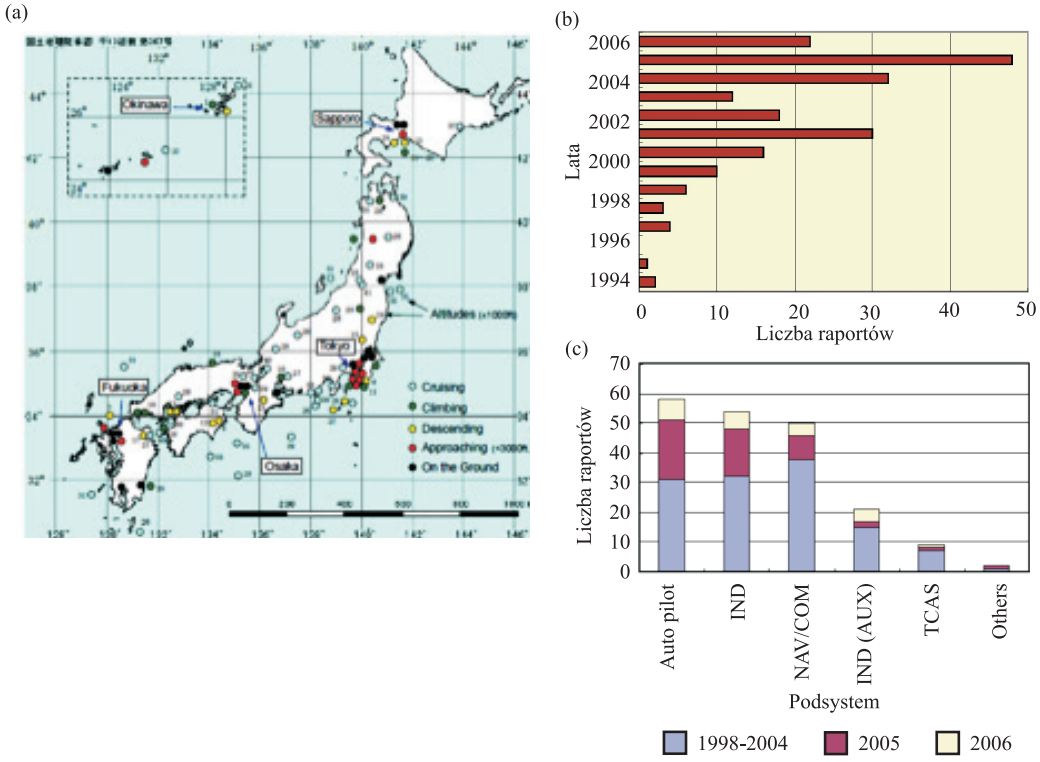
Sprawność transportu warunkuje efektywność wielu usług, jak pokazano na rysunku 1. Nawet prosta awaria sygnalizacji świetlnej w ruchu ulicznym może utrudnić akcje straży pożarnej i pogotowia; dużo poważniejsze następstwa może mieć awaria systemu kontroli lotów. Mimo wysiłków podejmowanych w celu zwiększenia niezawodności systemów nawigacji powietrznej, nadal obserwuje się zakłócenia w ich działaniu . Pozornie nieszkodliwe urządzenia (np. telefony komórkowe, laptopy, magnetofony, dyktafony, radia), mogą poważnie zakłócać pracę systemów elektronicznych na pokładach samolotów. Dla przykładu, w latach 1986–1995 w Stanach Zjednoczonych rejestrowano rocznie około 5200 raportów w sprawie zakłóceń w działaniu urządzeń pokładowych② [14].

Najbardziej chyba spektakularny przypadek opisany w literaturze dotyczy incydentu spowodowanego przez muchę. Zdarzenie miało miejsce na lotnisku Logan (Boston), kiedy mucha uruchomiła zainstalowany w lokalnej restauracji "*Fly-killer*" (urządzenie elektryczne do uśmiercania owadów latających). Zakłóciło to poważnie proces lądowania samolotu Air National Guard. Inny incydent zanotowano na lotnisku w Detroit. Tam, łukowy aparat spawalniczy emitował energię, która zagłuszyła istotny fragment komunikacji z samolotem podchodzącym do lądowania. W Minneapolis, z kolei, uszkodzone styki w domowym dzwonku do drzwi (w odległości około kilometra od lotniska World Chamberlain Field) powodowały krótkotrwałe emisje powtarzające się co kilka minut. Dzwonek działał normalnie, więc uszkodzenie pozostawało niezauważone, ale dzień i noc, uniemożliwiało ono prawidłową komu-

① *Cytowane za IEEE EMCS Newsletter Issue Nr 224, Winter 2010, p. 35; http://www.emcs.org/acstrial/newsletters/winter10/index.html (9 Jun. 2010).*

② *Raporty pilotów, w większości anonimowe, nie podawały ani modeli samolotów, ani nazw linii lotniczych; w 1995 r. zaniechano rejestracji, prawdopodobnie pod naciskiem zainteresowanych firm. Wg NASA Reference Publication 1374, [11].*

nikację z samolotami startującymi i lądującymi do czasu, aż styki te zostały wymienione na nowe. Po zderzeniu w powietrzu dwóch samolotów nad Nowym Jorkiem sugerowano, że niepożądane emisje z przemysłowych urządzeń grzejnych wielkiej częstotliwości uniemożliwiły samolotom prawidłowy odbiór sygnałów radionawigacyjnych, niezbędnych do precyzyjnej kontroli kursu. Sugestie te nie zostały ani odrzucone, ani potwierdzone, ale FCC (*Federal Communication Commission* – odpowiednik polskiego UKE) wydało nakaz wyłączenia tych urządzeń grzejnych z eksploatacji①.



Rys. 3. Przypadkowe (niezamierzone) zakłócenia w lotniczych systemach radioelektrycznych zarejestrowane w Japonii w latach 1998-2006: (a) lokalizacje, fazy i wysokości lotu, przy których zaobserwowano znaczące zakłócenia; (b) liczba incydentów w rozbiciu na lata; (c) podsystemy, których działanie było zakłócone [35]

Na rysunku 3 pokazano wyniki rejestracji i analizy zakłóceń zaobserwowanych w samolotach nad Japonią [39]. Wskazano miejsca występowania zakłóceń, wysokości i fazy lotu oraz typy urządzeń pokładowych, których działanie uległo zakłóceniu. Rysunek został sporządzony na podstawie nieobowiązkowych raportów, jakie piloci przygotowywali po zauważeniu niesprawności urządzeń pokładowych, z podejrzeniem, że zostały one spowodowane urządzeniami elektronicznymi PEDs (*Portable Electronic Devices*) wnoszonymi na pokład przez pasażerów. Analiza ponad 200 raportów z lat 1993–2006 wykazała jednak, że tylko około 30% przypadków można powiązać z urządzeniami wnoszonymi do samolotu. Stwierdzono, że prawdopodobieństwo zakłóceń jest większe na małych wysokościach. Oznacza to, że znaczna część tych zakłóceń jest powodowana przez urządzenia działające na ziemi.

① *Źródło: RFI: Invisible killer? IEEE EMCS Newsletter Issue Nr 224, Winter 2010, p. 35; http://www.emcs.org/acstrial/newsletters/winter10/index.html (9 Jun. 2010).*

Potwierdzają to inne dane. W 2003 r. ukazała się informacja o zakłóceniach elektromagnetycznych powodowanych w pobliżu lotnisk w Wielkiej Brytanii przez produkowane seryjnie urządzenie domowe do zdalnego nadzorowania niemowląt w łóżeczku①. W 2007 r. opisano przypadek zakłóceń spowodowanych układem elektronicznej regulacji seryjnego klimatyzatora umieszczonego na terenie lotniska, na dachu hangaru, w pobliżu pasa startowego [13]. Żaden z opisanych wyżej przypadków nie doprowadził do katastrofy, ale zakłócenia były na tyle poważne, że skłoniły pilotów do zadania sobie trudu formalnego zgłoszenia incydentu.

Pouczający przypadek dotyczy wojskowego satelity wystrzelonego w 1990 r., którego misja skończyła się w 1991 r.; z tą też datą jego pokładowy nadajnik powinien zakończyć swoją aktywność. Tak się jednak nie stało. Satelita pozostał na orbicie a jego nadajnik kontynuuje wysyłanie bezużytecznych sygnałów. Przyczyna jest banalna: nadajnik nie zostal wyposażony w wyłącznik zasilania, a pokładowe źródła energii pracują dłużej niż planowano. Ten satelita, umieszczony na orbicie polarnej „odwiedza" każdy punkt na Ziemi co najmniej dwa razy na dobę, a jego nadajnik, z wysokości około 700 km nad ziemią, zagłusza całkowicie obserwacje radioastronomiczne. Satelita obniża swoją orbitę i w końcu spali sie w atmosferze ziemskiej. Jest to jednak powolny proces i trzeba by czekać na to około tysiąca lat. Wykrycie właściciela satelity zajęło sześć lat i było możliwe tylko dzięki współpracy międzynarodowej. Aby uciszyć nadajnik i umożliwić obserwacje radio-astronomiczne, zatrudniono personel, który okresowo wysyła specjalne rozkazy [31].

Czasami skutki przypadkowych narażeń elektromagnetycznych są tragiczne. W latach 1981–1987 pięć helikopterów wojskowych typu Blackhawk rozbiło się w ówczesnej Republice Federalnej Niemiec, zabijając lub raniąc wszystkich członków załogi. Katastrofy te miały miejsce, kiedy maszyny przelatywały w pobliżu anten nadajników radiowych. Przyczyną były prądy wyidukowane w elektronicznych układach sterowania śmigłowców, interpretowane automatycznie jako polecenia wykonania manewrów, o których pilot nie miał pojęcia [14].

Zakłócenia elektromagnetyczne występują także w innych rodzajach transportu. Na przykład, samochody wyposażone we wczesne modele systemu hamulcowego ABS ulegały wypadkom na niektórych odcinkach niemieckiej autostrady. Wypadki te zdarzały się w pobliżu anten nadawczych urządzeń radiowych. Okazało się, że przyczyną były, wyindukowane w instalacji samochodowej przypadkowe prądy, które system ABS traktował tak jak wciśnięcie pedału hamulca przez kierowcę. Ta poważna usterka została usunięta zaraz po jej wykryciu i odporność systemów ABS na tego typu narażenia została odpowiednio poprawiona. Incydenty takie nie powtórzyły się [14].

Amerykański oddział koncernu Nissan ostrzegł nabywców określonej serii swoich samochodów, aby nie trzymali kluczyków samochodowych blisko telefonów komórkowych. W przeciwnym przypadku ich samochody mogą nie ruszyć z miejsca, będą zablokowane. Problem dotyczył serii umożliwiających zdalne otwieranie i zamykanie drzwi oraz blokowanie silnika samochodu drogą radiową. Stwierdzono, że przy odległościach między kluczykiem i telefonem mniejszych niż cal (2,5 cm) sygnały, jakie każdy telefon wysyła automatycznie do swojej stacji bazowej mogą zmienić zapis kodu niezbędnego do odblokowania silnika②. Ta sama zasada może być wykorzystana do celowego zatrzymywania pojazdów: policja w Los Angeles zamówiła specjalne urządzenie w celu zatrzymywania podejrzanych samochodów na odległość.

Niepożądane efekty przypadkowych narażeń elektromagnetycznych obserwuje się również w transporcie szynowym. Na przykład, po wprowadzeniu automatycznej rejestracji ruchu wagonów kolejowych,

① *Na podstawie http://www.ofcom.org.uk/static/archive/ra/topics/research/RAwebPages/Radiocomms/pages/interexpl/houseapp.htm#babyalarm (2003)*

② *Źródło: Gazeta Wyborcza, 11.06.2007 r.*

zaobserwowano na pewnym obszarze objawy podobne do „czarnej dziury", znanej z astronomii: wagony wjeżdżały do tego obszaru, ale żaden go nie opuszczał – wagony jakby „ginęły" w nim bez śladu. Badania wykazały, że powodem były uszkodzenia wagonowych urządzeń RFID *(Radio Frequency Identification)* spowodowane stacją radarową działającą na tym obszarze. System rejestrował prawidłowo symbole identyfikacyjne wagonów wjeżdżających, ale z powodu tych uszkodzeń nie mógł zarejestrować wagonów wyjeżdżających①. Tak jak w poprzednich przykładach, był to efekt niedostosowania poziomu wrażliwości urządzeń do poziomu środowiskowych narażeń elektromagnetycznych na tym obszarze. Inne zjawisko zaobserwowano w Japonii, po wprowadzeniu kolei magnetycznej (maglev – *Magnetic Levitation* – lewitacja magnetyczna). W tym rozwiązaniu, tradycyjne torowisko jest zastąpione przez pole elektromagnetyczne podtrzymujące wagony bez kontaktu mechanicznego z torowiskiem, co eliminuje zjawisko tarcia. Stwierdzono, że zmieniające się podczas ruchu pociągu pole magnetyczne powoduje przedwczesne zmęczenie zbrojenia mostów żelbetonowych i zmniejszenie ich wytrzymałości②.

W transporcie morskim, z kolei, znany jest przypadek, kiedy instrumenty pokładowe okrętu przycumowanego w porcie wskazywały, że okręt ten nie stoi w miejscu, lecz płynie z dużą prędkością. Przyczyną były niekompatybilne systemy energetyczne i nawigacyjne okrętu③.

Przyczyny katastrof są zazwyczaj badane komisyjnie. Komisja bierze zwykle pod uwagę szereg czynników, np. stan techniczny urządzeń (a w przypadku katastrof lotniczych zapis wskazań przyrządów pokładowych), ale czy te dane wystarczają do wykluczenia efektów przypadkowych narażeń elektromagnetycznych? Najczęściej podawaną przyczyną katastrofy jest błąd pilota, który już nie żyje i nie może przedstawić swojej wersji zdarzenia. Takie orzeczenia satysfakcjonują wszystkich zainteresowanych: opinię publiczną, państwowe organy kontrolne, producentów sprzętu, służby eksploatacji itd.

Sieci sensorowe

Rozłożone sieci sensorowe, przewodowe i bezprzewodowe, są szczególnie narażone na zakłócenia elektromagnetyczne. We wspomnianym Raporcie Grahama został opisany przypadek uszkodzenia sieci zaopatrujących ludność w wodę i gaz. W 1999 r. dwa duże przedsiębiorstwa, San Diego County Water Authority i San Diego Gas and Electric, doświadczyły poważnych zakłóceń w pracy zautomatyzowanych systemów rozdzielczych wody i gazu: zdalna kontrola i sterowanie zaworów przestały funkcjonować. San Diego County liczy 3 miliony mieszkańców i rozciąga się ponad 100 km w kierunku północ-południe i 200 km ze wschodu na zachód. Potencjalny efekt niesprawności sieci rozprowadzania wody, to przerwy w dostawach, powódź i znaczne szkody wyrządzone przedsiębiorstwom, organizacjom i osobom prywatnym. Aby ograniczyć straty i zapobiec katastrofie, przedsiębiorstwa te były zmuszone wyłączyć automatykę i wysyłać personel w teren w celu ręcznej kontroli i ustawiania zaworów rozmieszczonych w dużej odległości od siebie. Przyczyną tych wydarzeń było zniszczenie elementów systemu nadzoru i zbierania danych SCADA (*Supervisory Control and Data Acquision*), spowodowane przypadkowym „naświetleniem" wiązką fal radarowych z okrętu w odległości około 25 mil morskich (około 46 km).

Eksplozje

W 1984 r. wybuchł skład amunicji w ZSRR. Przyczyną był radar dalekiego zasięgu, który przypadkowo „oświetlił" skład [14]. Podobnie, Raport Grahama opisuje m.in. katastrofę, jaka wydarzyła się w 1980 r. w Holandii, w okolicy portu Den Helder. Miała tam miejsce awaria gazociągu średnicy

① *Komunikat prywatny (Parlow)*
② *Komunikat prywatny (Yoshino)*
③ *Komunikat prywatny (XXpl)*

36 cali, która zakończyła się poważnym wybuchem gazu. Przyczyną były przypadkowe zakłócenia systemu SCADA, spowodowane radarem okrętu przepływającego w sąsiedztwie. W 1967 r. głośny był „Forrestall incident" - seria wybuchów i pożar na lotniskowcu Forrestall. Zginęło wówczas ponad 130 osób, a straty przekroczyły 70 milionów dolarów. Przyczyną był radar okrętowy, który „oświetlił" uzbrojony samolot bojowy na pokładzie [33]. Podobne wydarzenia, w mniejszej skali, zdarzały się częściej. Inne pouczające przykłady można znaleźć, np. w poradniku opublikowanym w 2008 r. w Anglii przez The Institution of Engineering and Technology [8].

Wypadki przy pracy

Znane są przypadki narażeń elektromagnetycznych, które powodują naruszenie warunków bezpieczeństwa pracy. Należy do nich, np. przypadek poparzenia pracownika, który dotknął ładunku dźwigu budowlanego. Przyczyną była energia z pobliskiego nadajnika radiowego, wyindukowana w pętli utworzonej przez metalową konstrukcję dźwigu i jego linę nośną, przenoszony ładunek i ciało pracownika. Podobnie, w dokach wojskowych w Oakland, personel rozładowujący ładunek ulegał bolesnym poparzeniom i szokom elektrycznym. Badania wykazały, że stalowe dźwigi portowe działały jak anteny odbierające energię z pobliskiego nadajnika stacji radiofonicznej, która powodowała uderzenia prądem i poparzenia. Działo się to w odległości około kilometra od nadajnika. Rozwiązaniem problemu było przesunięcie rozładunku na godziny nocne, kiedy stacja nadawcza nie działała[①].

Urządzenia zdalnie sterowane drogą radiową są szczególnie wrażliwe na promieniowane narażenia elektromagnetyczne. W 2006 r. inwalida z Wielkiej Brytanii – były operator zdalnie sterowanego dźwigu – zwrócił się do autora z prośbą o ekspertyzę w jego sporze z pracodawcą. Uległ on wypadkowi przy pracy w wyniku uderzenia ładunkiem, który podnosił na dużą wysokość, posługując się wspomnianym dźwigiem. Twierdził, że ładunek spadł przypadkowo. Pamiętał, że w chwili wypadku przejeżdżał w pobliżu samochód pogotowia. Był przekonany, że to ten samochód spowodował upadek ładunku. Pracodawca natomiast twierdził, że to była wyłącznie wina pracownika. Rok po incydencie nie było jednak możliwe potwierdzenie jego wersji, ani wersji pracodawcy.

Nie jest to jedyny taki zbieg okoliczności. Znany jest przypadek śmierci pracownika w odlewni metalu, kiedy napowietrzny transporter wylał na niego kadź roztopionego metalu transportowanego z pieca do formy odlewniczej ponad głowami pracowników. Bezpośrednią przyczyną wypadku było promieniowanie radiotelefonu uruchomionego w pobliżu. Podobnie, działanie radiotelefonu pogotowia medycznego doprowadziło do śmierci pacjenta transportowanego do kliniki po ataku serca. W czasie transportu, w celu uruchomienia akcji serca, używano elektronicznego defilibratora. Kiedy personel medyczny telefonował z drogi do kliniki, w celu przygotowania operacji, defilibrator przestawał działać. W rezultacie pacjent zmarł przed dotarciem do kliniki. Wymiana dachu ambulansu z plastikowego na metalowy rozwiązała problem [14].

Nie tylko defilibratory mogą być wrażliwe na zakłócenia elektromagnetyczne; inny sprzęt medyczny również. W latach 1979–1993, agencja do spraw żywności i leków Stanów Zjednoczonych – FDA (*Food and Drug Administration*) otrzymała blisko sto raportów traktujących o poważnych problemach zakłóceń [14]. Przykład, który budzi wesołość na wykładach autora, dotyczy implantów. Pastorowi w San Francisco, leczącemu się na impotencję, wszczepiono sterowany radiem prototyp implantu, który wywoływał erekcję "po naciśnięciu guzika". Urządzenie działało bezbłędnie, ale pastor skarżył się, że doświadcza także niekontrolowanych, niechcianych erekcji, za każdym razem, kiedy sąsiad otwiera zdalnie

① *Źródło: RFI: Invisible killer? IEEE EMCS Newsletter Issue Nr 224, Winter 2010, p. 35; http://www.emcs.org/acstrial/newsletters/winter10/index.html (9 Jun. 2010)*

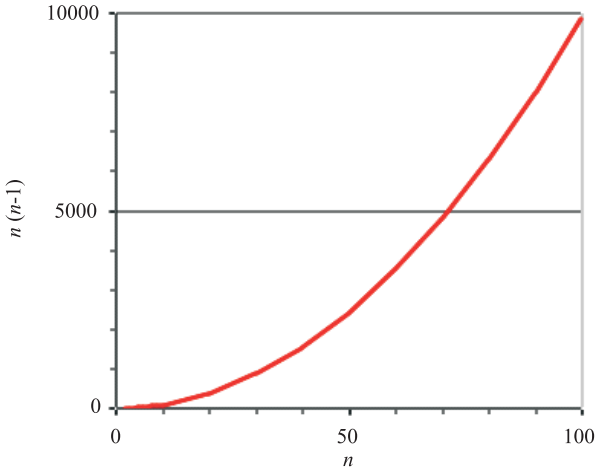
drzwi garażu. Komentował ten fakt następująco (w swobodnym przekładzie): „To jest dość niewygodne w czasie pracy w ogrodzie, ale naprawdę uciążliwe podczas odprawiania nabożeństwa”[①].

Czego możemy oczekiwać?

Współczesne urządzenia wykorzystują olbrzymie moce, na przykład radary wojskowe są zdolne dosłownie upiec człowieka znajdującego się w pobliżu anteny. Im większa moc, tym większe prawdopodobieństwo zakłóceń pracy innych urządzeń. Z drugiej strony szybkość transmisji informacji jest olbrzymia i stale rośnie; dziesięć milionów bitów przesyłanych drogą radiową w ciągu sekundy jest już standardem w wielu krajach. Kilkusekundowa przerwa w transmisji może zniszczyć pokaźną porcję informacji.

Wspomniany wcześniej wzrost liczby urządzeń elektrycznych i elektronicznych prowadzi do zmniejszania odległości między nimi, podobnie postępująca miniaturyzacja i gęstość upakowania elementów. Miniaturyzacja i rozpowszechnienie urządzeń zbliża „ofiary” zakłóceń do „agresorów”. Stosowanie coraz mniejszych mocy i coraz niższych napięć zasilających w urządzeniach elektronicznych (*Green Radio Technologies*), powoduje, że nowe układy elektroniczne są bardziej wrażliwe na narażenia elektromagnetyczne. Nawet słabe pola elektromagnetyczne mogą zakłócać ich działanie lub w szczególnych warunkach nawet powodować ich trwałe uszkodzenia.

Wzrasta liczba potencjalnych oddziaływań elektromagnetycznych między urządzeniami. Ich efekt zależy od poziomu narażeń generowanych, od poziomu wrażliwości na te narażenia i od stopnia (siły) sprzężenia. Teoretycznie, jeżeli jest n urządzeń, to każde z nich może oddziaływać z co najwyżej $(n-1)$ sąsiednimi urządzeniami. Potencjalna liczba oddziaływań wynosi więc co najwyżej $n(n–1)$ i rośnie w przybliżeniu (dla dużych n) z kwadratem liczby urządzeń (rys. 4).



Rys. 4. Wzrost liczby potencjalnych wzajemnych zakłóceń w zależności od liczby obiektów (n) powodujących zakłócenia i wrażliwych na nie

Przy obecnym stanie techniki i obecnym systemie kontroli wykorzystania fal radiowych przypadkowe narażenia i zagrożenia elektromagnetyczne są nieuniknione, niezależnie od regulacji krajowych i konwencji międzynarodowych. Przyczyną jest najczęściej lekceważenie problemu, oraz ignorancja

① *Źródło: Europa Times, 22.03.1995*

projektantów i użytkowników urządzeń. Środki przeciwdziałania narażeniom elektromagnetycznym i ich skutkom wydłużają czas opracowania urządzeń i powiększają ich koszt.

Przypadkowe oddziaływania elektromagnetyczne stosunkowo rzadko prowadzą do poważnych zakłóceń takich jak opisane w tej części artykułu. Zawsze powodują jednak wzrost tła szumów radiowych. Szumy te zmniejszają wierność, szybkość i zasięg transmisji informacji drogą radiową [25]. W latach osiemdziesiątych autor szacował, że poziom szumów radiowych w miastach podwaja się co pięć do dziesięciu lat [27]. Od tamtego czasu oszacowania te nie zostały ani potwierdzone ani poprawione. Jeżeli są one prawdziwe, to dla zachowania stałego poziomu szumów środowiskowych, wysiłki skierowane na ich ograniczanie powinny rosnąć w takim samym tempie.

Atak elektromagnetyczny i terroryzm

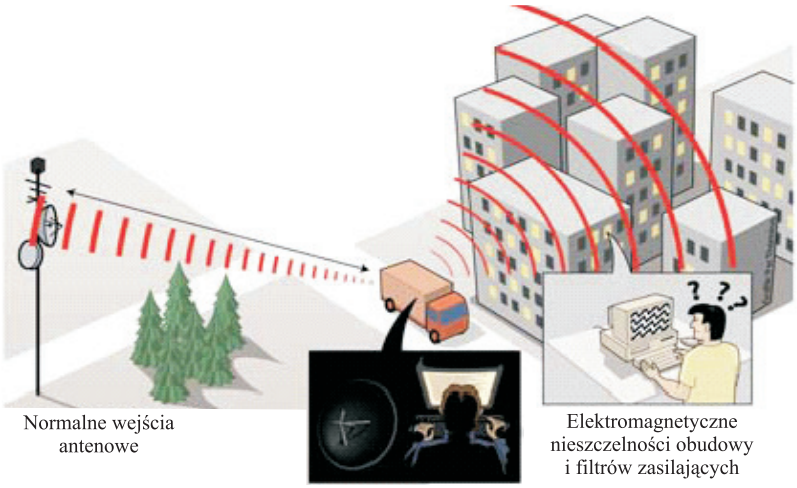
Niezamierzone narażenia elektromagnetyczne mogą prowadzić do poważnych następstw. Występują one wskutek zbiegu okoliczności, w przypadkowych miejscach i przypadkowych momentach. Tutaj zostaną omówione narażenia zamierzone, które mogą mieć następstwa jeszcze bardziej poważne; mogą być celowo wywoływane w krytycznych miejscach i w specjalnie wybranym czasie – ataki elektromagnetyczne. Badania w tym obszarze były przez długi czas ograniczone do urządzeń i instalacji wojskowych, stąd obecnie w wielu krajach urządzenia te są uodpornione na taki atak.

Jednak terroryzm przesunął obszar zagrożeń z urządzeń wojskowych na obiekty cywilne w centrach miast. Dodatkowo upowszechnienie wiedzy i techniki doprowadziło do tego, że przepisy na budowę tanich generatorów narażeń elektromagnetycznych w „warunkach domowych" krążą w internecie. Międzynarodowa Unia Nauk Radiowych URSI (*Union Radio-Scientifique Internationale*) na swym XXV Zgromadzeniu Plenarnym (Toronto, 1999 r.) przyjęła rezolucję zatytułowaną „Działania kryminalne przy wykorzystaniu narzędzi elektromagnetycznych" (*Criminal Activities Using Electromagnetic Tools*). Powstały nowe terminy, takie jak „Wojna elektroniczna" (*Electronic Warfare* – EW [1]) [4], „Terroryzm elektromagnetyczny" (*EM Terrorism*), „Atak elektromagnetyczny", „Przeżywalność" (*Survivability*), „Sabotaż elektromagnetyczny" (*Electromagnetic Sabotage*), „Nuklearny impuls elektromagnetyczny, NEMP" czy „Celowe zakłócenia elektromagnetyczne, IEMI" (*Intentional Electromagnetic Interference*), które weszły już na trwałe do terminologii fachowej.

Atak elektromagnetyczny jest definiowany jako celowa generacja energii elektromagnetycznej wprowadzająca szumy lub sygnały do systemów elektrycznych i elektronicznych i w ten sposób przerywająca, myląca lub niszcząca te systemy w celach terrorystycznych lub kryminalnych. Podobne określenia można znaleźć w innych miejscach. Na przykład, w amerykańskim słowniku terminów telekomunikacyjnych „intruzja elektromagnetyczna" jest zdefiniowana jako celowe wprowadzenie energii elektromagnetycznej do kanału telekomunikacyjnego, jakimkolwiek sposobem, w celu wprowadzenia w błąd lub dezorientacji operatora lub systemu (*Electronic Deception* [1]). Szkody spowodowane takim atakiem mogą być niezauważone natychmiast i pozostać niezauważone w ciągu długiego okresu czasu, albo też zauważone szkody mogą nie być kojarzone z takim atakiem.

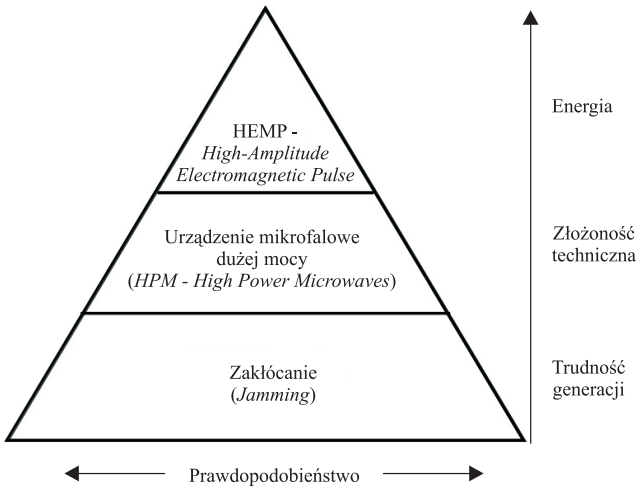
Atak elektromagnetyczny jest łatwiejszy w sieciach bezprzewodowych niż w sieciach kablowych, ponieważ może być dokonany na odległość. To dotyczy także przechwytywania informacji (*Intelligence, Signals Intelligence* (SIGINT), *Electronics Intelligence* (ELINT), *Foreign Instrumentation Signals Intelligence* (FISINT) [1]). Zagadnienie to przedstawiono na rysunku 5. Oprócz stacji bazowej i komputera (w pomieszczeniu biurowym lub mieszkalnym) pokazana jest aparatura użyta do ataku (ukryta w samochodzie), wytwarzająca niezbędną energię elektromagnetyczną. W samochodzie mogą być też generatory fałszywych sygnałów i/lub urządzenia przechwytywania informacji („podsłuchu") bez wiedzy i zgody nadawcy/odbiorcy. Na rysunku pokazano też dwa rodzaje sprzęże-

nia urządzenia atakującego (lub przechwytującego) i ofiary. Pierwszy to normalne wejście sygnałowe (*Front-Door Coupling*), drugi natomiast to elektromagnetyczne nieszczelności obudowy i filtrów zasilających (*Back-Door Coupling*).



Rys. 5: Energia fal elektromagnetycznych może być wykorzystana do skrytego ataku elektromagnetycznego lub do przechwytywania informacji (podsłuchu) na odległość [2]

Atak elektromagnetyczny może być nieniszczący lub niszczący. Przykładem ataku nieniszczącego może być zagłuszanie. Do ataków niszczących mogą być stosowane mikrofalowe generatory mocy lub generatory impulsów wielkiej mocy. Prawdopodobieństwo terrorystycznego ataku elektromagnetycznego jest tym większe im mniejszy jest stopień złożoności i energia narzędzi ataku, jak pokazano na rysunku 6.



Rys. 6. Kategorie narażeń elektromagnetycznych; ich prawdopodobieństwo maleje wraz z trudnością generacji, stopniem skomplikowania i energią

Szczególnie wrażliwe są rozległe systemy sensorowe, alarmowe, nadzoru i zbierania danych SCADA, oraz rozległe urządzenia sterowane zdalnie. Dotychczas większość takich systemów nie była projektowana z myślą o możliwych atakach elektromagnetycznych. Dotyczy to zwłaszcza systemów bezprzewodowych, których popularność ciągle rośnie. Na ogół nie są one odporne na ataki elektromagnetyczne, także ze względów ekonomicznych.

Cyberatak

Cyberatak polega na skrytej modyfikacji programów i danych, przechowywanych lub przesyłanych w formie elektronicznej, w celu przejęcia kontroli nad nimi. Tradycje takiego działania sięgają początków telekomunikacji. W 1867 r. zanotowano, że gracz na giełdzie Wall Street, wspólnie z pracownikiem operatora Western Union przechwytywał telegramy wysyłane z zachodu Stanów Zjednoczonych do gazet publikowanych na wschodzie i zmieniał ich treść informując czytelników o rzekomych bankructwach i innych finansowych problemach tamtejszych firm. Kiedy w wyniku takich wiadomości kursy akcji tych firm spadały, skupował je za bezcen.① Dzisiaj, przestępca internetowy najczęściej dokonuje podobnych fałszerstw samodzielnie. Narodowa rada naukowa Stanów Zjednoczonych (*National Research Council*) ujmuje sprawę następująco:

"*Współczesny złodziej, posługując się komputerem, może ukraść więcej niż używając broni. Jutrzejszy terrorysta może spowodować większe szkody posługując się komputerem niż bombą. Do tej pory mieliśmy duże szczęście. Tak, były kradzieże pieniędzy i informacji. Tak, były incydenty śmiertelne z powodu zakłócenia pracy komputerów. Tak, uszkodzone komputery przerywają normalne działanie systemów telekomunikacyjnych i finansowych. Ale, o ile możemy stwierdzić, nie było dotychczas systematycznej zakończonej sukcesem próby zniszczenia jakiegokolwiek z naszych krytycznych systemów komputerowych. Niestety, jest powód, aby spodziewać się, że nasze dotychczasowe szczęście wkrótce się skończy. Dotychczas nie było wrogich ludzi zdolnych i umotywowanych do szkodzenia naszemu państwu. W Stanach Zjednoczonych wrażliwość systemów teleinformatycznych na narażenia elektromagnetyczne, z punktu widzenia operacyjnego i technologicznego, powiększa się szybciej niż zdolność (i chęć) rządu do reakcji na to zagrożenie*." [20]

Opisana sytuacja istnieje nie tylko w Stanach Zjednoczonych: stwierdzenie cytowane powyżej znajduje pełne zastosowanie także w Polsce i w innych krajach. Co sześć sekund rejestruje się kradzież tożsamości w sieci i ponad 35 tysięcy ataków wirusowych, a „cybercrime" – przestępstwa dokonane za pośrednictwem sieci teleinformatycznej dają łup przewyższający dochody z nielegalnego handlu narkotykami② i straty dla legalnego biznesu szacowane na 1 trylion dolarów US③.

Cyberatak ma miejsce w przestrzeni wirtualnej, polega na modyfikacji programów i danych w pamięci komputera. Wymaga od atakującego mistrzowskiego opanowania tajników programowania komputerów. Można go porównać do precyzyjnej operacji neurochirurgicznej na otwartym mózgu, która wymaga najwyższych kwalifikacji i precyzyjnych narzędzi. Takie same efekty można uzyskać w sposób niewymagający wielkich kwalifikacji i precyzji, stosując prostsze środki: atak w przestrzeni elektromagnetycznej. Najłatwiejszy jest atak nieniszczący, znany też jako zakłócanie lub zagłuszanie.

Zagłuszanie

Zagłuszanie (zakłócanie) (*Jamming* [1]) w przestrzeni elektromagnetycznej powoduje, że przekazywana lub gromadzona informacja staje się bezużyteczna, ale fizyczna struktura zagłuszanego systemu nie ulega przy tym uszkodzeniu. Zagłuszanie jest stosowane przede wszystkim na polu walki. W czasie

① *Źródło: Technical Aspects of Lawful Interception; ITU-T Technology Watch Report 6, May 2008.*

② *Informacja zaczerpnięta z opisu programu "Norton antivirus".*

③ *Dane według ITU News, October 2009, str. 10.*

tzw. „Zimnej Wojny" minionego stulecia zagłuszanie audycji radiowych było stosowane na szeroką skalę na pewnych obszarach geograficznych z powodów politycznych, w celu blokowania informacji①. Obecnie, przy rozpowszechnieniu systemów zautomatyzowanych skutki zagłuszania informacji mogą być groźniejsze, urządzenia techniczne bowiem z reguły mają bardziej ograniczone możliwości rozróżniania sygnału użytecznego od zakłócenia niż ludzie. Łatwo sobie wyobrazić zagłuszenie (oślepienie) systemu nadzorującego krytyczny obszar w czasie napadu rabunkowego, albo terrorystycznego. Podobnie, zagłuszanie sygnałów nawigacji satelitarnej GPS może powodować błędy w działaniu systemów lądowania samolotów, co z kolei może doprowadzić do katastrofy.

Należy tu zwrócić uwagę, że urządzenia zakłócające są z reguły łatwiejsze do produkcji i znacznie tańsze niż urządzenie telekomunikacyjne projektowane z myślą o wiernej transmisji sygnałów i mogą być składane z elementów dostępnych w handlu bez ograniczeń, tzw. COTS (*Commercial-Off-The-Shelf*).

Atak niszczący

Tak jak atak w przestrzeni wirtualnej można porównać do operacji neurochirurgicznej, tak niszczący atak elektromagnetyczny można porównać do brutalnego uderzenia młotem. Nie wymaga on znajomości programowania: do zniszczenie elementów fizycznej infrastruktury potrzebna jest tylko odpowiednio duża energia. Taki atak elektromagnetyczny nie musi niszczyć całej infrastruktury: wystarczy uszkodzenie jednego elementu krytycznego, prowadzącego np. do krótkiej przerwy w zasilaniu ważnego systemu. Raport Komisji Grahama cytuje jako przykład efekty krótkotrwałego zaniku zasilania energią elektryczną rafinerii w Pembroke (Wielka Brytania). Przerwa w zasilaniu trwała zaledwie 0,4 s. W efekcie zakłócony został proces technologiczny powodując szereg wybuchów, pożarów i innych niekontrolowanych zdarzeń. Efekt końcowy to straty szacowane na 70 milionów dolarów USA, 4,5 miesiąca przymusowego postoju i spadek o 10% zdolności produkcyjnych całego krajowego przemysłu rafineryjnego.

W internecie można znaleźć informacje o urządzeniu promieniującym fale radiowe o wielkiej energii, o tzw. e-bombie lub bombie FCG (*Flux Compression Generator*), którą można rzekomo skompletować „domowym sposobem" z powszechnie dostępnych elementów za około 400 dolarów USA. Ta łatwość produkcji i niewielki koszt budzą uzasadniony niepokój. Inna wersja takiego urządzenia „domowej roboty" to HMP (*High Power Microwaves*) – urządzenia mikrofalowe dużej mocy, które można wykorzystać do trwałego uszkodzenia elementów elektronicznych na odległość. Co ważniejsze, można go stosunkowo łatwo, bezpiecznie, i niewielkim kosztem wytworzyć w prymitywnych warunkach, np. w garażu. Na rysunku 7 przedstawiono przykład takiego urządzenia.

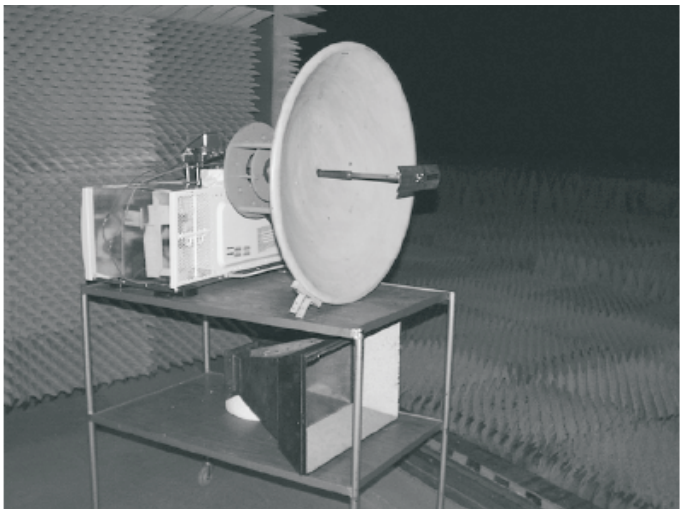
Składa się ono z elementów domowej kuchenki mikrofalowych i anteny do odbioru telewizji satelitarnej, łatwo dostępnych na rynku. Urządzenie to wytwarza energię elektromagnetyczną wystarczającą do zakłócenia lub zniszczenia na odległość wrażliwych elementów infrastruktury teleinformatycznej: układy scalone w telefonach komórkowych i stacjach bazowych, w odbiornikach systemów nawigacyjnych GPS, w bezprzewodowych sieciach komputerowych itd. Przeprowadzono eksperyment poddania komputerów Pentium 133 i Pentium II 233 i 300 MHz narażeniom elektromagnetycznym o parametrach:

- częstotliwość 1,040 – 2,887 GHz,
- natężenie pola 30 – 100 V/m,

① *Według prasy codziennej w niektórych państwach stosuje się go obecnie.*

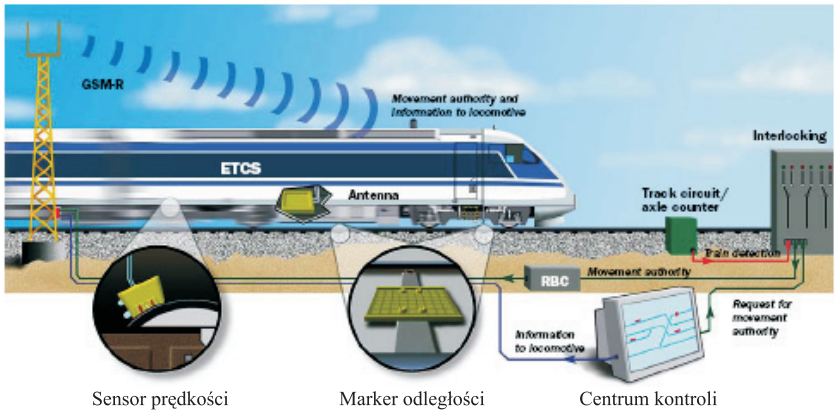
– modulacja CW, AM.

Wystąpiły takie niepożądane efekty, jak: błędy zapisu, utrata danych, resetowanie, utrata dostępu i utrata zasilania w komputerze [34].



Rys. 7. Elementy domowej kuchni mikrofalowej i anteny do odbioru telewizji satelitarnej, które mogą być wykorzystane do ataku elektromagnetycznego [2]

W paneuropejskim systemie sygnalizacji kolejowej i zarządzania ruchem, ERTMS (*European Rail Traffic Management System*), który jest wprowadzany w niektórych krajach europejskich: Holandii, Hiszpanii, Włoszech, Szwajcarii i Szwecji, wszystkie instrukcje i informacje dla motorniczego będą przekazywane drogą radiową (rys. 8). Działanie każdego z jego elementów, np. stacji bazowej, sensora prędkości, markera odległości, może być zakłócone na odległość w wyniku ataku elektromagnetycznego. W szeregu krajów prowadzone są badania nad wrażliwością i sposobami ochrony tego systemu przed takim atakiem.



Rys. 8. Elementy paneuropejskiego systemu sygnalizacji kolejowej i zarządzania ruchem, ERTMS, których działanie może być zakłócone w wyniku ataku elektromagnetycznego [18]

NEMP – nuklearny impuls elektromagnetyczny

Impuls elektromagnetyczny EMP (*Electromagnetic Pulse*) a zwłaszcza nuklearny impuls elektromagnetyczny NEMP (*Nuclear Electromagnetic Pulse*) jest najsilniejszym opisanym w literaturze źródłem energii, przeznaczonym specjalnie do trwałego niszczenia infrastruktury teleinformatycznej na dużym obszarze geograficznym. Dla zwiększenia zasięgu zniszczeń, impuls jest wytwarzany na pewnej wysokości nad powierzchnią ziemi (ponad ok. 120 km) i jest nazywany wówczas HEMP (*High-Altitude Electromagnetic Pulse* [1]). Taki impuls towarzyszący wybuchowi nuklearnemu zaobserwowano już przy pierwszych próbach broni jądrowej w 1945 r., jednak dopiero w 1954 r. opublikowano jego objaśnienie teoretyczne [5].

Dostępne są obecnie informacje na temat wczesnych eksperymentów z nuklearnym atakiem elektromagnetycznym. W 1962 r. Stany Zjednoczone przeprowadziły próbną eksplozję ładunku nuklearnego (1,4 Mt) na wysokości 400 km nad Pacyfikiem. Zanotowano wówczas uszkodzenia systemów alarmowych i oświetlenia ulicznego w odległości około 1500 km od miejsca wybuchu (w Honolulu). Zaobserwowano również przerwanie radiokomunikacji mikrofalowej. Niektóre satelity zostały uszkodzone w czasie testu i w okresie 6 miesięcy po nim, z powodu powstania wokół Ziemi nowych przejściowych obszarów intensywnego promieniowania [8].

Podobny eksperyment w Związku Radzieckim (na Syberii) pokazał np., że kabel elektroenergetyczny zakopany na głębokości kilkudziesięciu centymetrów pod ziemią uległ zniszczeniu w zasięgu kilkuset kilometrów od miejsca wybuchu. Eksperymenty dostarczyły danych do opracowania teorii i modeli symulacyjnych. Można spekulować, że ich celem było także zademonstrowanie skutków takiego ataku najwyższym władzom politycznym kraju. Te eksperymenty przeprowadzano nad obszarami niezamieszkałymi lub bardzo słabo zaludnionymi. Brak danych o skutkach takiego ataku na obszary uprzemysłowione i zurbanizowane. O skali szkód można jedynie wnioskować na podstawie raportów z katastrof naturalnych oraz z badań laboratoryjnych elementów sieci, lub na podstawie symulacji komputerowych [5], [8], [9], [21], [22], [36].

Rys. 9. Wyniki symulacji komputerowej ataku nuklearnym impulsem elektromagnetycznym, wytworzonym w celu zniszczenia krytycznej infrastruktury teleinformatycznej Stanów Zjednoczonych. Okrąg pokazuje zasięg zniszczeń. Dla porównania zamieszczono także mapę konturową Polski w tej samej skali.

Na rysunku 9 przedstawiono wyniki symulacji ataku Stanów Zjednoczonych impulsem NEMP, zaczerpnięte z raportu Grahama. Na mapie widać zasięg zniszczeń i energię impulsu (w przybliżeniu proporcjonalną do stopnia zniszczenia infrastruktury). W odróżnieniu od Stanów Zjednoczonych, wyniki podobnych symulacji dotyczących Polski nie są publicznie dostępne (jeżeli istnieją) i stopień zagrożenia telekomunikacyjnej infrastruktury Polski nie jest powszechnie znany. Dlatego, dla celów orientacyjnych, autor nałożył mapę konturową Polski na mapę Stanów Zjednoczonych (w odpowiedniej skali). Widać, że pojedynczy impuls może spowodować poważne szkody na terenie całego naszego kraju (przy założeniu identycznych warunków propagacji impulsu w obu krajach).

Atak elektromagnetyczny tego rodzaju niszczy w pierwszym rzędzie elementy infrastruktury państwa wrażliwe na narażenia w sieciach teleinformatycznych i energetycznych. Wzajemne powiązania powodują, że dysfunkcja jednego elementu może prowadzić do uszkodzenia kolejnych, aż do ogólnej katastrofy (efekt domina). Zasoby te obejmują m.in. systemy i sieci użytkowane przez administrację rządową, organy władzy ustawodawczej, władzy sądowniczej, samorządu terytorialnego, a także, strategiczne z punktu widzenia bezpieczeństwa państwa, podmioty gospodarcze działające w obszarze telekomunikacji, energii, gazu, bankowości, ochrony zdrowia i inne (por. rys. 1).

Ochrona przed narażeniami elektromagnetycznymi

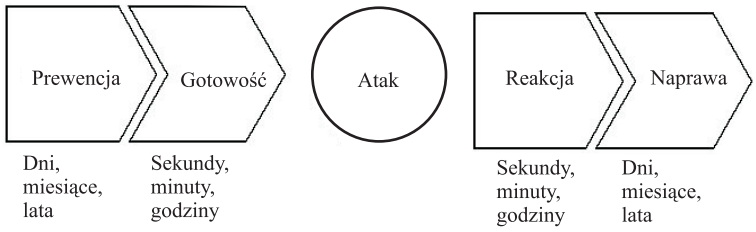
Ochrona przed narażeniami elektromagnetycznymi to problem holistyczny, w którym przeplatają się elementy techniczne, organizacyjne, ekonomiczne i socjalne (rysunek 10).

Rys. 10. Trzy obszary ochrony przed atakiem elektromagnetycznym: informacyjny, fizyczny i behawioralny ①

Ochrona infrastruktury przed atakiem niszczącym polega na takim dopasowaniu struktur organizacyjnych, parametrów technicznych (odporności) urządzeń i systemów, aby zapewnić „przeżywalność" infrastruktury z określonym prawdopodobieństwem i jej powrót do stanu normalnego w określonym czasie (proces naprawy wymaga czasu i nie może być szybszy niż jego najwolniejsze ogniwo). Wiąże się to z wysokimi kosztami.

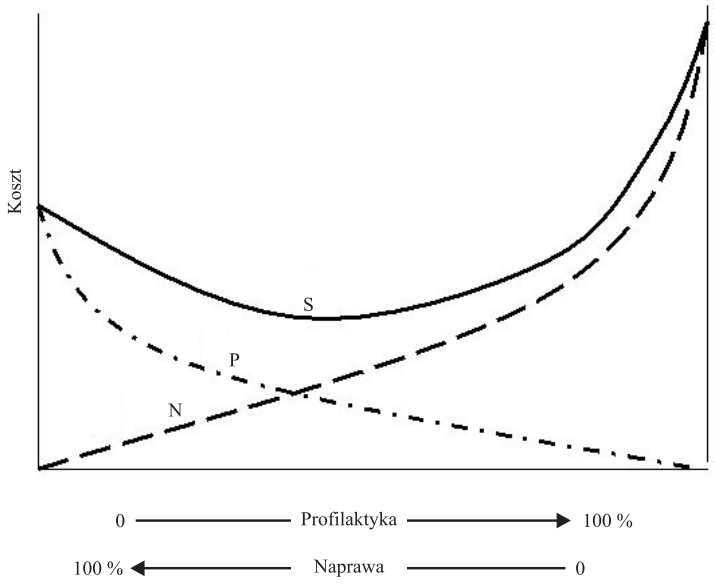
Proces obejmuje różne fazy: prewencję (uodpornienie), przygotowania na wypadek ataku, protekcję w czasie ataku, oraz ratunek i naprawę szkód po ataku, jak pokazano na rysunku 11.

① *Rysunek inspirowany [37]*



Rys. 11. Ochrona przed atakiem elektromagnetycznym obejmuje różne fazy

W ramach działalności profilaktycznej odporność urządzeń, systemów, instalacji, budynków itd. na narażenia elektromagnetyczne musi być kontrolowana i poprawiana tam gdzie potrzeba. Słabe elementy muszą być uodpornione albo zamieniona na nowe, bardziej odporne. Zaistniałe szkody muszą być po ataku naprawione. Może to być bardzo kosztowne i mimo to nie gwarantować pełnej, 100% ochrony. Przy ograniczonym budżecie powstaje pytanie: czy wydać więcej na działania prewencyjne czy na naprawy? Intuicja podpowiada, że istnieje optymalna kombinacja obu tych działań, która zapewnia określony stopień ochrony przy minimum kosztów (rys. 12). Z drugiej strony nie należy zapominać, że wydatki na ochronę infrastruktury stwarzają zapotrzebowanie na nowe usługi, urządzenia, instalacje i budynki, oraz na prace adaptacyjne i badawcze.



Rys. 12. Suma (S) kosztów działań profilaktycznych (P) i naprawczych (N) osiąga minimum przy określonej ich kombinacji

Ochrona przed narażeniami przypadkowymi

Systematyczne prace nad ochroną cywilnej przestrzeni informatycznej przed przypadkowymi narażeniami elektromagnetycznymi (nie używano wówczas tej nazwy) rozpoczęto w Polsce w 1956 r. pod kierunkiem autora w Instytucie Łączności we Wrocławiu z inicjatywy prof. Wilhelma Rotkiewicza [26]. Była to pierwsza, i przez długi czas jedyna, w Polsce placówka naukowo-badawcza, wyspecjalizowana w problemach narażeń elektromagnetycznych i odporności na nie. Prowadzone w niej prace stanowi-

ły podstawy naukowo-techniczne aktów prawnych i przepisów regulacyjnych oraz uzasadnienie merytoryczne stanowiska Polski w negocjacjach międzynarodowych. Oddział Instytutu Łączności we Wrocławiu stał się ośrodkiem wiodącym. Niewątpliwie przyczyniło się do tego Międzynarodowe Wrocławskie Sympozjum Kompatybilności Elektromagnetycznej, organizowane wspólnie z Politechniką Wrocławska i Stowarzyszeniem Elektryków Polskich.①

Prace Instytutu Łączności i jednostek współpracujących, które później powstały, doprowadziły do ustanowienia w Polsce systemu ochrony, opartego na przepisach prawnych i normach państwowych oraz do stworzenia struktury organizacyjnej zapewniającej ich przestrzeganie. Normy Polskie zgłoszone przez Instytut i ustanowione przez Polski Komitet Normalizacyjny określają [19]:

- wymagania techniczne stawiane urządzeniom w zakresie dopuszczalnych emisji energii elektromagnetycznej,
- wymagania stawiane urządzeniom w zakresie odporności na niezamierzone narażenia elektromagnetyczne,
- wymagania stawiane specjalistycznej aparaturze kontrolno-pomiarowej,
- standardowe warunki i metody kontroli urządzeń na zgodność z ww. wymaganiami dotyczącymi emisyjności i odporności,
- standardowe warunki i metody badania skuteczności podzespołów stosowanych do zmniejszania emisyjności i wrażliwości na niezamierzone oddziaływania elektromagnetyczne.

W świetle wzrastającej liczby urządzeń i powiększającego się poziomu środowiskowych szumów, prace nad przypadkowymi narażeniami powinny być kontynuowane, a istniejące przepisy i normy powinny być „dopasowywane" do zmieniającego się ciągle środowiska elektromagnetycznego.

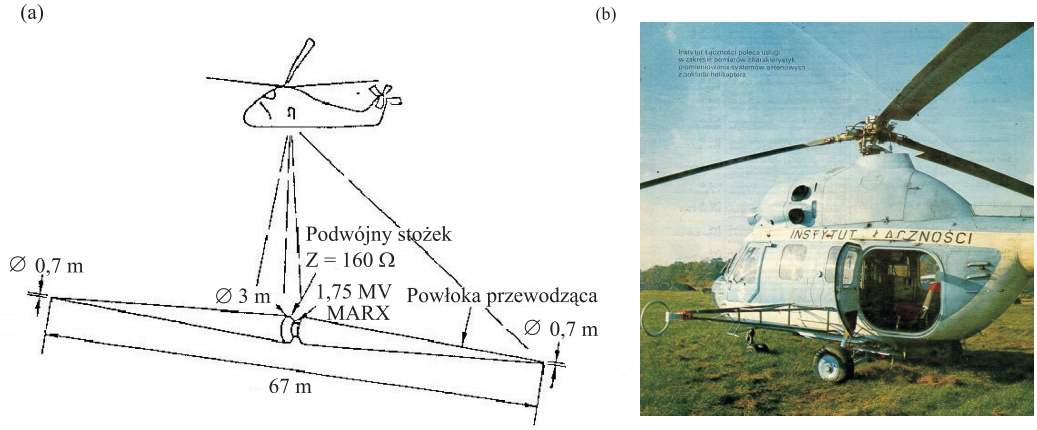
Odporność na atak

Podstawowym elementem jest tu identyfikacja słabych punktów systemu, które wymagają wzmocnienia. Prace takie w odniesieniu do infrastruktury cywilnej nie były w kraju prowadzone systematycznie i Polska jest opóźniona w stosunku do innych krajów, takich jak np. Szwecja, w których badania takie prowadzi się od szeregu lat [16], [17], [18], [36]. Jak wspomniano wcześniej, prace krajowe dotyczyły narażeń niezamierzonych, tj. o stosunkowo małej energii. Chociaż techniki dużych energii i małych energii są podobne jeśli chodzi o podstawowe procesy fizyczne, wyposażenie i utrzymanie laboratoriów narażeń elektromagnetycznych o dużej energii jest kosztowne z uwagi na unikatowy charakter aparatury pomiarowej. W latach siedemdziesiątych w Zakładzie Kompatybilności Elektromagnetycznej Instytutu Łączności we Wrocławiu, pod kierunkiem autora zostało utworzone wielozadaniowe laboratorium kontrolno-pomiarowe na śmigłowcu [27]. Było ono wykorzystywane do różnych celów; przewidywano rozszerzenie jego prac na aspekty ochrony cywilnych sieci teleinformatycznych.

Między innymi, planowano wykorzystać je do zbudowania mobilnego generatora silnych narażeń elektromagnetycznych, podobnego do opracowanego wcześniej w Stanach Zjednoczonych. Miałoby ono za zadanie pomiar odporności różnych sieci i obiektów w miejscu ich użytkowania i w normalnych warunkach pracy. Na rysunku 13 przedstawiono szkic śmigłowca amerykańskiego oraz fotografię śmigłowca Instytutu Łączności. Konstrukcja podwieszona pod śmigłowcem (rys. 14 a) to kompletny generator impulsu elektromagnetycznego o dużej energii. Wytworzony ponad badanym obiektem impuls naśladowałby rzeczywisty atak elektromagnetyczny impulsem HEMP.

① *Jest to najstarsze regularne sympozjum EMC w Europie, organizowane co dwa lata, począwszy od 1972 r. aż do roku 2010, w którym to roku zmieniło ono nazwę z "Wrocławskiego" na "Europejskie".*

Po prywatyzacji sektora telekomunikacyjnego w Polsce, plany podjęcia badań nad zwiększeniem odporności cywilnych instalacji teleinformatycznych na atak elektromagnetyczny zostały zawieszone. Nie zostały one podjęte dotychczas z uwagi na brak zainteresowania zarówno sektora prywatnego, jak i jednostek rządowych i samorządowych. Latające Laboratorium Instytutu Łączności zostało zlikwidowane z uwagi na brak źródeł finansowania i wysokie koszty amortyzacji.



Rys. 14. Mobilny generator impulsu elektromagnetycznego o dużej energii: a) szkic generatora amerykańskiego, (b) śmigłowiec Instytutu Łączności przewidywany do przenoszenia takiego generatora. Element z lewej strony kadłuba to generator narażeń o niewielkiej energii [5], [27]

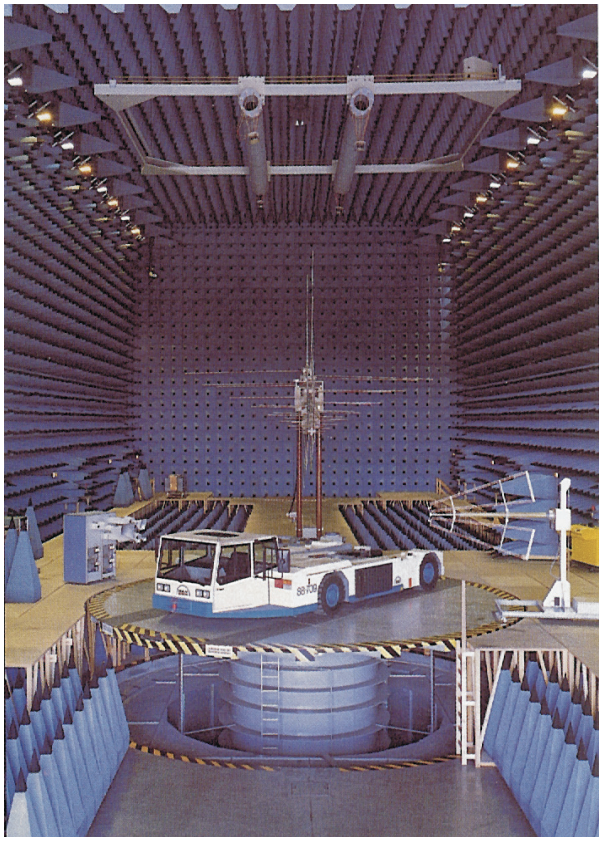
Rysunek 15 przedstawia widok jednego z amerykańskich stanowisk pomiarowych do oceny odporności stacji bazowych telefonii komórkowej na narażenia elektromagnetyczne, a rys. 16 widok stanowiska pomiarowego do badania odporności aparatury elektronicznej w samolocie na narażenia elektromagnetyczne[①]. Przedmiot widoczny nad samolotem wraz z siecią drutów, to generator impulsów EMP. Źródła energii, aparatura pomiarowa i kontrolna nie są pokazane.

Rys. 15. Stanowisko pomiarowe w terenie do badania odporności kontenerowych stacji bazowych telefonii komórkowej na narażenia elektromagnetyczne o dużej energii [8]

Rys. 16. Stanowisko pomiarowe do badania odporności aparatury elektronicznej zainstalowanej w samolocie na narażenia elektromagnetyczne o dużej energii typu EMP. Generator narażeń jest widoczny nad samolotem.[①]

① *Źródło: http://en.wikipedia.org/wiki/Electromagnetic_pulse (4.10.2009)*

Rysunek 17 przedstawia widok stanowiska pomiarowego w bezechowej hali ekranowanej do badania odporności dużych urządzeń na narażenia elektromagnetyczne o dużej energii.



Rys. 17. Stanowisko pomiarowe w bezechowej hali ekranowanej do badania odporności dużych urządzeń na narażenia elektromagnetyczne o dużej energii.[1]

Badania odporności na narażenia elektromagnetyczne prowadzone w Instytucie Łączności i innych laboratoriach w kraju są ograniczone do obiektów stosunkowo niewielkich rozmiarów i nie obejmują badań niszczących, które wymagają dużych energii. Polskie Normy dotyczące kompatybilności elektromagnetycznej (po kolejnych aktualizacjach), zgodne z Dyrektywami Europejskimi i standardami międzynarodowymi, nie uwzględniają możliwości ataku elektromagnetycznego. Podane w nich poziomy dopuszczalne narażeń elektromagnetycznych (i wrażliwości) dotyczą standardowych (tj. przeciętnych) warunków eksploatacji. Ustalone one zostały w konsultacji ze wszystkimi zainteresowanymi, na podstawie przeprowadzonych badań i danych zebranych w przeszłości, biorąc pod uwagę zarówno aspekty kompatybilności elektromagnetycznej, jak i aspekty ekonomiczne. Należy w tym miejscu dodać, że normy i przepisy legislacyjne reagują z opóźnieniem na nowe technologie i nowe zagrożenia. Tymczasem środowisko elektromagnetyczne zmienia się ciągle, w rezultacie wzrostu liczby urządzeń i systemów generujących energię elektromagnetyczną i wrażliwych na nią, co już wcześniej podkreślano.

[1] *Źródło: materiały firmowe, Rohde & Schwartz*

Zalecenia Komisji Grahama

Pilne zalecenie Komisji Grahama dotyczy zwiększenia niezawodności systemów i sieci teleinformatycznych w służbach awaryjnych, takich jak pogotowie medyczne straż pożarna, służby porządkowe itd. Systemy zarządzania, kontroli, komunikacji i informacji (C3I – *Command, Control, Communications, and Information*) mają w sytuacjach kryzysowych podstawowe znaczenie dla koordynacji, gotowości i efektywności działań. Niestety, są one szczególnie wrażliwe na atak; a wiele z nich stosuje przestarzałe mechanizmy bezpieczeństwa i niezawodności. Według Komisji, organizacje powołane do rozwiązywania sytuacji kryzysowych nie dysponują wiedzą dotyczącą najnowszych technologii telekomunikacyjnych i komputerowych i dlatego należy pomóc im w tym zakresie. W przeciwieństwie do niektórych działów gospodarki o znaczeniu ogólnonarodowym, w sektorze teleinformatyki rząd ma niewielkie pole do wprowadzania innowacji. Dlatego ważne jest zaangażowanie sektora prywatnego i wykorzystanie mechanizmów rynkowych. Prawdziwym wyzwaniem dla polityków jest zachęcenie sektora prywatnego do większego zainteresowania sprawami bezpieczeństwa sieci i odporności na atak elektromagnetyczny.

Komisja stwierdziła, że obecne (2008 r.) modele matematyczne niezbędne do oszacowania szkód w razie ataku elektromagnetycznego mają istotne ograniczenia i nie pozwalają na adekwatną ocenę skutków jednoczesnego uszkodzenia wielu powiązanych ze sobą dynamicznie elementów infrastruktury:

„*Komisja zaleca prowadzenie badań w celu lepszego zrozumienia wzajemnych zależności różnych systemów infrastruktury i rożnych scenariuszy ataku elektromagnetycznego. W szczególności Komisja zaleca badania i modelowanie współzależności. Ich finansowanie może być z wielu źródeł, w tym z National Science Foundation i Department of Homeland Security. Komisja uważa za właściwe obecne prace nakierowane na ochronę systemów SCADA przed cyberatakiem. Komisja zaleca, aby prace te rozszerzyć na rozwiązanie problemu wrażliwości tych systemów na inne formy ataku elektronicznego, jak np. impuls elektromagnetyczny EMP* [8]."

Dalej, Komisja zaleca rządowi federalnemu prowadzenie multidyscyplinarnych badań naukowych zorientowanych problemowo i mających na uwadze potrzeby zarówno użytkowników cywilnych, jak i wojskowych. Badania powinny wykraczać poza znane rozwiązania i prowadzić do innowacyjnych rozwiązań, które nie wynikają w sposób oczywisty z technologii teleinformatycznych dnia dzisiejszego. Raport zaleca w szczególności następujące kroki [8]:

- Systematycznie zbierać, analizować i rozpowszechniać istotne informacje na temat zagrożeń elektromagnetycznych i cyberataków;
- Przeprowadzać testy w celu zidentyfikowania słabych ogniw w istniejących instalacjach i systemach;
- Zapewnić sprawne funkcjonowanie infrastruktur łącznie sektora prywatnego, rządowego i samorządowego, zwłaszcza w sytuacjach krytycznych (krok wymagający ścisłej współpracy wszystkich sektorów);
- Uwzględniać wymagania dotyczące zabezpieczenia przed narażeniami elektromagnetycznymi i cyberatakami w specyfikacji i wymaganiach stawianych nowym sieciom/systemom;
- Monitorować na bieżąco technologie ataku elektromagnetycznego i cyberataku oraz przeciwdziałań zabezpieczających, rozumieć je i oceniać stopień zagrożenia; monitorować wczesne symptomy zagrożeń;
- Prowadzić badania w celu udoskonalenia środków/systemów obrony;

- Promować popularyzację problemów ochrony przed cyberatakiem i atakiem elektromagnetycznym;
- Ustanowić i wdrożyć do praktyki standardy techniczne i operacyjne w zakresie ochrony przed cyberatakiem i atakiem elektromagnetycznym;
- Ustanowić i wdrożyć kryteria oceny stopnia zagrożenia i stopnia odporności na atak.

Zdaniem autora, zalecenia te powinny być wdrożone także w Polsce.

Trudności

Organizacje zaatakowane (lub poszkodowane w wyniku niezamierzonych oddziaływań), nie są zainteresowane dzieleniem się swoimi doświadczeniami. Przeciwnie, wolą ukrywać fakt ataku i jego efekty zasłaniając się prawem (*Trade Secret*). Dzieje się tak, ponieważ upublicznienie takich (niekorzystnych) informacji może podkopać reputację firmy, zaufanie publiczne, oraz zaszkodzić w karierze dyrektorów. Z tego też powodu pracownicy i eksperci zewnętrzni są zazwyczaj związani tajemnicą służbową, co prowadzi często do absurdalnych sytuacji. Na przykład, po każdym napadzie na bank z bronią w ręku ukazują się szczegółowe opisy tego wydarzenia w prasie, radiu i telewizji. Tymczasem bardzo rzadko publikowane są informacje o kradzieży banku dokonanej na drodze elektronicznej, jeżeli w ogóle są takie informacje publikowane. Stan taki utrudnia wymianę doświadczeń, systematyczne gromadzenie i analizę faktów oraz identyfikację słabych punktów systemu w celu ich wyeliminowania.

System zabezpieczony przed atakiem oferuje użytkownikowi takie same podstawowe funkcje jak system niezabezpieczony, ale jest z reguły droższy. Z tego powodu sektor prywatny poświęca minimum środków na bezpieczeństwo, tyle tylko ile można uzasadnić argumentami biznesowymi. Zwykle jest to znacznie mniej niż wynika to z odczucia społecznego. To samo dotyczy agencji rządowych i samorządowych, które pracują w warunkach ograniczonego budżetu. Sprawy bezpieczeństwa są chronicznie niedoinwestowane.

„*Ze względów ekonomicznych, systemy są zwykle budowane przy użyciu powszechnie dostępnych podzespołów. Takie podzespoły nie są bardzo bezpieczne. Nie ma też zapotrzebowania na wykonania bardziej bezpieczne. Nabywcy kupują raczej funkcjonalność i wydajność niż bezpieczeństwo. Fiasko programu rządowego <Orange Book> jest tu dobrym przykładem. Rząd zażądał bezpiecznych systemów, przemysł opracował i wyprodukował takie systemy, a wtedy agencje rządowe odmówiły zakupienia ich, ponieważ okazały się one wolniejsze i mniej funkcjonalne niż inne niezabezpieczone systemy dostępne na wolnym rynku* [20]*”.*

Program rządowy

W Polsce nie ma cywilnego laboratorium, które byłoby w stanie ocenić stopień odporności istniejących urządzeń, instalacji i sieci na atak elektromagnetyczny o dużej energii na podstawie pomiarów lub symulacji. Brak również ogólnie dostępnych zweryfikowanych modeli symulacyjnych. Wszystkie kraje Unii Europejskiej planują upowszechnienie usług internetowych (*e-usług*), publicznych i komercyjnych. Wobec dużej wrażliwości tych usług na zakłócenia, Rada Europy przyjęła w 2003 r. Europejską Strategię Bezpieczeństwa i program „Zapobieganie, gotowość i zarządzanie skutkami aktów terroryzmu” w ramach ogólnego programu „Bezpieczeństwo i ochrona wolności” na lata 2007–2013.
W skali ogólnoświatowej, szereg organizacji prowadzi prace zmierzające do ograniczenia takich ataków, m.in. Międzynarodowy Związek Telekomunikacyjny ITU [12], Międzynarodowa Unia Nauk Radiowych URSI [35], Międzynarodowa Komisja Elektrotechniczna IEC [6], [34].

Zamierzenia Polski w zakresie upowszechnienia e-usług przedstawione w dokumencie rządowym „Strategia Rozwoju Społeczeństwa Informacyjnego w Polsce do roku 2013" są imponujące [24]. Podobnie jak plany europejskie wymagają odpowiednich działań wspomagających w zakresie ochrony infrastruktury. Takie działania zawierają Założenia do rządowego „Programu ochrony cyberprzestrzeni RP na lata 2009–2011" [40]. Przez „cyberprzestrzeń" rozumie się ogólnie media cyfrowe wszelkiego rodzaju od telefonii komórkowej do usług internetowych. Dokument rządowy zawiera założenia do działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym. Ich głównym celem jest zwiększenie zdolności do zapobiegania i zwalczania cyberterroryzmu oraz innych zagrożeń dla bezpieczeństwa państwa, pochodzących z publicznych sieci teleinformatycznych①. Przewiduje w przyszłości utworzenie kompleksowego narodowego programu ochrony infrastruktury krytycznej. Działania wyszczególnione w programie obejmują osiem elementów:

- rozbudowę zespołu reagowania na incydenty komputerowe,
- rozbudowę systemu wczesnego ostrzegania przez atakami sieciowymi,
- wdrażanie dodatkowych rozwiązań prewencyjnych,
- zarządzanie ćwiczeń obejmujących badanie odporności krytycznej infrastruktury teleinformatycznej na kontrolowane cyberataki,
- szczególną ochronę kluczowych systemów informatycznych,
- wdrażanie rozwiązań zapasowych, które mogą przejąć realizację procesu w sytuacji uszkodzenia, zniszczenia lub niedostępności systemów i sieci zaliczonych do krytycznej infrastruktury teleinformatycznej,
- rozwój witryny www.cert.gov.pl jako podstawowego źródła informacji o metodach przeciwdziałania, podatnościach i atakach z cyberprzestrzeni,
- konsolidację dostępu do usług publicznych.

Miarą ich skuteczności będzie ocena stworzonych regulacji, instytucji i relacji.

Program rządowy koncentruje się na ochronie przed wrogą modyfikacją programów komputerowych i baz danych („miękkiej" infrastruktury). Łatwo zauważyć, że założenia rządowe nie wspominają o narażeniach elektromagnetycznych. Nie ma tam przedsięwzięć zmierzających do oceny stopnia wrażliwości fizycznej („twardej") infrastruktury państwa na możliwy elektromagnetyczny atak terrorystyczny. Nie ma w nim informacji o inwestycjach niezbędnych do uodpornienia infrastruktury teleinformatycznej na takie narażenia i na prace badawczo-projektowe wymagane do właściwego przygotowania takich inwestycji. Takie przygotowanie powinno obejmować rozpoznanie istniejącego stanu, identyfikację elementów wymagających poprawy, propozycje poprawy z uzasadnieniem sugerowanego rozwiązania. Nie jest określona w programie rola państwowych placówek badawczych w tym zakresie. Placówki te zostały powołane do wspierania decyzji administracji państwowej i samorządowej niezbędnymi analizami i badaniami i do rozwiązywania problemów ważnych dla państwa.

Założenia do programu rządowego ograniczają się do ochrony przed atakiem w cyberprzestrzeni. W artykule przedstawiono, że atak elektromagnetyczny oraz niezamierzone zakłócenia elektromagnetyczne, mogą powodować równie poważne, albo nawet większe, szkody. Wydaje się więc, że program rządowy powinien być rozszerzony na ochronę przed narażeniami elektromagnetycznymi.

① *Ang.: Information security, cyber security: The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. ATIS Telecom Glossary 2007*

Zakończenie

W artykule omówiono wybrane problemy oddziaływań elektromagnetycznych, celowych i niezamierzonych, w aspekcie programów rozwoju społeczeństwa informacyjnego. Założenia programu rządowego dotyczące ochrony cyberprzestrzeni kraju koncentrują się na ataku w przestrzeni wirtualnej (cyberataku). Problemy ochrony infrastruktury przed narażeniami elektromagnetycznymi są w tych założeniach pominięte. W opracowaniu wykazano, że atak elektromagnetyczny stanowi rzeczywiste zagrożenie, takie jak cyberatak, albo większe.

Istnieje potrzeba strategicznych decyzji w sprawie ochrony infrastruktury kraju przed atakiem elektromagnetycznym i przed przypadkowymi oddziaływaniami elektromagnetycznymi. Decyzje te mogą wiązać się ze znacznymi nakładami finansowymi i mieć duże znaczenie dla gospodarki kraju. Wobec chronicznego niedostatku środków finansowych, wydaje się niezbędna publiczna debata w tej sprawie. Taka debata jest potrzebna dla zapewnienia społecznego zrozumienia i poparcia dla podejmowanych decyzji. Z uwagi na możliwe konflikty różnych grup interesów, powinni w tej debacie uczestniczyć wszyscy zainteresowani: użytkownicy, właściciele i operatorzy sieci teleinformatycznych, naukowcy i praktycy, producenci, wykonawcy i dostawcy urządzeń i instalacji, ekonomiści, finansiści oraz ludzie polityki. Przykłady ważnych pytań, na które należy odpowiedzieć w tej dyskusji są następujące:

- Jak należy traktować w Polsce problem ochrony infrastruktury teleinformatycznej przed narażeniami i terroryzmem elektromagnetycznym?
- Jakie miejsce powinien ten problem zająć na liście priorytetów rządowych?
- Jakie niezbędne przedsięwzięcia należy podjąć i w jakiej kolejności?
- Jaka powinna być rola sektora państwowego, sektora prywatnego, kapitału obcego?
- Jak należy ustawić współpracę z zagranicą z sąsiednimi krajami i z organizacjami międzynarodowymi, w tym europejskimi?
- Jaka powinna być rola rządu, i państwowych instytutów badawczych (w tym Instytutu Łączności) oraz wyższych uczelni?
- Jaki jest koszt i źródła finansowania niezbędnej działalności w tej dziedzinie?

Autor ma nadzieję, że niniejsze opracowanie stanowi wystarczające wprowadzenie do takiej dyskusji.

Bibliografia

[1] *ATIS Telecom Glossary 2007*, American National Standard; The Alliance for Telecommunications Industry Solutions; http://www.atis.org/glossary/foreword.aspx

[2] Bäckström M.: *The Threat From Intentional EMI Against the Civil Technical Infrastructure*; Reprint from ESW2006, 3rd European Survivability Workshop, Toulouse, France, 16 – 19 May 2006

[3] Bobiński E., Żelaziński J.: *Ocena przyczyn lipcowej powodzi. Wnioski do programu ochrony przeciwpowodziowej w przyszłości na Odrze*. Ekspertyza opracowana dla Sejmowej Komisji Ochrony Środowiska, Zasobów Naturalnych i Leśnictwa, 15.09.1997 http://www.odra.pl/pl/dokumenty/962585850.shtml

[4] Denning D.: *Information Warfare and Security.* Addison-Wesley, ACM Press Books, 1999

[5] Degauque P., Hamelin J.: *Electromagnetic Compatibility*. Oxford University Press, 1993, p. 652

[6] *Electromagnetic compatibility (EMC),* Part 2: Environment, Section 9: Description of HEMP environment – Radiated disturbance. Basic EMC publication, IEC 61000-2-9; http://www.iec.ch/cgi-bin/procgi.pl/www/iecwww.p?wwwlang=E&wwwprog=cat-det.p&wartnum=020728

[7] Fitzek F.H.P., Katz M.D.: *Cognitive Wireless Networks.* Springer, 2007

[8] Graham R. et all: *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack.* Executive summary. http://www.empcommission.org/docs/empc_exec_rpt.pdf; Critical National Infrastructures, April 2008, http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf

[9] Ianoz M., Wipf H.: *Modeling and Simulation Methods to Assess EM Terrorism Effects*. Proceedings of 13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility, 1999

[10] *IET Electromagnetic Compatibility for Functional Safety*. IET, 2008. www.theiet.org

[11] *ITU Internet Reports: The Internet of Things*. Geneva, November 2005

[12] ITU-T, Telecommunication Standardization Sector of ITU, Series K.78. *Protection Against Interference.* HEMP Immunity Guide For Telecommunication Centres (Approved 06-2009)

[13] Kohns N.: *Ground-Based Air-Conditioning System Interfered Aircraft Communication Channel*. IEEE EMCS Newsletter, Issue 215, Fall 2007, pp. 90-94

[14] Leach R. D., Alexander M. B.: *Electronic Systems Failures and Anomalies Attributed to Electromagnetic Interference*. NASA Reference Publication 1374, July 1995

[15] Leese R., Hurley S. (eds.): *Methods and Algorithms for Radio Channel Assignment*. Oxford University Press, 2002, pp. 7 -21;

[16] Månsson D., Thottappillil R. and Bäckström M.; *Propagation of UWB Transients in Low-Voltage Power Installation Networks*. IEEE Transactions on Electromagnetic Compatibility, vol. 50, no. 3, August 2008, pp. 619-629

[17] Månsson D., Thottappillil R., Nilsson T., Lundén O., Bäckström M.: *Susceptibility of Civilian GPS Receivers to Electromagnetic Radiation*. IEEE Transactions on Electromagnetic Compatibility, vol. 50, no. 2, May 2008, pp. 434-437

[18] Månsson D., Thottappillil R., Bäckström M., Lundén O.: *Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI*. IEEE Transactions on Electromagnetic Compatibility, vol. 50, no. 1, Feb. 2008, pp. 101-109

[19] Moroń W.: *Kompatybilność elektromagnetyczna. Co to jest i dlaczego jest ona ważna?* Normalizacja nr 7, 2003, s. 23-29. Cz 2. Działalność normalizacyjna. Normalizacja nr 8, 2003, s. 12-18

[20] *National Research Council: Cybersecurity Today and Tomorrow*. 2002

[21] *National Research Council: Making the Nation Safer: The Role and Technology in Countering Terrorism*. 2002

[22] Radasky W.A.: *2007 Update on Intentional Electromagnetic Interference (IEMI) and High-altitude Electromagnetic Pulse (HEMP).* ITEM – Interference Technology an online Guide to Electromagnetic Compatibility, http://www.interferencetechnology.com/articles/articles/article/2007-update-on-intentional-electromagnetic-interference-iemi-and-high-altitude-electromagnetic-pul.html

[23] Rotkiewicz W. (ed.): *Electromagnetic Compatibility in Radio Engineering*; Elsevier 1982, pp. 3-56

[24] *Strategia Rozwoju Społeczeństwa Informacyjnego w Polsce do roku 2013.* Projekt, wersja 3.00, 2008, http://www.mswia.gov.pl/strategia/

[25] Strużak R.: *On spectrum congestion and capacity of radio links*. Annales of Operational Research, no 107, 2001, pp. 339-347

[26] Strużak R. i inni: *Pół wieku innowacji – Prace Oddziału Instytutu Łączności we Wrocławiu*. Telekomunikacja i Techniki Informacyjne, nr 3-4, 2009, s. 68-82

[27] Strużak R.: *Terrestrial electromagnetic environment*. In: Electromagnetic Compatibility in Radio Engineering; (ed. W. Rotkiewicz), Elsevier, 1982, pp. 3-56

[28] Strużak R., Żernicki E.: *Latające Laboratorium Instytutu Łączności*. Przegląd Telekomunikacyjny, 1981, nr. 9/10, s. 258-282

[29] Strużak R.: *Emergency telecommunications with and in the field*: *evaluation report*. United Nations, New York and Geneva, July 2000, http://www.reliefweb.int/telecoms/evalu/evaluation.html

[30] Strużak R.: *Improved utilization of the radio spectrum respecting physical laws.* In: Proceedings of the URSI General Assembly, Chicago, Illinois, USA, 9-16 August 2008

[31] Strużak R.: *Introduction to International Radio Regulations.* In: International Centre for Theoretical Physics, (Ed: Radicella S.), 2003, http://publications.ictp.it/lns/vol16.html

[32] Strużak R.: *Trends in use of RF spectrum.* Journal of Telecommunications and Information Technology, no. 4/2009, pp. 1-6

[33] Tesche F. M.: *Modeling techniques for EMC analysis.* In: Review of Radio Science 1966–1999, (ed. Stone R.), pp. 365-370

[34] Wik M. W., Radasky W.A.: *Intentional electromagnetic interference (IEMI): background and status of the standardization work in the International Electrotechnical Commission (IEC)*. The Radio Science Bulletin, no 299, Dec. 2001, pp. 13-18

[35] Wik M. W.: *Revolution in Information Affairs*: *Global Communications Americas 2000*, Hanson Cooke Ltd, 2000

[36] Wik M. W.: *URSI statement - Nuclear electromagnetic pulse [EMP] and associated effects.* Antennas and Propagation Society Newsletter, IEEE, vol. 29/3, Jun 1987, pp 19- 23

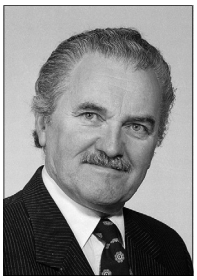
[37] Wik M. W.: *What is Network-Based Defence (NBD) and the Impact on the Future Defence?* Royal Swedish Academy of War Sciences, October 2003

[38] Wik M.W: *Global Information Infrastructure: Threats; Global Communications Interactive*. Hanson Cooke limited, 1997, www.intercomms.net/content/threats.php)

[39] Yamamoto K., Yamada K., Yonemoto N.: *PED Interference Reporting System in Japan*. In: Electromagnetic Compatibility and Electromagnetic Ecology, 2007 7th International Symposium on, Saint-Petersburg, 26-29 June 2007, pp. 220-223

[40] *Założenia do rządowego programu ochrony cyberprzestrzeni RP na lata 2009-2011.* 2009, http://www.mswia.gov.pl/portal/pl/2/6966/

Ryszard Strużak



Profesor dr hab. inż. Ryszard Strużak (1933) – absolwent Politechniki Wrocławskiej (1956), doktorat (1962); habilitacja (1968) na Politechnice Warszawskiej; tytuły profesora nadzwyczajnego (1975) i zwyczajnego (1988); nauczyciel akademicki Politechniki Wrocławskiej (1954–1961, 1964–1985 i od 2007) oraz Wyższej Szkoły Informatyki i Zarządzania w Rzeszowie (2004/2005); pracownik naukowy/kierownik Oddziału Instytutu Łączności we Wrocławiu (1956–1961, 1964–1985, od 2005); współorganizator/ przewodniczący Międzynarodowego Wrocławskiego Sympozjum EMC (od 1972); przewodniczący Podkomitetu EMC KEiT PAN (1975–1985); autor/współautor 10 patentów oraz ponad 200 publikacji; trzykrotny laureat nagród ministerialnych (1974, 1979 i 1983), sześciokrotny laureat konkursów PTETIS O. Wrocław; odznaczony m.in. Złotą Odznaką Zasłużony Pracownik Łączności (1973), Złotą Odznaką Honorową SEP (1981), Krzyżem Kawalerskim Orderu Odrodzenia Polski (1982); członek międzynarodowych organizacji CISPR, ITU-CCIR, URSI, ICTP, CEI, Senior Counselor, Head of Technical Dept. & Acting Assistant Director, ITU/CCIR (1985–1993), Member/V-Chair ITU Radio Regulations Board (1994–2002), Consultant UN-OCHA, World Bank (1993–2004); Editor-in-Chief „Global Communications" (1996–2000); dwukrotny laureat konkursów międzynarodowych (Montreux 1975, Rotterdam 1977); uhonorowany m.in. Srebrnym Medalem ITU za szczególne zasługi dla rozwoju telekomunikacji na świecie (1998) oraz tytułem IEEE Fellow (1985) i Life Fellow (2007) za wybitne osiągnięcia zawodowe; Member New York Academy of Sciences (1993); Academician, International Telecommunication Academy (1997); zainteresowania zawodowe: nauki radiowe, radiokomunikacja, kompatybilność elektromagnetyczna.

e-mail: r.struzak@ieee.org

Ochrona środowiska przed elektromagnetycznym promieniowaniem niejonizującym

Marta Macher,
Marek Kałuski, Karolina Skrzypek

Opisano oddziaływanie pola elektromagnetycznego pochodzącego z różnych źródeł na organizm człowieka i skalę zagrożeń dla zdrowia. Przeanalizowano zasady określania wartości dopuszczalnych pola w Polsce i na świecie dla ogółu społeczeństwa i osób pracujących w otoczeniu źródeł pola. Przedstawiono działalność Instytutu Łączności w dziedzinie kompatybilności elektromagnetycznej i pomiarów pola dla celów BHP i ochrony środowiska.

źródła pola elektromagnetycznego, wpływ elektromagnetycznego promieniowania niejonizującego na człowieka, dopuszczalne poziomy pól elektromagnetycznych w Polsce i na świecie

Wprowadzenie

Stale wzrasta liczba i różnorodność źródeł pól elektromagnetycznych w większości wytwarzanych przez systemy radiokomunikacyjne. Powoduje to wzrost zagrożeń, o których istocie brak niejednokrotnie rzetelnej informacji, co sprzyja powstawaniu mitów i przesądów.

Celem niniejszego artykułu jest przedstawienie głównych zagadnień z dziedziny ochrony środowiska przed elektromagnetycznym promieniowaniem niejonizującym, z konieczności tylko w ogólnym zarysie.

Pole elektromagnetyczne

Naturalne procesy elektromagnetyczne rozwijały się we wszechświecie od początku jego istnienia i stanowią zasadniczy składnik środowiska Ziemi. Człowiek stosunkowo niedawno wprowadził do tego środowiska urządzenia emitujące energię elektromagnetyczną w szerokim zakresie częstotliwości. Ostatnie lata związane są z dużym wzrostem liczby i mocy źródeł wytwarzających pola elektromagnetyczne, EM. Naturalne środowisko Ziemi zostało zakłócone przez pole EM, którego źródłem są, przede wszystkim, urządzenia energetyczne, stacje radiowe i telewizyjne, łączność satelitarna, stacje radiolokacyjne, radionawigacyjne, radiokomunikacji ruchomej lądowej, w tym telefonii komórkowej.

Środowisko odbiera naturalne i sztuczne oddziaływania pola magnetycznego. Składnikami pola naturalnego są: stałe pole magnetyczne odpowiadające w naszej szerokości geograficznej natężeniu 40 A/m, stałe pole elektryczne o średniorocznej wartości 100 – 150 V/m i zmienne pole elektromagnetyczne pochodzące od Słońca. Powłoki gazowe otaczające Ziemię przepuszczają pola elektromagnetyczne w określonych pasmach częstotliwości. Jedną grupę stanowi tzw. „okno świetlne" obejmujące podczerwień, światło widzialne i część ultrafioletu, a drugą tzw. „okno radiowe" obejmujące fale radiowe. Energia docierająca oknem radiowym jest niewielka, okno świetlne zaś jest podstawą życia biologicznego na Ziemi, które wydaje się być dobrze przystosowane do naturalnych pól elektromagnetycznych.

Sztuczne pole elektromagnetyczne jest wynikiem działalności człowieka w takich dziedzinach jak: radiofonia i telewizja, komunikacja, nawigacja, radiolokacja, medycyna i przemysł. Jego źródłem są także urządzenia gospodarstwa domowego.

Promieniowanie elektromagnetyczne w zakresie częstotliwości 0 – 300 GHz jest promieniowaniem niejonizującym, natomiast właściwości jonizujące ma promieniowanie nadfioletowe, rentgenowskie oraz gamma, czyli promieniowanie o częstotliwościach powyżej $3 \cdot 10^6$ GHz. Oddziaływanie tych pól na organizmy żywe w obydwu przypadkach jest odmienne. Promieniowanie jonizujące ze względu na jego destrukcyjne oddziaływanie z żywą materią jest przedmiotem zainteresowania radiologii, a substancje emitujące to promieniowanie są nazywane promieniotwórczymi, natomiast promieniowanie niejonizujące może spowodować efekt termiczny, polegający na miejscowym lub ogólnoustrojowym wzroście temperatury w żywym organizmie lub atermiczny, wywołujący zmiany funkcji biologicznych organów wewnętrznych człowieka. W dalszym ciągu omawiane będzie jedynie oddziaływanie promieniowania niejonizującego.

Typowym bezpośrednim źródłem promieniowania jest antena. Jest to urządzenie połączone przewodem współosiowym (fiderem) z nadajnikiem lub odbiornikiem i w przypadku nadajnika służy do wypromieniowania w swobodną przestrzeń fali elektromagnetycznej. Podstawowymi typami anten, używanymi w systemach telekomunikacyjnych są: dipol półfalowy, antena typu Yagi-Uda, logarytmiczno-periodyczna, panelowa oraz układ antenowy składający się z kilku anten. Geometria anteny zależy od zakresu częstotliwości, do którego jest ona przeznaczona oraz od wymaganych parametrów, np. zysku energetycznego, mocy czy kierunkowości.

Obecnie systemy telekomunikacyjne pokrywają praktycznie teren całego kraju i są to: radiofonia, telewizja naziemna, systemy radiokomunikacji ruchowej, telefonia komórkowa, sieci Wi-Fi, Bluetooth, systemy satelitarne, mikrofalowe linie radiowe. Zakres fal radiowych odpowiada częstotliwościom w przedziale 0,1 MHz – 300 GHz.

Innymi źródłami pól elektromagnetycznych są linie i stacje elektroenergetyczne, urządzenia gospodarstwa domowego, np. kuchenka mikrofalowa, telewizor, lodówka czy odkurzacz, urządzenia medyczne stosowane do fizjoterapii, takie jak diatermia długo- i krótkofalowa, lancetron czy magnetronik oraz urządzenia przemysłowe, np. piece indukcyjne. Obecnie człowiek wszędzie jest narażony na promieniowanie elektromagnetyczne i dlatego powinien zdawać sobie sprawę z realnych zagrożeń i wiedzieć, jak może zminimalizować ich skutki, a także umieć ocenić zasłyszane wiadomości na temat szkodliwego wpływu pola EM na człowieka.

Oddziaływanie pól elektromagnetycznych na człowieka

W obecnym stanie wiedzy, mimo sporej liczby badań, trudno o jednoznaczne wnioski dotyczące nie tylko charakteru, ale w ogóle istnienia swoistych efektów biologicznych związanych z działaniem pola elektromagnetycznego, zwłaszcza zakresu radiowego. Do zaakceptowania efektu jako swoistego konieczne jest bowiem ustalenie stopnia prawdopodobieństwa poznania trzech elementów: związku przyczynowego między zadziałaniem czynnika i wystąpieniem efektu, zależności efektu od dawki czynnika oraz mechanizmu działania czynnika.

Biologiczna aktywność pola elektromagnetycznego od wielu już lat jest faktem znanym i niekwestionowanym, ale nie oznacza to jeszcze bezwarunkowej jej szkodliwości.

Do określenia niepożądanego oddziaływania niejonizującego pola elektromagnetycznego na człowieka stosowane są dwa kryteria, których podstawą są wyniki badań eksperymentalnych.

Kryterium biologiczne jest oparte na wynikach badań zmian, jakie pola EM wywołują w ośrodkowym układzie nerwowym, w układzie neurohormonalnym, swoistym i nieswoistym układzie odporności immunologicznej i w funkcjach generatywnych. Podczas badań stosuje się metodę fizjologiczną,

elektrofizjologiczną, immunologiczną, biochemiczną i morfologiczną. Przyjętymi parametrami do badań są gęstość mocy pola EM i czas ekspozycji. Z wyników badań wynika, że dla gęstości mocy mniejszych niż 4 mW/cm^2 istnieje liniowa zależność między efektem biologicznym i gęstością mocy. W przypadku gęstości mocy przekraczających 4 – 10 mW/cm^2 ta zależność jest już nieliniowa.

Kryterium energetyczne, jako miarę oddziaływania pola EM na organizmy żywe, przyjmuje wartość energii absorbowanej przez organizm (albo jego część) odniesioną do 1 kg masy, mierzoną w W/kg. Tę wartość nazwano „swoistym tempem pochłaniania energii" i oznaczono w skrócie symbolem SAR, od ang. *Specific Absorption Rate*. Na podstawie precyzyjnych badań ustalono, że progowa wartość absorbowanej mocy, wywołująca mierzalny efekt termiczny tj. przyrost temperatury ciała o 1°C wynosi 4 W/kg. Stwierdzono, że pochłanianie energii w układach biologicznych jest zależne od częstotliwości pola.

Dotychczas jedynym rodzajem swoistych efektów udowodnionych dla częstotliwości radiowych, RF są efekty termiczne i odpowiedź ustroju na te zmiany (np. uruchomienie efektów termoregulacyjnych, takich jak zredukowanie produkcji ciepła metabolicznego i rozszerzenie naczyń krwionośnych). Z badań nad tym efektem wynikają dopuszczalne poziomy pola EM zawarte w obowiązujących obecnie normach w Europie i na świecie.

W celu rozpoznania efektów atermicznych (biologicznych) w polach częstotliwości radiowych małych intensywności i przy długotrwałej ekspozycji są prowadzone następujące rodzaje badań:

- badania laboratoryjne (*in vitro* i *in vivo*),
- badania epidemiologiczne i ochotników.

Badania *in vitro* wykonywane na izolowanych składnikach układów biologicznych są ważne dla określenia przypuszczalnych mechanizmów oddziaływania pól RF z układami biologicznymi oraz dla ustalenia warunków ekspozycji, w których należy testować całe zwierzęta (*in vivo*). Pozwalają one zrozumieć, jak pola RF działają na poziomie molekularnym czy komórkowym oraz powinny umożliwić ekstrapolację wyników *in vitro* na poziom *in vivo*, a także umożliwić wykrycie interakcji, które mogą być nieczytelne przy badaniach całego zwierzęcia. Jednakże efekty stwierdzone w badaniach *in vitro* powinny być testowane w badaniach *in vivo*.

Badania *in vivo* są przeprowadzane na kompletnych układach biologicznych, takich jak zwierzęta laboratoryjne, w laboratoriach, w których warunki mogą być dokładnie kontrolowane. Aby wyeliminować przypadkowość w ocenie, wyniki badań na zwierzętach mogą się odnosić do ludzi tylko wtedy, gdy obserwowane efekty występują u różnych gatunków zwierząt.

Największy, jak dotąd, niepokój społeczny budzi możliwość, że narażenie na pola RF małych intensywności może powodować nowotwory. Dotychczasowe badania epidemiologiczne są mało przekonujące i nie potwierdzają hipotezy, że narażenie na pola RF powoduje powstanie nowotworów lub wpływa na ich rozwój. We wszystkich badaniach epidemiologicznych istnieje niedostateczna ocena ekspozycji i czynników zaburzających oraz zła metodyka.

Pola magnetyczne o częstotliwości sieciowej

Najwięcej wątpliwości ekspertów badających skutki oddziaływania pól EM na ludzi [13] budzą pola magnetyczne o częstotliwości sieciowej (50 Hz), występujące w otoczeniu linii elektroenergetycznych i stacji transformatorowo-rozdzielczych. Chociaż istnieją dane wskazujące, że mogą one zwiększyć ryzyko zachorowalności ludzi na nowotwory, to z uwagi na nieznany mechanizm działania nie udało

się przy użyciu takich pól wywołać nowotworów u zwierząt, w związku z czym nie można twierdzić, że pola te są rakotwórcze, można jedynie, że są przypuszczalnie rakotwórcze (klasyfikacja Międzynarodowej Agencji Badań nad Rakiem – IARC[1]).

Z punktu widzenia oceny wpływu na człowieka najwięcej problemów sprawiają linie energetyczne, ze względu na ich rozpowszechnienie. Istnieje cały szereg badań, np. zestawionych w [8] i [13], wskazujących, że komunalna (domowa) ekspozycja na pola magnetyczne 50/60 Hz zwiększa ryzyko zachorowania dzieci na białaczkę i guza mózgu, a próg tego efektu występuje już dla indukcji 0,3–0,4 μT. Istnieją także pojedyncze, niepotwierdzone doniesienia o związku ekspozycji komunalnej dzieci z zachorowaniami na inne nowotwory, np. chłonniaki, mięsaki czy guzy ośrodkowego układu nerwowego. Podobne badania prowadzono u ludzi dorosłych. Doniesienia te są pojedyncze i w powszechnej opinii specjalistów nie można ich uznać za wystarczające do uznania ekspozycji na podwyższone komunalne pole magnetyczne za czynnik rakotwórczy u dorosłych. Równolegle z badaniami epidemiologicznymi prowadzone są badania na zwierzętach, które są eksponowane bardzo długo, niekiedy całe życie, przy czym ekspozycje są podobne do komunalnych (a nawet wyższe). Jak dotychczas nie potwierdziły one występowania podobnych efektów jak w przypadku ludzi. Mimo to głównie ze względu na wyniki badań u dzieci, IARC uznała w 2002 r. pola magnetyczne ELF (3–3000 Hz) za przypuszczalnie rakotwórcze dla ludzi (grupa 2B), czyli uznała, że istnieje dowód działania rakotwórczego tych pól u ludzi przy braku wystarczającego dowodu rakotwórczości u zwierząt doświadczalnych. Taka klasyfikacja jest przyczyną nieustannych sporów między zwolennikami i przeciwnikami negatywnego działania pola EM – ci pierwsi wskazują, że wyniki badań epidemiologicznych, które są najważniejsze przy ocenie wpływu danego czynnika, jednoznacznie wskazują na szkodliwość pól sieciowych, ci drudzy twierdzą, że brak potwierdzenia w badaniach na zwierzętach może być sygnałem, że wyniki badań epidemiologicznych są tylko artefaktami (nowotwory powodowane przez pole EM są stosunkowo rzadkie, a ryzyko względne, bardzo niskie). Dla równowagi należy powiedzieć, że w grupie 2B kancerogenów znajduje się np. kawa (jako przypuszczalny czynnik zachorowania na nowotwór pęcherza moczowego) i marynowane warzywa.

Oprócz badania ewentualnych skutków kancerogennych ekspozycji komunalnej sprawdzono również jej inne możliwe skutki zdrowotne, jednakże nie dały one wyników pozytywnych poza kilkoma badaniami wpływu na funkcjonowanie centralnego układu nerwowego, np. zwiększenie ryzyka wystąpienia zaburzeń psychiatrycznych zwłaszcza depresji.

Pola stacji bazowych, telefonów bezprzewodowych i stacji radiowo-telewizyjnych

Komisja ICNIRP (*International Commission on Non-Ionizing Radiation Protection*) [2] w 1998 r. opublikowała również swoje stanowisko na temat zagadnień zdrowotnych związanych z użytkowaniem radiotelefonów przenośnych oraz stacji bazowych. Oficjalny komunikat wydany na podstawie zebranych wówczas wyników badań naukowych wykluczał możliwość wpływu pola EM pochodzącego od stacji bazowych i od radiotelefonów na zdrowie człowieka, min. ze względu na małe poziomy mocy pochodzące od wyżej wymienionych systemów i urządzeń.

Przeprowadzane dotychczas badania wpływu stacji radiowych i telewizyjnych na zdrowie ludzi sygnalizowały pojedyncze przypadki wpływu na wzrost ryzyka zachorowalności na białaczkę u dzieci i do-

[1] *Grupa 1: czynnik jest rakotwórczy dla ludzi.*
Grupa 2A: czynnik jest prawdopodobnie rakotwórczy dla ludzi.
Grupa 2B: czynnik jest przypuszczalnie rakotwórczy dla ludzi.
Grupa 3: czynnik nie jest klasyfikowany ze względu na jego rakotwórczość dla ludzi.
Grupa 4: czynnik nie jest rakotwórczy dla ludzi.

rosłych oraz zależności zachorowań na czerniaka. Jednakże badania te nie dają podstaw, by zaklasyfikować pole elektromagnetyczne o częstotliwości radiowej jako czynnik kancerogenny. Nadal prowadzone są badania epidemiologiczne oraz laboratoryjne w tym zakresie [8], [13].

Pomiary pól elektromagnetycznych w środowisku

Intensywność promieniowania mierzy się w W/m^2, natomiast ilość energii RF zaabsorbowanej w tkankach mierzy się wielkością SAR, wyrażaną w W/kg. Pola RF mogą być, w zależności od ich natężenia, czynnikiem ekspozycji o dużej lub o małej intensywności. Ekspozycje w polach RF małych intensywności nie powodują jakiejkolwiek znaczącej zmiany temperatury ustroju. Nazywane są one efektami atermicznymi, są słabo rozpoznane i są obecnie przedmiotem badań.

Na podstawie wyników badań powstały i ciągle powstają nowe uregulowania prawne. Wspólną cechą norm w Europie i na świecie jest dwupoziomowa struktura. Podawane są tzw. ograniczenia podstawowe, których nie można przekroczyć pod żadnym warunkiem i zalecane poziomy odniesienia, które mogą zostać przekroczone, jeżeli zostanie udowodnione, że nie zostały przekroczone ograniczenia podstawowe.

Podstawowe ograniczenia są zdefiniowane przez gęstość indukowanego prądu i swoiste tempo pochłaniania energii (SAR) lub dla impulsowych pól EM przez swoiste pochłanianie energii (SA). Wielkości SAR i SA są zdefiniowane jako ilość energii absorbowana w jednostkowej masie (tkanki) mieszczącej się w określonej objętości o danej gęstości i wyrażane są w W/kg lub J/kg.

Wielkości tych nie można wyznaczyć bezpośrednio, dlatego w normach wprowadza się mierzalne poziomy odniesienia, które są wyrażone w wielkościach natężenia pola elektrycznego i magnetycznego oraz gęstości mocy.

Dwupoziomowość struktury obecnych norm dotyczy również rozróżnienia poziomów dopuszczalnych ekspozycji, odrębnie dla ogółu ludności i odrębnie dla pracowników.

Podstawowym sposobem ochrony ludzi przed ewentualnym szkodliwym wpływem pól EM jest ustalenie poziomów dopuszczalnych i opracowanie metodyk sprawdzania tych poziomów w warunkach rzeczywistych. Niemal powszechnie są stosowane pomiary, wykonywane zgodnie z prawnie usankcjonowaną metodyką i procedurą pomiarową i porównywanie zmierzonych poziomów z poziomami dopuszczalnymi w danym zakresie częstotliwości.

Obowiązek wykonywania pomiarów pola EM w środowisku wynika z zapisów art. 122a ustawy [12].

Uregulowania prawne

Normalizacją związaną z ochroną zdrowia ludzi przed elektromagnetycznym promieniowaniem niejonizującym zajmuje się wiele organizacji międzynarodowych i europejskich. Wśród nich do najbardziej aktywnych i znaczących należą:

- Światowa Organizacja Zdrowia (*World Health Organization* – WHO),
- Międzynarodowa Komisja Ochrony przed Promieniowaniem Niejonizującym (*International Commission on Non-Ionizing Radiation Protection* – ICNIRP),
- Europejski Komitet ds Normalizacji w dziedzinie Elektrotechniki (*European Committee for Electrotechnical Standardization* – CENELEC),

– Międzynarodowa Komisja Elektrotechniczna (*International Electrotechnical Commission* – IEC),
– Komisja Europejska (*European Commission* – EC).

Wartości graniczne pól EM w przepisach międzynarodowych

Obowiązujące wytyczne, zalecenia lub normy międzynarodowe i europejskie zawierające dopuszczalne poziomy pól są oparte na dobrze rozpoznanym efekcie termicznym, jedynym swoistym efektem udowodnionym dla częstotliwości radiowych. Wyniki badań i znajomość mechanizmów pochłaniania energii w układach biologicznych w zależności od częstotliwości stały się podstawą uregulowań prawnych wyrażanych za pomocą ograniczeń podstawowych definiowanych poprzez gęstość indukowanego prądu i wielkość zwaną SAR. Ponieważ tych wielkości nie można wyznaczyć bezpośrednio, w normach wprowadzono, z odpowiednim marginesem bezpieczeństwa, mierzalne poziomy odniesienia, wyrażone wielkościami natężenia zmiennego pola elektrycznego i magnetycznego, indukcji magnetycznej oraz gęstości mocy. Ustalono odrębne wartości graniczne dla ogółu społeczeństwa oraz wyższe dla ekspozycji zawodowej. Zalecenia EC w pełni pokrywają się z rekomendowanymi poziomami odniesienia podawanymi przez ICNIRP. W tabl. 1 i 2 podano poziomy odniesienia zgodne z zaleceniami obu komisji [1], [2].

Umieszczona przy danych liczbowych wartość f jest wyrażona w jednostkach zgodnych z kolumną *Zakres częstotliwości.*

Tabl. 1. Poziomy odniesienia dla ekspozycji ludności w zmiennych w czasie polach elektrycznych i magnetycznych (niezaburzone wartości skuteczne)

Zakres częstotliwości	Natężenie pola elektrycznego E [V/m]	Natężenie pola magnetycznego H [A/m]	Indukcja magnetyczna B [μT]	Gęstość mocy równoważnej fali płaskiej S_{eq} [W/m^2]
do 1 Hz	–	$3{,}2 \cdot 10^4$	$4 \cdot 10^4$	–
1 – 2 Hz	10000	$3{,}2 \cdot 10^4/f^2$	$4 \cdot 10^4/f^2$	–
8 – 25 Hz	10000	4000/f	5000/f	–
0,025 – 0,8 kHz	250/f	4/f	5/f	–
0,8 – 3 kHz	250/f	5	6,25	–
3 – 150 kHz	87	5	6,25	–
0,15 – 1 MHz	87	0,73/f	0,92/f	–
1 – 10 MHz	$87/f^{1/2}$	0,73/f	0,92/f	–
10 – 400 MHz	28	0,073	0,092	2
400 – 2000 MHz	$1{,}375/f^{1/2}$	$0{,}0037/f^{1/2}$	$0{,}0046f^{1/2}$	f/200
2 – 300 GHz	61	0,16	0,20	10

Tabl. 2. Poziomy odniesienia dla ekspozycji pracowników w zmiennych w czasie polach elektrycznych i magnetycznych (niezaburzone wartości skuteczne)

Zakres częstotliwości	Natężenie pola elektrycznego E [V/m]	Natężenie pola magnetycznego H [A/m]	Indukcja magnetyczna B [μT]	Gęstość mocy równoważnej fali płaskiej S_{eq} [W/m^2]
do 1 Hz	–	$1{,}63 \cdot 10^5$	$2 \cdot 10^5$	–
1 – 8 Hz	20000	$1{,}63 \cdot 10^5/f^2$	$2 \cdot 10^5/f^2$	–
8 – 25 Hz	20000	$2 \cdot 10^4/f$	$2{,}5 \cdot 10^4/f$	–
0,025 – 0,82 kHz	500/f	20/f	25/f	–
0,82 – 65 kHz	610	24,4	30,7	–
0,065 – 1 MHz	610	1,6/f	2,0/f	–
1 – 10 MHz	610/f	1,6/f	2,0/f	–
10 – 400 MHz	61	0,16	0,2	10
400 – 2000 MHz	$3f^{1/2}$	$0{,}008/f^{1/2}$	$0{,}01f^{1/2}$	f/40
2 – 300 GHz	137	0,36	0,45	50

Przyjęto wyższe wartości poziomów odniesienia dla pracowników niż dla ludności. Komisja ICNIRP uznała za słuszne założenie, zgodnie z którym ludzie świadomi występowania pól elektromagnetycznych, znający zasady unikania negatywnych skutków oddziaływania tych pól i mający możliwość kontrolowania ekspozycji, mogą przebywać w polach o wyższych parametrach. Ponadto stan zdrowia tych osób jest okresowo kontrolowany.

Dopuszczalne poziomy pola EM w Polsce

Normy dotyczące najwyższych dopuszczalnych natężeń, obowiązujące w Polsce do lat osiemdziesiątych, były wzorowane na przepisach radzieckich, które ustalono przy założeniu, że efekt termiczny powodujący podwyższenie temperatury tkanek i narządów, nie jest jedynym mechanizmem oddziaływania pola EM na organizmy żywe. Podstawę do tego stanowiły intensywne badania ludzi na stanowiskach pracy narażonych na działanie promieniowania EM, jak również badania doświadczalne na zwierzętach.

W początkowym okresie w krajach zachodnich (głównie w USA) przyjęto założenie, że oddziaływanie biologiczne pól EM uwarunkowane jest jedynie efektem termicznym promieniowania EM, uzasadniając to wynikiem bilansu cieplnego, tzn. ilością energii pochłoniętej w jednostce czasu w przeliczeniu na ilość ciepła oraz ilością ciepła, jaką ustrój człowieka może wydalić w normalnych warunkach. Generalnie można wysnuć wniosek, że normy zachodnie uwzględniały aspekt ekonomiczny oraz wojskowy, normy radzieckie zaś aspekt społeczny. Normy innych państw są pochodną obu tych rozważań i ewoluowały w kierunku wzajemnego zbliżenia. Przepisy polskie oparte na normie radzieckiej często nie były przestrzegane zarówno w zastosowaniach wojskowych, jak i cywilnych.

Ochrona środowiska (ogół ludności)

Obowiązujące w Polsce rozporządzenie [11] określa dopuszczalne poziomy elektromagnetycznego promieniowania niejonizującego, jakie mogą występować w środowisku, w postaci pól elektrycznych i magnetycznych stałych, pól elektrycznych i magnetycznych o częstotliwości 50 Hz, wytwarzanych przez stacje i linie elektroenergetyczne, pól elektromagnetycznych o częstotliwościach 1 kHz – 300 GHz, wytwarzanych w szczególności przez urządzenia radiokomunikacyjne, radionawigacyjne i radiolokacyjne. Rozporządzenie to określa także wymagania obowiązujące przy wykonywaniu pomiarów kontrolnych elektromagnetycznego promieniowania niejonizującego.

W Polsce na obszarach zabudowy mieszkaniowej oraz na obszarach, na których zlokalizowane są zwłaszcza szpitale, żłobki, przedszkola, internaty, składowa elektryczna elektromagnetycznego promieniowania niejonizującego o częstotliwości 50 Hz, czyli pochodzącego od linii elektroenergetycznych, nie może przekraczać wartości 1 kV/m.

Określone w rozporządzeniu dopuszczalne poziomy pól elektromagnetycznych, nie obowiązują w miejscach niedostępnych dla ludzi.

Polskie przepisy [11], [12] określają dużo niższe niż obowiązujące w dokumentach międzynarodowych [1], [2] i [3] dopuszczalne poziomy pól elektromagnetycznych.

Dopuszczalne poziomy pól elektromagnetycznych mogące występować w środowisku, w miejscach dostępnych dla ludności podano w tabl. 3 i 4 [11, zał. 1].

Tabl. 3. Dopuszczalne poziomy pól elektromagnetycznych na terenach przeznaczonych pod zabudowę mieszkaniową

Zakres częstotliwości	Składowa elektryczna	Składowa magnetyczna	Gęstość mocy
50 Hz	1 kV/m	60 A/m	–

Tabl. 4. Dopuszczalne poziomy pól elektromagnetycznych w miejscach dostępnych dla ludności

Zakres częstotliwości	Składowa elektryczna	Składowa magnetyczna	Gęstość mocy
0 Hz	10 kV/m	2500 A/m	–
0 – 0,5 Hz	–	2500 A/m	–
0,5 – 50 Hz	10 kV/m	60 A/m	–
0,05 – 1 kHz	–	3/f A/m	–
0,001 – 3 MHz	20 V/m	3 A/m	–
3 MHz –300 MHz	7 V/m	–	–
300 MHz – 300 GHz	7 V/m	–	0,1 W/m^2

Ochrona pracowników – przepisy BHP

Polskie przepisy dotyczące ochrony pracowników przed polami elektromagnetycznymi opierają się na rozporządzeniu [10] oraz wykorzystują szereg norm.

Rozporządzenie [10] zostało skonstruowane przy założeniu, że czas przebywania w polach elektromagnetycznych jest limitowany w zależności od częstotliwości pola i parametrów. Wyznaczono trzy rodzaje stref ochronnych:

- strefa niebezpieczna – obszar, w którym przebywanie pracowników jest zabronione,
- strefa zagrożenia – obszar, w którym dopuszczalne jest przebywanie pracowników zatrudnionych przy źródłach przez czas ograniczony,
- strefa pośrednia – obszar, w którym dopuszczalne jest przebywanie pracowników zatrudnionych przy źródłach w ciągu całej zmiany roboczej.

Wartości pola elektrycznego i magnetycznego dla granicy stref pośredniej i zagrożenia (E_1 i H_1) umieszczono w tabl. 5 i 6 [10].

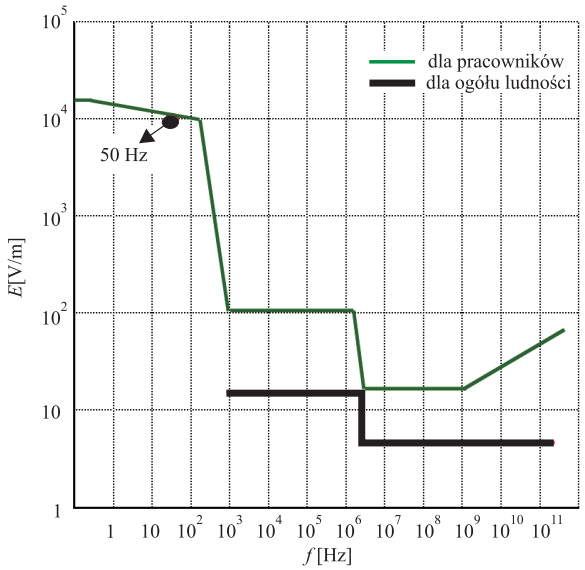
Tabl. 5. Dopuszczalne wartości natężenia pola elektrycznego E_1 na granicy strefy zagrożenia i pośredniej oraz doza dopuszczalna pola elektrycznego Dd_E

Zakres częstotliwości	E_1 [V/m]	Dd_E
0 – 0,5 Hz	20000	3200 $(kV/m)^2h$
0,5 – 300 Hz	10000	800 $(kV/m)^2h$
0,3 – 1 kHz	100/f	$0,08/f^2$ $(kV/m)^2h$
0,001 – 3 MHz	100	0,08 $(kV/m)^2h$
3 MHz – 5 MHz	300/f	$0,72/f^2$ $(kV/m)^2$ h
0,015 – 3 GHz	20	3200 $(V/m)^2$ h
3 GHz – 300 GHz	0,16f+19,5	$(f/2+55)^2$ $(V/m)^2$ h

Tabl. 6. Dopuszczalne wartości natężenia pola magnetycznego H_1 na granicy strefy zagrożenia i pośredniej oraz doza dopuszczalna pola magnetycznego Dd_H

Zakres częstotliwości	H_1 [A/m]	Dd_H
0 – 0,5 Hz	8000	512 $(kA/m)^2h$
0,5 – 50 Hz	200	0,32 $(kA/m)^2h$
0,05 – 1 kHz	10/f	$800/f^2$ $(A/m)^2h$
1 – 800 kHz	10	800 $(A/m)^2h$
0,8 – 150 MHz	8/f	$512/f^2$ $(A/m)^2$ h
0,15 – 3 GHz	0,053	0,022 $(A/m)^2$ h

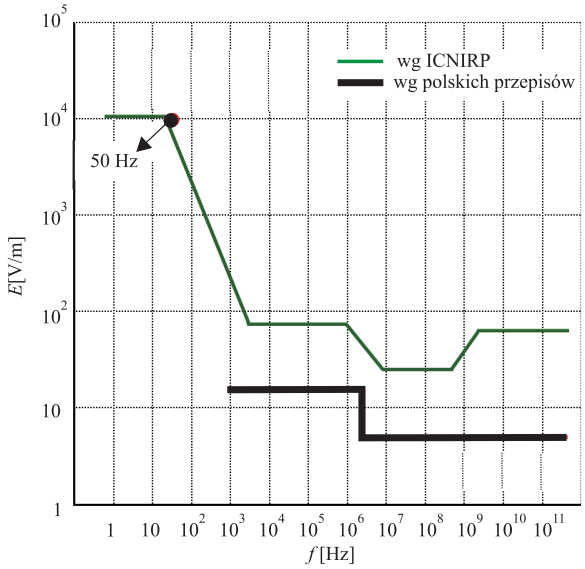
Zasady ustalania dopuszczalnych poziomów pól elektromagnetycznych są na całym świecie podobne. W Polsce obowiązują odrębne niższe poziomy dopuszczalne dla ogółu ludności bez ograniczania czasu przebywania w ich zasięgu oraz wyższe dla pracowników z limitowanym czasem ekspozycji (rys. 1).



Rys. 1. Dopuszczalne w Polsce poziomy składowej elektrycznej pola EM

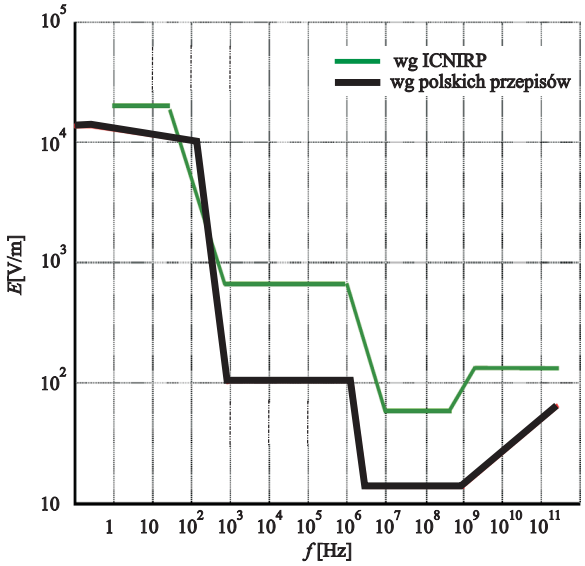
Polskie przepisy na tle uregulowań europejskich

Zasady ustalania wartości granicznych pola elektromagnetycznego w Polsce są inne niż w krajach Unii Europejskiej i na świecie, w polskich przepisach bowiem nie występuje uśrednianie natężenia pola EM w czasie i objętości, a także nie uwzględnia się kumulacji efektów działania pola elektromagnetycznego w czasie. Jednak ze względu na to, że wartości graniczne w obu przypadkach oparte są na tych samych wielkościach fizycznych porównano polskie i unijne wartości granicznych dopuszczalnych poziomów, przyjmując jako wspólny wskaźnik równoważną wartość składowej elektrycznej pola elektromagnetycznego.



Rys. 2. Dopuszczalne poziomy natężenia pola elektrycznego dla ogółu ludności

Na rys. 2 i 3 przedstawiono poziomy dopuszczalnej wartości natężenia pola elektrycznego dla ogółu ludności i dla pracowników w funkcji częstotliwości dla ustaleń polskich i ICNIRP/EC.



Rys. 3. Dopuszczalne poziomy natężenia pola elektrycznego dla pracowników

Z porównania przedstawionych uregulowań wynikają następujące wnioski:

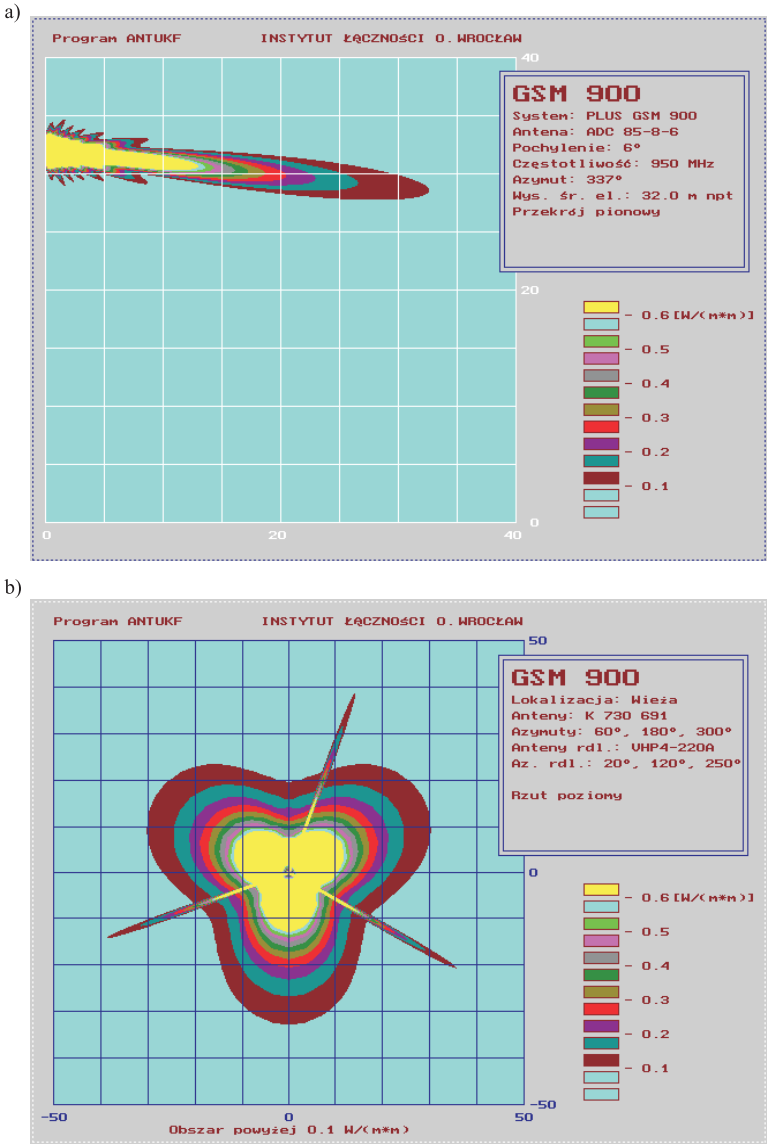
- Dopuszczalne poziomy pól EM, przyjęte w krajowych przepisach, zarówno w odniesieniu do osób zatrudnionych przy obsłudze i konserwacji źródeł pól EM (czyli pracowników) [10], jak i w odniesieniu do ogółu ludności [11], są kilka lub nawet kilkadziesiąt razy niższe niż w aktualnych normach lub zaleceniach zagranicznych [1] i [2].
- W odniesieniu do pracowników obsługi źródeł pól EM, przepisy polskie wyróżniają kilka stref (strefa pośrednia, zagrożenia, niebezpieczna), czego nie spotyka się w normach lub zaleceniach zagranicznych.
- Większość ustaleń zagranicznych bierze pod uwagę jako wskaźnik pól EM wartość uśrednioną w pewnym obszarze przestrzennym i określonym przedziale czasowym, podczas gdy przepisy polskie przyjmują jako wskaźnik pól EM wartości skuteczne natężeń pól elektrycznych i magnetycznych o częstotliwości 50 Hz i 0,001 – 300 MHz oraz wartości średnie gęstości mocy pól elektromagnetycznych o częstotliwości 300 MHz – 300 GHz (poprzednio były to wartości maksymalne).

Działalność Instytutu Łączności

Instytut Łączności posiada akredytację Polskiego Centrum Akredytacji (PCA) w zakresie pomiarów dla celów BHP i ochrony środowiska. Wykonuje liczne pomiary natężenia pola elektromagnetycznego pochodzącego od różnych źródeł: stacji bazowych telefonii komórkowej, linii energetycznych powyżej 110 kV, sieci energetycznych wewnątrz budynków, urządzeń medycznych (współpraca z przychodniami rejonowymi we Wrocławiu) oraz urządzeń przemysłowych (piece indukcyjne, zgrzewarki) itp.

Instytut dysponuje programem inżynierskim do obliczeń rozkładu pola wokół jego źródeł. Program przedstawia w wersji graficznej przekrój pionowy i poziomy na kierunkach maksymalnego promienio-

wania. Przedstawiony na rys. 4 przykład rozkładu pola wokół stacji bazowej został wykonany przy użyciu specjalistycznego oprogramowania ANTUKF metodą superpozycji, opisaną w [5], [6] i [7], czyli wektorowego (przestrzennego) sumowania składowych pola elektromagnetycznego.



Rys. 4. Stacja bazowa GSM 900, (a) przekrój pionowy, (b) rzut poziomy

Oddział Wrocławski Instytutu Łączności ma duże doświadczenie w obszarze kompatybilności elektromagnetycznej. Wykorzystując ten dorobek, pracownicy Oddziału wspólnie z pracownikami Politechniki Wrocławskiej, opracowali poradnik [8], przydatne kompendium wiedzy w zakresie:

- morfologii i źródeł pola elektromagnetycznego,
- systemów radiokomunikacyjnych, w tym systemów nowych generacji,

- kryteriów oceny niepożądanego oddziaływania pola elektromagnetycznego na ludzi,
- wyników badań wpływu pola elektromagnetycznego na organizmy żywe w różnych zakresach częstotliwości,
- stanu normalizacji w zakresie oddziaływania pola elektromagnetycznego na ludzi wraz z analizą porównawczą różnych norm,
- metod sprawdzania dopuszczalnych poziomów pól elektromagnetycznych w środowisku, a w szczególności: ustalania dopuszczalnych poziomów pól elektromagnetycznych, przeglądu metod obliczeniowych rozkładów pola elektromagnetycznego wokół obiektów nadawczych, pomiarów jako metody wyznaczania rozkładu pola wokół stacji nadawczych.

Bibliografia

[1] *Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz).* (1999/519/EC)

[2] *Guidelines for limiting exposure to time-varying electric, magnetic and electromagnetic fields (up to 300 GHz).* International Commission on Non-Ionizing Radiation Protection, Health Physics, Apr. 1998, Vol. 74, No 4

[3] *IEEE standard for safety levels with respect to human exposure to radio frequency electromagnetic fields, 3 kHz to 300 GHz.* New York, IEEE, 1999

[4] *Implementation report on the Council Recommendation limiting the public exposure to electromagnetic fields (0 Hz to 300 GHz).* Brussels, European Commission, March 2002

[5] Kałuski M., Macher M. : *Modelowanie numeryczne rozkładu pola elektromagnetycznego wokół stacji nadawczych w świetle aktualnych przepisów ochronnych*. KKRRiT, 2002

[6] Kałuski M., Macher M.: *Prezentacja oprogramowania służącego do wyznaczania obszarów ograniczonego użytkowania i stref ochronnych*. Warsztaty EMC, Wrocław 2001

[7] Kałuski M., Stasierski L.: *Electromagnetic Field Estimation in the Vicinity of Panel Antenna System for FM and TV Broadcasting***.** IEEE Trans. on Broadcasting, vol. 41, no. 4, pp. 136-142, December 1995

[8] *Ochrona przed narażeniami elektromagnetycznymi wynikającymi z rozwoju telekomunikacji współczesnej i telekomunikacji nowych generacji – pomiary anten radiokomunikacyjnych i pól elektromagnetycznych. Poradnik z zakresu ochrony przed narażeniami elektromagnetycznymi od systemów radiokomunikacyjnych.* Macher M., Tyrawa P., Kałuski M., Bieńkowski P., Grudziński E., Wrocław, 2008
http://www.mi.gov.pl/files/0/1790133/SPIV6Poradnik2008.pdf

[9] *Proposal for a council recommendation on the limitation of exposure of the general public to electromagnetic fields 0 Hz-300 GHz*. (presented by the European Commission)

[10] *Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 29 listopada 2002 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy*. Dz. U., 2002, nr 217, poz. 1833 (z późn. zm.)

[11] *Rozporządzenie Ministra Środowiska z dnia 30 października 2003 r. w sprawie dopuszczalnych poziomów pól elektromagnetycznych w środowisku oraz sposobów sprawdzania dotrzymania tych poziomów.* Dz. U., 2003, nr 192, poz. 1883

[12] Ustawa z dnia 27 kwietnia 2001 r. – *Prawo ochrony środowiska.* Dz. U., 2008, nr 25 poz. 150 (z późn. zm.)

[13] Zmyślony M.: *Ocena działania biologicznego i skutków zdrowotnych pól elektromagnetycznych w aspekcie wymagań raportów o oddziaływaniu przedsięwzięć na środowisko*. Warsztaty IMP, Łódź 2006

Marta Macher

Mgr Marta Macher – absolwentka Wydziału Matematyki, Fizyki i Chemii Uniwersytetu Wrocławskiego, kierunek fizyka (1973); pracownik Instytutu Łączności (od 1973 do 2010); autor i współautor prac badawczych i wielu publikacji; praca zawodowa: ochrona środowiska przed elektromagnetycznym promieniowaniem niejonizującym, modelowanie numeryczne rozkładu pola elektromagnetycznego wokół obiektów nadawczych, pomiary źródeł pól elektromagnetycznych.

Marek Kałuski

Mgr inż.Marek Kałuski (1947) – absolwent Wydziału Elektroniki Politechniki Wrocławskiej (1970); długoletni pracownik Instytutu Łączności Oddziału we Wrocławiu (od 1970); autor wielu prac konstrukcyjnych i publikacji, autor i współautor wielu patentów; zainteresowania naukowe: metrologia i modelowanie numeryczne źródeł pól EM, sterowanie pomiarowych systemów antenowych.

e-mail: m.kaluski@itl.waw.pl

Karolina Skrzypek

Mgr inż. Karolina Skrzypek – absolwentka wydziału Elektroniki Politechniki Wrocławskiej (2006); pracownik Instytutu Łączności we Wrocławiu od 2006 r.; bierze udział w pracach badawczych związanych z górnictwem i kompatybilnością elektromagnetyczną, praca zawodowa: zagadnienia związane z ochroną środowiska i BHP, kompatybilność elektromagnetyczna urządzeń m.in. przemysłowych i wojskowych, publikacje, artykuły oraz prowadzenie szkoleń z powyższych zagadnień.

e-mail: K.Skrzypek@itl.waw.pl

Polityka regulacyjna dotycząca sieci dostępowych nowej generacji

Stanisław Piątek

Omówiono proces formułowania polityki regulacyjnej Unii Europejskiej w sprawach sieci dostępowych nowej generacji (NGA) oraz czynniki techniczne, ekonomiczne i informacyjne, które powodują konieczność zmiany istniejącej regulacji dostosowanej do specyfiki sieci miedzianych. Wskazano główne założenia nowego podejścia regulacyjnego, elementy i węzły sieci obejmowane regulacją oraz wymagania inwestycyjne dla różnych wariantów FTTx. Uwzględniono zasady regulacji opłat hurtowych w sieci NGA oraz możliwości wycofywania regulacji w związku z upowszechnianiem tych sieci. Omówiono ryzyka związane z likwidacją dotychczasowych punktów dostępu do sieci operatora dominującego oraz możliwości rozwiązania spornych kwestii powstających na tym tle w stosunkach z operatorami alternatywnymi.

sieci nowej generacji, dostęp nowej generacji, FTTH, sieć pasywna, zalecenie Komisji Europejskiej, drabina inwestycyjna

Formułowanie polityki regulacyjnej dotyczącej sieci dostępowych nowej generacji

Regulacja rynków telekomunikacyjnych oparta na dyrektywach Unii Europejskiej o komunikacji elektronicznej wchodzi w okres konfrontacji ze zmianami technicznymi związanymi z budową sieci dostępowych nowej generacji, NGA (*New Generation Access*). Są one podstawową warstwą sieci nowej generacji, NGN (*New Generation Networks*). Sieci NGA są odpowiedzią na szybki wzrost liczby urządzeń przyłączanych do sieci oraz udostępnianie nowych usług wymagających wysokiej przepływności oraz jakości transmisji. Na poziomie UE sieci nowej generacji zostały włączone do strategii *Europa 2020* i *Europejskiej agendy cyfrowej*. W państwach członkowskich UE rozwój sieci nowej generacji staje się elementem polityki gospodarczej sprzyjającej utrzymaniu lub zwiększeniu poziomu konkurencyjności państw i regionów, utrzymaniu wzrostu gospodarczego lub przezwyciężaniu kryzysu.

Dostęp nowej generacji może być realizowany w sposób przewodowy lub bezprzewodowy. Zagadnienia regulacyjne sieci przewodowych i bezprzewodowych różnią się znacznie. Najtrudniejsze zagadnienia regulacyjne są związane z ewolucją sieci przewodowych w kierunku NGA. Władze regulacyjne muszą uwzględnić nowe uwarunkowania techniczne, ekonomiczne i informacyjne związane z rozwojem sieci NGA prowadzące do zmiany decyzji regulacyjnych, wokół których ukształtowały się modele biznesowe i interesy uczestników rynku telekomunikacyjnego.

Inwestycje związane z sieciami NGA polegają głównie na zastępowaniu światłowodami elementów dostępowej sieci miedzianej oraz budowie nowych, w pełni światłowodowych sieci dostępowych. Operator inwestujący w sieci światłowodowe uzyskuje znaczną obniżkę kosztów eksploatacyjnych, większą niezawodność sieci, możliwość szybszego uruchamiania nowych usług i podniesienia ich jakości [9, s. 6]. Podejmuje również znaczne ryzyko, szczególnie w przypadku budowy nowych, w pełni

światłowodowych sieci NGA. Ryzyko jest związane z popytem na nowe usługi, zwrotem nakładów na inwestycję oraz zmianą warunków konkurencyjnych na rynku. Zastosowanie światłowodów powoduje przebudowę architektury sieci, a w konsekwencji zmianę warunków dostępu do sieci dla innych operatorów. Ma to szczególne znaczenie w przypadku inwestowania w sieci NGA operatora dominującego. Warunki dostępu do jego sieci są regulowane, co powoduje że zmiana techniczna jest również poważnym wyzwaniem dla regulatora.

Główny problem regulacyjny polega na tym, w jaki sposób sprzyjać inwestowaniu w sieci NGA nie zmniejszając jednocześnie korzyści, jakie osiągnięto polityką regulacyjną dotyczącą sieci miedzianych oraz nie powodując powstania nowych barier w dostępie do rynku. Regulator musi rozstrzygnąć, w jakim zakresie dotychczasowa regulacja powinna być utrzymana bez zmian, dostosowana do nowych rozwiązań technicznych i warunków ekonomicznych lub wycofana. Regulator, podobnie jak operatorzy, działa w warunkach niepewności co do przyszłej sytuacji rynkowej. Decyzje największych operatorów w sprawie uruchomienia inwestycji w sieci światłowodowe nie zostały jeszcze podjęte. Koszty związane z tymi inwestycjami będą dopiero ponoszone, co powoduje, że warunki regulacyjne mają istotne znaczenie dla oceny celowości podjęcia inwestycji [4, s. 80].

Rozwiązania szerokopasmowe w sieci szkieletowej i dystrybucyjnej są wprowadzane ewolucyjnie, głównie na podstawie przesłanek ekonomicznych i technicznych [13]. W sieciach dostępowych zaś, infrastruktura dostępowa musi powstać w wyniku jednorazowych, skoncentrowanych nakładów inwestycyjnych, a wzrost popytu jest trudny do przewidzenia. Ryzyko inwestycyjne wynikające z niepewności rynkowej było dotychczas znacznie powiększone przez brak wyraźnych perspektyw regulacyjnych w odniesieniu do sieci NGA. Dookreślenie polityki regulacyjnej w odniesieniu do tych sieci powinno sprzyjać ograniczeniu niepewności odczuwanej przez operatorów podejmujących inwestycje oraz przedsiębiorców korzystających z cudzej infrastruktury. **Przewidywalność regulacji** w odniesieniu do sieci światłowodowych jest warunkiem podejmowania inwestycji. W odniesieniu do sieci miedzianych regulacja była reakcją na stan zastany, który blokował rozwój konkurencji. Regulacja służyła otwarciu rynku ukształtowanego w warunkach monopolu naturalnego wynikającego z charakterystyki techniczno-ekonomicznej sektora telekomunikacyjnego oraz finansowania rozwoju sieci ze środków publicznych lub dzięki rencie monopolistycznej. Regulacja była skierowana na otwarcie dostępu do istniejących sieci i ustalenie warunków odzyskiwania nakładów poniesionych w przeszłości. Regulacja sieci NGA kształtuje nowe środowisko gospodarcze, w którym dopiero będą podejmowane decyzje inwestycyjne prowadzące do budowy lub modernizacji sieci dostępowych. Dlatego polityka regulacyjna musi być wyklarowana zanim zostaną podjęte zasadnicze inwestycje.

Proces **formułowania polityki regulacyjnej** w sprawie sieci NGA toczy się równolegle na poziomie organów Unii Europejskiej i krajowym. Pierwsze próby określenia stanowiska w sprawie dostępowych sieci światłowodowych podjęto w latach 2007–2008, w początkowej fazie drugiego cyklu regulacyjnego. Nowe elementy dotyczące sieci NGA pojawiły się w ramach nowelizacji dyrektyw o komunikacji elektronicznej zakończonej w 2009 r. Obszerne stanowisko w sprawie regulacyjnego podejścia do sieci NGA przedstawiła Europejska Grupa Regulatorów, ERG (*European Regulators Group*) [7]. Następnie ERG uzupełniła swoje stanowisko o pogłębioną analizę ekonomiczną sieci NGA [8]. Analizy ERG zostały rozwinięte i zaktualizowane w raporcie Organu Europejskich Regulatorów Łączności Elektronicznej, BEREC (*Body of European Regulators for Electronic Communications*) z marca 2010 [1]. Jednak największy wpływ na przyszłą politykę regulacyjną powinno mieć **zalecenie Komisji w sprawie regulowanego dostępu do sieci dostępu nowej generacji**, ogłoszone we wrześniu 2010 r. [11]. Krajowe polityki wobec sieci NGA przedstawiły władze niektórych państw członkowskich UE. Również prezes UKE ogłosił w 2008 r. opinię dotyczącą budowania i eksploatacji infrastruktury NGA w Polsce [14]. Ponieważ odbiega ona od zalecenia Komisji Europejskiej można spodziewać się jej aktualizacji.

Źródła problemów regulacyjnych w sieciach NGA

Uwarunkowania techniczne

Charakterystyka techniczna sieci NGA ma wpływ na rodzaj i złożoność problemów wymagających rozwiązania przy formułowaniu polityki regulacyjnej w odniesieniu do tych sieci. Znaczna część współpracy międzyoperatorskiej jest oparta na rozstrzygnięciach regulacyjnych określających warunki dostępu do sieci operatora dominującego. Rozstrzygnięcia te uwzględniają charakterystykę techniczną i architekturę sieci miedzianych. Zmiana techniki w sieci dostępowej w nowy sposób określa możliwości dostępu do tych sieci, a to przekłada się na warunki konkurowania z operatorem dominującym.

Najprostsza zmiana regulacyjna polega na zastąpieniu wymagań dotyczących miedzianej linii abonenckiej, określonej w obowiązujących regulacjach jako "pętla metalowa" (*Metallic Loop*) wymaganiami uwzględniającymi również linię światłowodową. Zalecenie Komisji w sprawie rynków z 2003 r. dotyczyło metalowej pętli i podpętli, natomiast w zaleceniu z 2007 r. jest już mowa o fizycznej infrastrukturze dostępowej.

Trudniejszym zadaniem jest przygotowanie wymagań regulacyjnych dla różnych rozwiązań sieci NGA, jakie może zastosować operator dominujący. Wyróżnia się kilka **wariantów sieci FTTx**, (*Fiber to the x*) gdzie x określa miejsce zakończenia części światłowodowej sieci po stronie abonenta [3, s. 10]. Najczęściej dla potrzeb regulacyjnych rozpatruje się trzy warianty.

Pierwszy, określany jako FTTC (*Fiber to the Curb*) polega na doprowadzeniu światłowodu do szafki rozdzielczej, gdzie następuje styk z podpętlą miedzianą prowadzącą do obiektu użytkownika. Skraca się w ten sposób miedzianą pętlę abonencką do 300–1000 m. W zależności od długości odcinka miedzianego można osiągnąć przepływność do 15 Mbit/s (*Asymetric Digital Subscriber Line* – ADSL2+) lub do ok. 50 Mbit/s (*Very High Speed DSL* – VDSL). Zastosowanie wariantu FTTC w szerszej skali i uzyskanie odpowiednich przepływności jest bezpośrednio uzależnione od przeciętnej długości podpętli lokalnej w danym państwie [12, s. 30, 36]. Celowość podejmowania znaczących inwestycji w wariancie FTTC jest podważana ze względu na przewidywane zmiany w zapotrzebowaniu na przepływność, któremu sieci te mogą nie sprostać [3, s. 18].

Drugi wariant oznaczany skrótem FTTB (*Fiber to the Building*), polega na doprowadzeniu światłowodu do budynku i wykorzystaniu istniejącej w budynku sieci miedzianej. Odcinki sieci miedzianej nie powinny być dłuższe niż 100 m, co umożliwia osiąganie przepływności do 100 Mbit/s. W budynku lub w jego pobliżu jest lokalizowany punkt koncentracji. Sieci światłowodowe wykorzystujące odcinki linii miedzianych są określane jako sieci hybrydowe.

Trzeci wariant określany jako FTTH (*Fiber to the Home*) polega na doprowadzeniu światłowodu do lokalu użytkownika, co oznacza wyeliminowanie sieci miedzianej. Sieć w pełni światłowodowa jest wariantem najbardziej kosztownym w fazie inwestycyjnej, natomiast wykazuje wiele zalet podczas eksploatacji oraz zapewnia niemal nieograniczone możliwości zaspokojenia potrzeb przyszłych usług.

Sieć w pełni światłowodowa jest realizowana jako **sieć pasywna,** PON (*Passive Optical Network*). Między urządzeniem centralowym a obiektem użytkownika nie ma aktywnych urządzeń umożliwiających dostęp innym operatorom. W zależności od wybranego przez operatora wariantu inwestycyjnego, do użytkowników mogą być prowadzone dedykowane włókna światłowodu, co określa się jako **sieć typu punkt-punkt**. Uwolnienie takich linii dla potrzeb operatora alternatywnego jest stosunkowo proste, gdyż następuje w centrali operatora sieci dostępowej na poziomie przełącznicy optycznej, ODF (*Optical Distribution Frame*). Jest to wariant bardzo dogodny dla operatora korzystającego, ale jedno-

cześnie najbardziej obciążający pod względem inwestycyjnym operatora infrastruktury, ponieważ wymaga zaangażowania oddzielnego włókna dla każdego użytkownika końcowego na całej długości linii. Ze względów ekonomicznych korzystniejsze jest instalowanie na zakończeniu segmentu magistralnego światłowodu pasywnych urządzeń rozdzielających sygnał (*Splitter*), które umożliwiają obsługę większej liczby użytkowników (8,16, 32) za pomocą jednej linii. Dopiero odcinek światłowodu od rozdzielacza do użytkownika jest przeznaczony tylko do obsługi jednego użytkownika. Powstaje w ten sposób **sieć typu punkt-wiele punktów**. Brak urządzeń aktywnych w takiej sieci eliminuje szereg trudności technicznych i kosztów związanych z zasilaniem pośrednich punktów w sieci. Taka architektura utrudnia jednak dostęp do sieci operatorom alternatywnym. Operator alternatywny może bowiem w centrali uzyskać dostęp tylko do całej gałązki obsługującej większą grupę użytkowników, co jest trudne do pogodzenia z rynkowymi warunkami sprzedaży usług. Dostęp do końcowego segmentu linii abonenckiej na poziomie urządzenia rozdzielającego sygnał w linii światłowodowej jest wprawdzie możliwy, ale wiąże się ze znacznie większym zaangażowaniem inwestycyjnym operatora alternatywnego.

Przybliżanie zakończenia światłowodu do użytkownika końcowego w wariantach FTTB i FTTC powoduje, że coraz bliżej użytkownika znajdują się również urządzenia, w których następuje koncentracja ruchu i coraz mniejsza jest liczba użytkowników obsługiwanych w tych punktach. To oznacza, że operatorzy alternatywni ubiegający się o dostęp do użytkownika muszą doprowadzić swoją sieć coraz bliżej użytkownika końcowego. Wynikające stąd wydłużanie równoległej sieci dosyłowej operatora alternatywnego i zmniejszanie liczby użytkowników obsługiwanych przez dany węzeł prowadzi do pogorszenia jego efektywności. Dlatego rozmieszczenie punktów koncentracji ma duży wpływ na możliwość konkurowania z operatorem dominującym. Od rozmieszczenia tych punktów i ich charakterystyki technicznej zależy uzyskanie efektywnego dostępu do sieci przez operatorów alternatywnych.

Zmiana architektury sieci dostępowej ma przede wszystkim wpływ na usługę dostępu do uwolnionej pętli lokalnej. Dostęp operatorów alternatywnych do pętli lokalnej jest dotychczas realizowany głównie w centrali operatora dominującego. Operator alternatywny uzyskuje dostęp na poziomie przełącznicy głównej, MDF (*Main Distribution Frame*). Dostęp do podpętli abonenckiej jest wykorzystywany znacznie rzadziej ze względu na wyższe nakłady inwestycyjne operatora korzystającego. W przypadku FTTC konieczne będzie przeniesienie punktu dostępu z MDF do szafki rozdzielczej, w której linia światłowodowa zostanie połączona z istniejącą siecią miedzianą. Zmiana punktu dostępu do linii abonenckiej wymaga zapewnienia dosyłu sygnału pomiędzy nowym punktem dostępu a siecią operatora alternatywnego.

Kolejną istotną cechą techniki światłowodowej, o poważnych konsekwencjach dla polityki regulacyjnej, jest zdolność do przenoszenia sygnału przez włókno światłowodu na duże odległości bez konieczności regeneracji sygnału. Sieci miedziane zawierają pętle o długości do ok. 10 km, przy czym szerokopasmowa transmisja danych jest możliwa na odcinku do 5-6 km. Linie światłowodowe mogą obsługiwać obszar o promieniu do 20 km, a w nieodległej przyszłości zasięg ten może się znacznie zwiększyć. Ta właściwość sieci światłowodowej umożliwia likwidację części central, w których operatorzy alternatywni uzyskiwali dostęp do sieci miedzianej. Likwidacja central i odzysk środków zainwestowanych w te obiekty ma być jednym ze źródeł finansowania inwestycji w NGA [10, s. 421].

Zmiany te rodzą jednak istotne problemy po stronie operatorów alternatywnych. Muszą oni zapewnić kontynuację obsługi swoich klientów. Są zagrożeni utratą środków zainwestowanych w uzyskanie dostępu do likwidowanych central oraz muszą doprowadzić linie dosyłowe do nowych punktów dostępu. Sprawy te wymagają uwzględnienia w polityce regulacyjnej.

W związku z architekturą i funkcjonalnością sieci NGA konieczne jest rozstrzygnięcie, czy regulatorowi należy zapewnić wpływ na wybór wariantu inwestycyjnego realizowanego przez operatora dominu-

jącego, a jeżeli taki wpływ jest pożądany, to w jakim zakresie. Nawet wówczas, gdy regulator zgodnie z zasadą neutralności technicznej dopuszcza wszelkie warianty inwestycyjne, to ostatecznie rozkład uprawnień i obowiązków po stronie dysponenta sieci NGA i operatorów alternatywnych będzie motywował do przyjęcia określonych rozwiązań technicznych i architektury sieci.

Uwarunkowania ekonomiczne

Analiza podstawowych rodzajów sieci NGA wskazuje, że rozwiązania techniczne bardziej obciążające operatora sieci w fazie inwestycyjnej stwarzają jednocześnie dogodniejsze warunki do korzystania z sieci NGA przez innych operatorów. Warianty wymagające mniejszych nakładów od operatora sieci są bardziej kosztowne pod względem inwestycyjnym dla operatorów korzystających z jego sieci, a jednocześnie mniej dogodne pod względem handlowym. Minimalizując bowiem własne nakłady inwestycyjne dysponent sieci NGA podnosi bariery dostępu do tej sieci i utrudnia warunki konkurencji. Uwarunkowania te mogą motywować do podejmowania strategicznych decyzji inwestycyjnych z uwzględnieniem ich wpływu na konkurentów. Jeżeli inwestorem jest operator dominujący, to czynniki te muszą być uwzględnione przez regulatora.

Rozpoznanie przez regulatora uwarunkowań ekonomicznych budowy sieci NGA jest koniecznym etapem formułowania polityki regulacyjnej. Kluczowym czynnikiem wpływającym na decyzje dotyczące architektury sieci są koszty inwestycyjne. Koszty inwestycyjne są zależne od wybranego rozwiązania oraz warunków budowy sieci. Koszty inwestycji w światłowodową sieć dostępową obejmują prace ziemne i budowlane dotyczące kanalizacji, instalację światłowodów w kanalizacji, okablowanie budynków oraz wyposażenie węzłów sieci. Jednostkowe koszty prac ziemnych są odwrotnie proporcjonalne do gęstości zabudowy. Koszt prac ziemnych wynosi w zależności od warunków lokalnych 50-80% wartości całej inwestycji [7, s. 17]. Widać więc, jak bardzo wykorzystanie istniejącej kanalizacji zmniejsza koszt początkowej inwestycji. W wariancie FTTC kolejną pozycję kosztową stanowią urządzenia elektroniczne niezbędne do wyposażenia głównie węzłów sieci. Istotna jest więc liczba tych węzłów (szafek ulicznych). Generalnie, im światłowód jest doprowadzany bliżej do użytkownika i im większa jest liczba węzłów sieci, tym koszty przypadające na jedną linię są wyższe. Szczególnie znacząca różnica, na poziomie 1:5, występuje między wariantem FTTC oraz wariantami FTTB i FTTH, gdyż wariant FTTC wykorzystuje istniejącą podpętlę abonencką i okablowanie w budynkach.

Poza uwarunkowaniami kosztowymi wybór wariantu jest uzależniony od przewidywanych wymagań przepływności nowych usług, przestrzennego usytuowania użytkowników końcowych, rodzaju i gęstości zabudowy, a w przypadku inwestycji modernizacyjnych, także od stanu istniejącej infrastruktury. W dłuższym horyzoncie czasowym podstawowe znaczenie mają wymagania dotyczące przepływności. Czynniki te przesądzają o wyborze wariantu inwestycyjnego przez operatora. Natomiast dla regulatora istotne jest również to, jak poszczególne warianty sieci wpływają na możliwości budowy konkurencyjnego rynku.

Charakterystyczną cechą inwestycji w sieci NGA jest znacząca przewaga pierwszego inwestora na danym obszarze (*First Mover Advantage*). Inwestycje w NGA łączą się z istotnym wzrostem znaczenia skali i zakresu działalności dla efektywności operatora [7, s. 19]. Efektywna ekonomicznie inwestycja drugiego i kolejnych inwestorów w sieć NGA na tym samym obszarze jest mało prawdopodobna przy przeciętnej intensywności zabudowy. Dla ekonomicznego powodzenia przedsięwzięcia konieczne jest bowiem uzyskanie znacznego udziału w rynku. Tylko obszary o bardzo wysokiej gęstości zabudowy umożliwiają wprowadzenie konkurencyjnej infrastruktury NGA.

Sieć NGA może być zatem jeszcze bardziej niż miedziana sieć dostępowa zasobem niereplikowanym, stanowiącym „wąskie gardło" dla rozwoju konkurencji (*Bottleneck*). Istnienie miedzianej sieci

telefonicznej na wielu obszarach nie stanowiło przeszkody inwestycyjnej dla operatorów telewizji kablowej, czy operatorów lokalnych sieci internetowych, którzy obecnie konkurują na tych obszarach. Wprowadzenie na określony obszar sieci NGA bardzo ogranicza możliwość powstania równoległych infrastruktur dostępowych. Ekonomiczna charakterystyka sieci NGA może zatem potęgować problemy konkurencyjne, gdyż bariery dostępu do tego segmentu sieci mogą wzrastać. Uwarunkowania ekonomiczne sieci NGA mogą bez kontroli regulacyjnej prowadzić do remonopolizacji warstwy dostępowej sieci. Charakterystyka ekonomiczna NGA wykazuje więcej cech monopolu naturalnego niż tradycyjna sieć miedziana.

Z przedstawionych wyżej powodów tzw. konkurencja usługowa może być trudniejsza do osiągnięcia w warunkach sieci NGA. Dlatego twierdzi się, że ekonomiczna charakterystyka sieci NGA spowoduje wykształcenie się nowego poziomu równowagi pomiędzy konkurencją infrastrukturalną a konkurencją usługową [5, s. 225].

Uwarunkowania informacyjne

Decyzja o podjęciu inwestycji w sieci NGA i wyborze wariantu inwestycyjnego należy do operatora. Różnorodność scenariuszy inwestycyjnych przemawia jednak za tym, aby regulator wypracował preferowany model inwestycji w NGA odpowiadający lokalnym warunkom rynkowym. Projektowanie rozwiązań regulacyjnych możliwe jest tylko przy spełnieniu określonych warunków informacyjnych.

Zarówno na poziomie unijnym, jak i krajowym dąży się do zapewnienia **przejrzystości planów inwestycyjnych operatora dominującego**. Dotychczasowa regulacja skierowana na usuwanie zastanych barier dostępu do rynku nie wymagała pozyskiwania przez regulatora i konkurentów informacji o planach inwestycyjnych operatora dominującego. Plany inwestycyjne, ekspansja na nowe obszary i uruchamianie nowych usług były traktowane jako element konkurencji między operatorami i były objęte poufnością. Sprawa inwestycji w sieć dostępową pozostawała poza obszarem oddziaływania regulatora, a zatem brak było uzasadnienia i podstaw do żądania informacji w tej sprawie.

Inwestycje w sieci NGA kształtują przyszłe warunki konkurencji. Dlatego dużą wagę przywiązuje się do przejrzystości działań operatora dominującego i regulatora w sprawach sieci NGA. ERG stwierdza, że "*bez jasnego i przejrzystego obrazu intencji graczy rynkowych na zastosowanie sieci NGA, regulator nie ma możliwości jasnego wskazania środowiska regulacyjnego, które będzie miało zastosowanie do tych inwestycji*" [7, s. 27]. Brak dostatecznej informacji po stronie regulatora może zwiększyć udział kosztów utraconych, przyczynić się do nieuzasadnionych inwestycji i zmniejszyć potencjał konkurencji. Informacje o planach inwestycyjnych operatora dominującego są potrzebne nie tylko regulatorowi, lecz również operatorom korzystającym z sieci operatora dominującego. Muszą oni bowiem dostosować swoją sieć do planowanych zmian i opracować sposób migracji do nowej sytuacji infrastrukturalnej.

W obecnym porządku regulacyjnym przepływ informacji między operatorami zapewnia się za pomocą obowiązku przejrzystości. W prawie unijnym wynika on z art. 9 *Dyrektywy o dostępie*, który jest należycie odzwierciedlony w art. 37 *Prawa telekomunikacyjnego*. Obowiązek przejrzystości obejmuje ogłaszanie lub udostępnianie informacji w sprawach zapewnienia dostępu telekomunikacyjnego, specyfikacji technicznych sieci i urządzeń telekomunikacyjnych, charakterystyki sieci, zasad i warunków świadczenia usług, w tym także opłat. Obowiązek przejrzystości ma jednak charakter statyczny, w tym znaczeniu, że obejmuje jedynie sieć istniejącą oraz bieżące plany jej dostosowania do potrzeb współpracy z operatorami alternatywnymi. Perspektywa inwestycji w sieci NGA powoduje postulaty objęcia obowiązkiem przejrzystości zmian w sieci przewidywanych w najbliższych 2-5 latach [6, s. 7]. Realizacja tych postulatów nie może prowadzić do związania operatora obowiązkiem realizacji wszystkich

przedsięwzięć ujętych w planach inwestycyjnych, przekazanych regulatorowi i innym operatorom. Ryzyko odstąpienia od zamierzeń ujętych w planie nie może obciążać tylko operatora planującego budowę sieci. Musi ono w pewnej mierze obciążać przedsiębiorców zamierzających oprzeć swoją działalność telekomunikacyjną na wykorzystaniu cudzej sieci dostępowej.

Odejściu od zasady, że plany inwestycyjne stanowią tajemnicę operatora sprzyja współzależność regulatora i uczestników rynku. Ze względu na wielość wariantów inwestycyjnych i różne skutki, jakie mogą one wywoływać w konkretnych warunkach rynkowych, regulator może precyzyjnie określić politykę stosowania środków regulacyjnych tylko w odniesieniu do konkretnych zamierzeń inwestycyjnych. W interesie inwestującego operatora jest ustalenie długofalowej i stabilnej polityki stosowania obowiązków regulacyjnych. Tylko w stabilnym środowisku regulacyjnym może on racjonalnie ocenić ryzyko związane z inwestycjami w NGA. Operatorzy alternatywni są z kolei zainteresowani informacją o planach inwestycyjnych operatora dominującego ze względu na własne plany rozwojowe oraz konieczność adaptacji wcześniejszych inwestycji do zmienionej architektury sieci [5, s. 228]. Wzajemna zależność realizacji celów regulatora, operatora dominującego i operatorów alternatywnych powinna również sprzyjać dokładności i wiarygodności informacji o zamierzeniach inwestycyjnych operatora dominującego.

Gwarancji stabilności środowiska regulacyjnego nie da się wyprowadzić z obowiązującego prawa. Przewiduje ono bowiem bardzo znaczny zakres uznania dla organu regulacyjnego. Sprecyzowany plan inwestycji w sieci NGA operatora dominującego może być podstawą szczegółowych i stabilnych warunków regulacyjnych. Na podstawie takiego planu regulator może przedstawić swoje oczekiwania dotyczące zapewniania dostępu operatorom alternatywnym i zamierzone środki regulacyjne gwarantujące taki dostęp. Ostatecznie, w interesie wszystkich stron leży zmniejszenie asymetrii informacyjnej w sprawie zamierzeń inwestycyjnych dotyczących NGA. Operator dominujący ujawniając swoje plany inwestycyjne ryzykuje wprawdzie utratę części korzyści przypadających pierwszemu inwestorowi, ale redukuje niepewność związaną z regulacyjnymi wymaganiami dotyczącymi przyjętego wariantu inwestycyjnego.

Pożądany i rekomendowany w literaturze model współdziałania regulatora i operatora dominującego polega na wymianie informacji o planach inwestycyjnych w zamian za wiążące określenie założeń polityki regulacyjnej w sprawie wymaganych usług dostępowych do sieci NGA oraz zasad ustalania cen za usługi dostępowe. Z kolei znoszenie wcześniejszych obowiązków dostępowych w stosunku do operatora dominującego byłoby uzależnione od wyprzedzającego przekazywania konkurentom informacji o zmianach w sieci [6, s. 11]. Odstąpienie od planu lub jego modyfikacja prowadziłyby do odpowiedniego przedłużenia obowiązku zapewniania dostępu w dotychczasowej formie, co z reguły będzie dodatkowym obciążeniem dla operatora. Regulacja może w ten sposób budować bodźce do skrupulatnego przestrzegania obowiązku przejrzystości w odniesieniu do sieci NGA przez operatora dominującego.

Inwestycje utracone

Regulacja usług opartych na wykorzystaniu miedzianej sieci operatora dominującego doprowadziła w państwach członkowskich UE do powstania infrastruktury służącej wyłącznie wykorzystaniu tej sieci przez operatorów alternatywnych. Po stronie operatora dominującego są to inwestycje związane z przystosowaniem infrastruktury do potrzeb kolokacji urządzeń operatorów alternatywnych. Po stronie operatorów alternatywnych są to nakłady związane z doprowadzeniem własnej sieci do punktów styku z siecią operatora dominującego. W znacznej części są to inwestycje oparte na warunkach współpracy ustalonych przez regulatora, w formie ofert ramowych lub decyzji rozstrzygających sprawy sporne.

Budowa sieci NGA powoduje przesunięcie lub likwidację znacznej części punktów dostępu do sieci operatora dominującego, w których operatorzy alternatywni uzyskiwali dostęp do uwolnionej pętli lokalnej i usługi strumienia bitów. Z tego powodu mówi się nawet o "dramacie zagrożenia" dotychczasowego modelu konkurencji opartego na uwalnianiu pętli lokalnej [10, s. 244]. W tej kwestii regulator musi wypracować sposób kojarzenia dwóch, częściowo sprzecznych celów. Z jednej strony zmiana techniki miedzianej na światłowodową zwiększa efektywność operatora dominującego oraz przynosi korzyści użytkownikom w zakresie różnorodności, jakości i ceny usług. Z drugiej jednak, może ograniczyć efektywną konkurencję ze strony operatorów alternatywnych i narazić ich na utratę środków zainwestowanych w infrastrukturę dostępu.

Na regulacyjne rozwiązanie tego problemu składa się kilka elementów. Podjęcie inwestycji w sieć NGA nie znosi obowiązków regulacyjnych operatora dominującego. Decyzje regulacyjne przewidują obowiązek utrzymywania dostępu telekomunikacyjnego, który został wcześniej ustanowiony. Zatem do czasu zniesienia tego obowiązku operator dominujący musi zapewniać dostęp do określonych elementów sieci lub usług, niezależnie od zmian następujących w jego sieci. Pełna kontrola regulatora nad znoszeniem obowiązków dostępowych, w powiązaniu ze stabilizującym oddziaływaniem "obowiązku utrzymywania dostępu wcześniej ustanowionego", stwarza dla operatorów alternatywnych dostateczną ochronę przed antykonkurencyjnymi efektami strategii inwestycyjnej polegającej na usuwaniu dotychczasowych punktów dostępu.

Możliwość blokowania zmian w istniejącej infrastrukturze miedzianej nie rozwiązuje jednak problemu ścieżki dojścia do sytuacji konkurencyjnej w środowisku sieci NGA. Harmonizacja środków zapobiegających zmianom w infrastrukturze dostępowej w celu uniknięcia nadmiernych strat po stronie operatorów alternatywnych oraz rozwiązań umożliwiających przejście do nowej architektury sieci dostępowej jest zadaniem regulatora. Rozwiązanie takie może powstać jedynie przez wyważenie kosztów i korzyści związanych z utrzymywaniem istniejącego dostępu oraz przechodzeniem do nowej architektury sieci dostępowej, z uwzględnieniem okresów zwrotu z dokonanych wcześniej inwestycji.

Największe ryzyko dla operatorów alternatywnych wydaje się towarzyszyć inwestycjom w wariant FTTC. Inwestycje w doprowadzenie linii dosyłowych do szafek (węzłów) koncentrujących podpętle lokalne oraz w kolokację i wyposażenie węzłów na tym poziomie, a także utracone inwestycje w uwolnienie pętli na poziomie MDF mogą być zbytnim obciążeniem dla operatorów alternatywnych. Inwestycje operatorów alternatywnych w wariant FTTC są tym bardziej problematyczne, iż brak jest pewności co do stabilności tego wariantu. Kolejny etap przebudowy sieci w kierunku wariantu FTTB/FTTH mógłby ponownie narazić operatorów alternatywnych na utratę zainwestowanych środków.

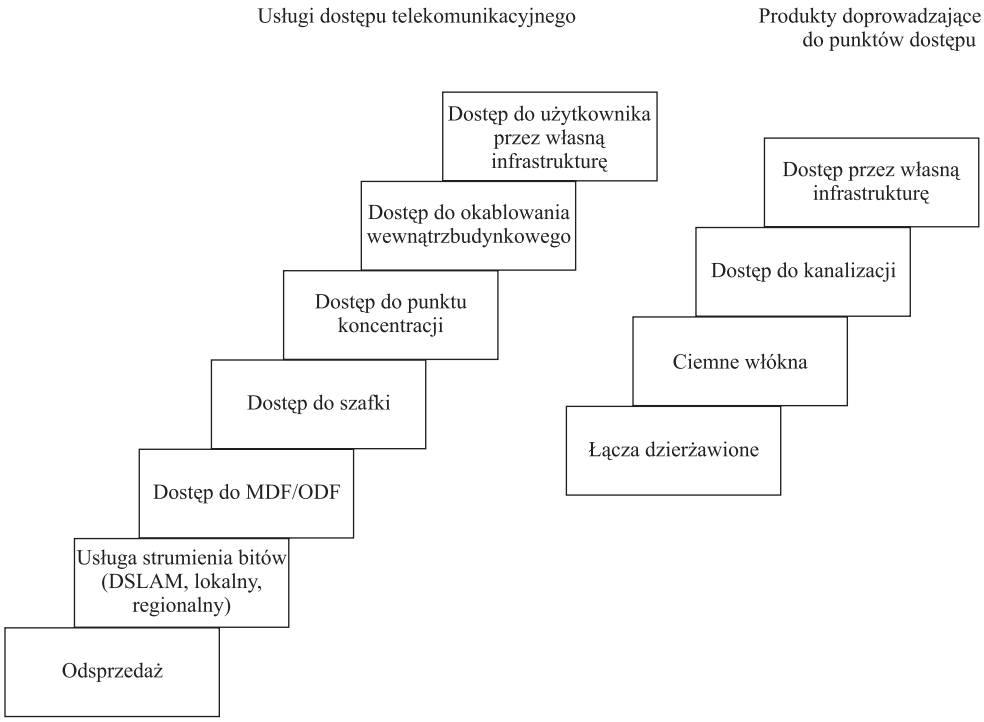
Bezsporne jest, że regulator może utrzymać wcześniejsze obowiązki dostępowe w niezbędnym zakresie i czasie. Powstaje jednak wówczas problem ich utrzymywania tylko dla potrzeb operatora alternatywnego. Regulator ma do wyboru dwa rozwiązania – utrzymanie istniejących punktów dostępu (z reguły MDF) na dotychczasowych zasadach lub określenie warunków, których spełnienie przez operatora dominującego, pozwoli na zniesienie obowiązku zapewniania dostępu w dotychczasowej lokalizacji. W żadnym wypadku uruchomienie sieci NGA nie powinno prowadzić do zaprzestania usługi hurtowej, prowadzącego do przejęcia użytkowników końcowych przez operatora dominującego. Podkreśla się również, że użytkownik końcowy nie może być obciążany dodatkowymi kosztami wynikającymi z utrzymywania infrastruktury sieci miedzianej tylko dla potrzeb operatora alternatywnego. Jednocześnie przestrzega się przed automatycznym gwarantowaniem ochrony przez regulatora wszelkim wcześniejszym inwestycjom, kosztem dynamiki rozwoju rynku jako całości [2, s. 752]. Tylko całościowa ocena zakresu i czasu utrzymywania obowiązków dostępowych wcześniej ustanowionych, warunków ich wykonywania w okresie przejściowym oraz zasad migracji do nowej architektury może złożyć się na rozwiązanie wspierające długofalowo konkurencję usługową i infrastrukturalną.

Koncepcja regulacyjnego podejścia do sieci NGA

Konceptualizacja sieci NGA dla potrzeb regulacyjnych

Koncepcja sieci NGA kształtuje się jako złożony zbiór technik, standardów i podejść ekonomicznych opracowywanych, a coraz częściej także wykorzystywanych w praktyce. Coraz ściślejszy związek tej koncepcji z celami realizowanymi przez władze publiczne w sektorze telekomunikacyjnym wymaga uzupełnienia wielowariantowych prognoz dotyczących przyszłości sieci NGA podstawowymi kategoriami pojęciowymi, za pomocą których regulator może formułować swoje stanowisko w tych sprawach. Koniecznym etapem przygotowania polityki regulacyjnej była konceptualizacja sieci NGA dla potrzeb regulacji poprzez określenie pojęć dotyczących głównych węzłów, techniki oraz procesów, które należy uwzględnić w polityce regulacyjnej. Obecny stan tych prac odzwierciedla zalecenie Komisji w sprawie regulowanego dostępu do sieci NGA [11] oraz raport BEREC w sprawie implementacji NGA i produktów hurtowych [1].

Komisja zaleca podejście do sieci NGA oparte na **koncepcji drabiny inwestycyjnej.** Kształt drabiny inwestycyjnej w środowisku sieci NGA odbiega od drabiny inwestycyjnej w sieci miedzianej (rys. 1).



Rys.1. Drabina inwestycyjna w sieci NGA [1]

Drabina inwestycyjna w sieci NGA jest bardziej rozbudowana, przy czym znaczenie poszczególnych szczebli jest uzależnione od zastosowanego wariantu inwestycyjnego FTTx. Nie ulega natomiast zmianie sama idea drabiny inwestycyjnej. Poszczególne poziomy dostępu są usytuowane coraz bliżej użyt-

kownika końcowego, co wymaga wzrastającego zaangażowania własnej infrastruktury operatora alternatywnego. Kolejne szczeble usług dostępowych ulokowanych na drabinie to: odsprzedaż usług, usługa strumienia bitów na różnych poziomach, dostęp na poziomie przełącznicy głównej, na poziomie szafki ulicznej, punktu koncentracji, okablowania budynkowego i dostęp z wykorzystaniem wyłącznie własnej infrastruktury. Równolegle funkcjonuje drabina produktów doprowadzających sieć operatora alternatywnego do poszczególnych poziomów dostępu. Znajdują się na niej produkty o coraz mniejszym udziale wartości wnoszonej przez operatora dominującego i narastającym udziale własnej infrastruktury operatora alternatywnego – łącza dzierżawione, ciemne włókna w kablu światłowodowym, dostęp do kanalizacji teletechnicznej, w której operator alternatywny instaluje własne media transmisyjne oraz dostęp przez własną infrastrukturę.

Podstawowe pojęcia dotyczą węzłów sieci NGA i obszarów obsługiwanych z tych węzłów. **Obszarowy punkt dystrybucyjny**[①] jest podstawowym węzłem sieci NGA. Znajduje się w miejscu styku sieci dostępowej z siecią dystrybucyjną lub szkieletową. Wszystkie linie abonenckie znajdujące się na tym obszarze dystrybucyjnym są przyłączone do przełącznicy optycznej ODF. Ze względu na wydłużenie linii abonenckiej obszary dystrybucyjne w sieci NGA są znacznie większe niż dawne obszary centralowe sieci miedzianej. Przez ODF linie abonenckie są połączone z urządzeniami operatora sieci dostępowej albo z urządzeniami operatorów alternatywnych. Połączenie z urządzeniami operatora alternatywnego może być bezpośrednie lub następować przez linię dosyłową (*Backhaul*).

Punkty koncentracji ruchu na obszarze dystrybucyjnym są usytuowane inaczej w wariancie FTTH i FTTB oraz w sieci FTTC. Dla sieci FTTH i FTTB drugim kluczowym węzłem jest **punkt dystrybucji** zlokalizowany w piwnicy budynku wielomieszkaniowego lub w pobliskiej studzience. Znajduje się on na styku segmentu magistralnego łącza abonenckiego oraz segmentu końcowego tego łącza. W tym węźle światłowód segmentu magistralnego wyprowadzony z obszarowego punktu dystrybucyjnego rozdziela się na łącza prowadzące do lokali użytkowników końcowych. W punkcie tym znajduje się przełącznica umożliwiająca połączenie włókien z odcinka magistralnego z przewodami segmentu końcowego oraz mogą znajdować się pasywne rozdzielacze optyczne. Dla sieci FTTC takim punktem koncentracji ruchu jest szafka uliczna, w której światłowodowy odcinek magistralny łączy się z miedzianymi przewodami prowadzącymi do lokali użytkowników.

Segment końcowy sieci NGA łączy lokal użytkownika z pierwszym punktem dystrybucji. Składa się z okablowania budynkowego i ewentualnie z dodatkowego odcinka prowadzącego do pierwszego punktu koncentracji. Segment końcowy w sieci FTTH/FTTB odpowiada pod względem regulacyjnym podpętli w sieci hybrydowej FTTC.

W sprawie pokonywania „wąskich gardeł" w sieci NGA rekomenduje się trzy podstawowe rozwiązania. Pierwsze jest oparte na zastosowaniu **sieci wielowłóknowej**. Polega to na instalowaniu większej liczby światłowodów na odcinku magistralnym oraz w segmencie końcowym niż wymaga zaspokojenie potrzeb inwestora. Nadwyżkowe włókna światłowodu mają służyć innym operatorom. Druga koncepcja jest oparta na zastosowaniu różnych wersji **zwielokrotnienia długości fali,** WDM (*Wavelength Division Multiplexing*), czyli zwielokrotnienia sygnałów przez wyodrębnienie wielu fal o różnych długościach, przesyłanych równocześnie we włóknie światłowodu. Alternatywą rozwiązań technicznych jest rozwiązanie czysto regulacyjne polegające na symetrycznym obowiązku udostępniania końcowego segmentu, będącego takim wąskim gardłem, przez każdego operatora, który zrealizował inwestycję, niezależnie od jego pozycji rynkowej.

① *W angielskojęzycznej wersji zalecenia Komisji jest „Metropolitan Point of Presence", trudne do określenia w innych językach.*

Założenia regulacji dotyczące sieci NGA

U podstaw zalecenia Komisji leży deklaracja **celów regulacyjnych dotyczących sieci NGA**. Celem regulacji jest promowanie efektywnych inwestycji w nową i modernizowaną infrastrukturę NGA, przy utrzymaniu skutecznej konkurencji i z uwzględnieniem ryzyka ponoszonego przez inwestorów. Działania regulacyjne w sprawach NGA koncentrują się na dostępie fizycznym do infrastruktury sieciowej (rynek 4) i hurtowym dostępie szerokopasmowym (rynek 5). Komisja zaleca prowadzenie **skoordynowanej analizy rynków** i spójne stosowanie środków regulacyjnych. Środki skutecznie zastosowane na rynku 4 mogą bowiem eliminować konieczność regulowania rynku 5. Niepowodzenia na rynku 4 można skompensować odpowiednimi usługami strumienia bitów na rynku 5. Wachlarz stosowanych środków regulacyjnych i ich nowe kombinacje powinny odzwierciedlać strukturę drabiny inwestycyjnej, która obejmuje usługi dostępowe z obydwu rynków.

Polityka prowadzona na rynkach związanych z sieciami NGA powinna zapewniać **pewność regulacyjną** wszystkim inwestującym operatorom. Ze względu na oczekiwania inwestycyjne władz regulacyjnych wychodzi się poza wymóg stabilności regulacji dodając postulat wyjaśniania w jak najszerszym możliwym zakresie, jak przewidywane zmiany warunków rynkowych mogą wpłynąć na stosowane środki regulacyjne. Regulator powinien prognozować zmiany obowiązków regulacyjnych w kolejnych cyklach regulacyjnych, na podstawie przewidywanych zmian warunków rynkowych. Jest to konsekwencją długiego okresu zwrotu nakładów ponoszonych na wytworzenie sieci NGA.

Komisja uznaje, że wprowadzenie sieci NGA zmieni ekonomiczne warunki świadczenia usług i zmodyfikuje sytuację konkurencyjną. Skala tej zmiany może być na tyle znacząca i trwała, że uzasadni wyróżnienie **lokalnych rynków geograficznych** objętych inwestycjami, na których obowiązki regulacyjne zostaną ograniczone lub wycofane. Jeżeli zmiany spowodowane inwestycjami nie będą uzasadniać wyróżnienia odrębnego rynku geograficznego, należy rozważyć zróżnicowanie obowiązków regulacyjnych w zależności od poziomu konkurencji na poszczególnych obszarach. Można zatem przyjąć, że założeniem podejścia regulacyjnego jest terytorialna segmentacja rynków lub co najmniej dyferencjacja intensywności regulacji na skutek inwestycji w sieci NGA.

Regulacja usług hurtowych w sieci NGA operatora dominującego ewoluuje od prostej zasady niedyskryminacji w kierunku **zasady ścisłej równoważności dostępu**. Punktem wyjścia są takie same warunki nabywania usług hurtowych przez operatorów alternatywnych, jak przez część detaliczną operatora dominującego. Dochodzi do tego wymóg identycznych warunków dostępu do informacji o istniejącej infrastrukturze, planach inwestycyjnych oraz zastosowanie takich samych procedur rezerwowania i zamawiania usług. Utrwaleniu równoważności ma służyć oferta ramowa, która powinna wiązać w stosunkach zewnętrznych i wewnętrznych. Zasada ścisłej równoważności dostępu wymaga uporządkowania przepływów informacyjnych w strukturach operatora dominującego. Zablokowanie przepływu informacji o planach wdrożeniowych operatorów alternatywnych między częścią hurtową a detaliczną operatora dominującego ma zapobiec uzyskaniu przez niego przewagi handlowej na rynku detalicznym. Wdrożenie **systemu kluczowych wskaźników** dotyczących jakości usług świadczonych podmiotom zewnętrznym oraz własnym ogniwom detalicznym powinno dać regulatorowi instrument służący ocenie stopnia realizacji zasady ścisłej równoważności.

Trwała obecność w sieciach NGA elementów, których powielanie jest gospodarczo nieefektywne lub fizycznie niewykonalne, prowadzi do rozbudowy arsenału regulacyjnego o **obowiązki symetryczne** w zakresie zapewniania dostępu i współkorzystania z infrastruktury. Obciążają one wszystkich operatorów sprawujących kontrolę nad takimi elementami. Obowiązki symetryczne były stosowane już wcześniej, jeżeli zasoby zostały uzyskane w wyniku dostępu do cudzych terenów, albo nie mogły zo-

stać zwielokrotnione z powodów środowiskowych. W przypadku sieci NGA, stosowanie obowiązków symetrycznych np. w zakresie okablowania budynkowego jest uzasadnione brakiem ekonomicznych przesłanek dla równoległych inwestycji.

Polityka regulacyjna w sprawie sieci NGA powinna w znacznie większym stopniu zostać oparta na **uzgodnieniach operatora dominującego z operatorami alternatywnymi.** Dotyczy to szczególnie uzgodnień między operatorami, którzy już współpracują na poziomie hurtowym. Nie oznacza to przejścia na mechanizm kontraktowy, lecz wypracowywanie treści rozstrzygnięć regulacyjnych w drodze uzgodnień sankcjonowanych przez regulatora.

Informacyjne warunki prowadzenia regulacji

Komisja potwierdza, że regulacja sieci NGA stawia nowe wymagania informacyjne dotyczące rozpoznania bieżącego stanu infrastruktury, planów jej modernizacji oraz budowy nowych zasobów. Organy regulacyjne powinny wspólnie z innymi władzami tworzyć **bazy danych o infrastrukturze**, w szczególności o lokalizacji geograficznej, pojemności i innych właściwościach fizycznych infrastruktury technicznej, którą można wykorzystać do budowy sieci światłowodowych. Dostęp do takich baz powinni mieć wszyscy operatorzy w ramach polityki ułatwiania inwestycji. Ujawnianie istniejących zasobów i tworzenie warunków informacyjnych do projektowania i budowy sieci NGA staje się zadaniem publicznym, wspierającym działania inwestycyjne wszystkich operatorów oraz inwestorów publicznych (samorządów).

Drugi kluczowy zasób informacyjny tworzą **dane o planach inwestycyjnych** operatora dominującego. Projektowanie przez regulatora warunków regulacyjnych dla przyszłych inwestycji musi być poprzedzone przekazaniem przez inwestora informacji o planowanych działaniach, wybranej technologii i architekturze sieci. Projektowanie warunków regulacyjnych dla wszystkich możliwych wariantów inwestycyjnych należy uznać za wysiłek niecelowy.

Regulator powinien tworzyć odpowiednie warunki informacyjne do podejmowania decyzji inwestycyjnych przez operatorów alternatywnych. Następstwem ogłoszenia planów inwestycji w sieci NGA operatora dominującego powinna być **ramowa oferta usług dostępowych w sieci NGA**. Dzięki ofercie operatorzy alternatywni będą mogli w odpowiednim czasie podjąć decyzje o sposobie działania w zmienionych warunkach konkurencyjnych i przeprowadzić w razie potrzeby niezbędne inwestycje dostosowawcze. Przewaga jaką uzyskuje operator dominujący uruchamiając jako pierwszy usługi w sieci FTTH może być zniwelowana obowiązkiem wyprzedzającego zaoferowania usług hurtowych, co pozbawi go przewagi czasowej pozwalającej na opanowanie rynku. Wyprzedzenie oferty hurtowej w stosunku do oferty detalicznej powinno wynosić zdaniem Komisji 6 miesięcy. Oferta hurtowa powinna zawierać wszystkie gwarancje jakościowe i udogodnienia podwyższające walory oferty detalicznej opartej na FTTH.

Wszelkie **zamiary wycofania usług hurtowych** powinny być zgłaszane regulatorowi z odpowiednim wyprzedzeniem, a następnie przekazywane zainteresowanym operatorom korzystającym. Regulator powinien określić szczegółowe warunki i terminy przekazywania informacji niezbędnych do prowadzenia regulacji w środowisku sieci NGA.

Ustalanie wymagań inwestycyjnych

Działalność regulatora w sprawach sieci NGA nie może się ograniczać do reagowania na zmiany sytuacji konkurencyjnej wywołane inwestycjami. Inwestycje operatorów alternatywnych są wyni-

kiem ich swobodnej decyzji, natomiast w przypadku inwestycji operatora dominującego krajowe organy regulacyjne powinny formułować warunki dotyczące nowej infrastruktury, od których uzależniona jest konkurencyjność rynku. Szczegółowe zalecenia dotyczące takich warunków wypracowano w sprawie dostępu do infrastruktury (kanalizacji, studni, kabli), dostępu do segmentu końcowego sieci FTTH oraz dostępu do całej pętli światłowodowej FTTH.

Obiekty **nowej infrastruktury** powinny być przygotowane do obsługi operatorów alternatywnych doprowadzających swoje światłowody do punktów dostępu [11, pkt 15]. Regulator powinien zachęcać, a jeżeli pozwala na to prawo krajowe, wymusić na operatorze dominującym budowę infrastruktury o większej pojemności niż wynoszą potrzeby tego operatora. Nadwyżkowa pojemność infrastruktury ma być przeznaczona dla operatorów alternatywnych.

Zakłada się, że powielanie segmentu końcowego linii światłowodowej będzie nieefektywne. Skutkiem takiego założenia są **wymagania dotyczące segmentu końcowego**. Warunek podstawowy dotyczy zapewnienia dostępu do segmentu końcowego włącznie z okablowaniem budynkowym. Dostęp do segmentu końcowego powinien być zapewniany w takim punkcie dystrybucyjnym, aby operator alternatywny doprowadzając swoją infrastrukturę do tego punktu mógł uzyskać minimalną skalę efektywności pozwalającą na skuteczną i zrównoważoną konkurencję. Jest to uzależnione od liczby użytkowników końcowych obsługiwanych przez punkt dystrybucyjny. Wpływ na lokalizację punktów dystrybucyjnych mieści się zatem w zakresie oddziaływania regulatora na decyzje podejmowane w sprawach inwestycyjnych.

Najdalej pod względem obciążeń inwestycyjnych idzie **wymóg stosowania światłowodu wielowłóknowego** w segmencie końcowym. W ocenie Komisji nieco podwyższy to koszty inwestycji, ale umożliwi trwałą konkurencję dzięki zapewnieniu kilku operatorom możliwości równoległego dostępu do użytkownika przez segment końcowy [11, pkt 19]. Wymusza to nakłady inwestycyjne przekraczające potrzeby inwestora, dlatego rozwiązanie to uzależnia się od dopuszczalności takiego obowiązku w świetle prawa krajowego. Rozłożenie ciężaru finansowego instalowania kabli wielowłóknowych może również nastąpić w wyniku wspólnych inwestycji operatorów w sieci NGA. W tej sprawie regulator może jedynie oferować swoje wsparcie dla współpracy operatorów, nie może zaś takiego współdziałania wymuszać.

Jeżeli operator realizuje inwestycję FTTH należy go zobowiązać do **uwolnienia światłowodowych linii abonenckich**. Obowiązek ten należy stosować niezależnie od architektury sieci i technologii stosowanej przez operatora. Rezygnacja z tego wymogu może nastąpić tylko w przypadku stwierdzenia skutecznej konkurencji na odpowiednim rynku detalicznym. Jeżeli operator nie realizuje wariantu punkt – punkt, wówczas może być zmuszony do zastosowania technologii zwielokrotnienia długości fali lub innego równoważnego rozwiązania w celu umożliwienia operatorowi alternatywnemu dotarcia do użytkownika końcowego.

Dostęp powinien być udzielany w najbardziej dogodnym dla konkurentów punkcie sieci, którym z reguły jest obszarowy punkt dystrybucyjny. Ze względu na możliwość różnej architektury sieci regulator powinien ustalać **minimalne warunki dostępu**, jakie operator dominujący powinien uwzględnić w swojej ofercie ramowej. Regulator nie może narzucić inwestorowi wyboru pomiędzy wariantem sieci punkt – punkt oraz punkt – wiele punktów, choć wybór wariantu jest istotny dla warunków konkurencji. Decydując się na konfigurację punkt – wiele punktów operator dominujący musi rozwiązać problem przestrzeni kolokacyjnej w punktach koncentracji oraz usług umożliwiających operatorom alternatywnym dotarcie do punktu koncentracji z linią dosyłową. Regulator powinien w każdej sytuacji egzekwować warunki dostępu najbardziej zbliżone do fizycznego uwolnienia linii światłowodowej, zapewniając w najwyższym możliwym stopniu równoważność tych rozwiązań

z usługą uwolnionej pętli lokalnej. Dla operatora dominującego może to oznaczać konieczność zastosowania nowych technik służących uwolnieniu linii. Zatem dokonując wyboru wariantu inwestycyjnego operator powinien mieć świadomość konsekwencji, jakie będą towarzyszyć wykonywaniu obowiązku zapewnienia dostępu do linii abonenckiej w warunkach zastosowanej architektury sieci. Regulator może zachęcać operatorów do wspólnych inwestycji w wielowłóknowe sieci punkt – punkt perspektywą wycofania obowiązku udostępniania linii abonenckiej, jeżeli wspólna inwestycja zapewni im i pozostałym konkurentom równoprawne warunki korzystania z linii światłowodowej.

W przypadku realizacji wariantów FTTC i FTTB konieczne jest nałożenie na operatora dominującego obowiązku **uwolnienia podpętli miedzianych** oraz zapewnienia odpowiednich usług dosyłowych, umożliwiających operatorom alternatywnym dotarcie do punktu dystrybucyjnego ze swoją siecią. W tym wariancie operatorzy alternatywni muszą mieć możliwość korzystania z przestrzeni kolokacyjnej w szafce lub w budynku, albo z innych równoważnych rozwiązań. Uwolnienie podpętli, od szafki do użytkownika końcowego, jest jednak uzależnione od planów inwestycyjnych operatorów alternatywnych. Dlatego nie zaleca się automatyzmu w nakładaniu obowiązku uwolnienia tego ogniwa. Nałożenie obowiązku przystosowania szafek do dostępu operatorów alternatywnych powinno być poprzedzone konsultacjami na temat zainteresowania rynku taką usługą oraz skutków finansowych przystosowania szafek. Stwierdzenie potrzeby zapewnienia takiego punktu dostępu prowadzi do rozstrzygnięć w sprawie minimalnych wymagań na szafki, umożliwiających kolokację urządzeń innych operatorów.

Wszystkie wymagania dotyczące zapewnienia punktów dostępu na określonych poziomach sieci muszą być zabezpieczone przez regulatora środkami umożliwiającymi operatorom alternatywnym dotarcie ze swoją siecią do wyznaczonych punktów dystrybucyjnych i **dosyłanie sygnału** (linie dzierżawione, ciemne światłowody, kable, kanalizacja).

Zalecenia Komisji dotyczące uwolnienia segmentu końcowego linii światłowodowej muszą dopiero znaleźć potwierdzenie dotyczące ekonomicznej wykonalności tego scenariusza. W przypadku, gdyby potwierdziły się obawy o brak ekonomicznych warunków inwestowania przez operatorów alternatywnych w dostęp do segmentu końcowego i podpętli miedzianej, rozwiązaniem zastępczym może się okazać usługa strumienia bitów. Scenariusz ten przewidywała ERG zapowiadając wzrost znaczenia usługi strumienia bitów w warunkach ekonomicznych i technologicznych sieci NGA [7, s. 50]. Nastąpi wówczas odsunięcie infrastruktury operatora alternatywnego od użytkownika końcowego, co będzie krokiem w dół drabiny inwestycyjnej. Nie można wykluczyć, że równocześnie z przesuwaniem przez operatora dominującego zakończenia światłowodu w kierunku użytkownika końcowego, operatorzy alternatywni chcąc utrzymać udział w rynku i obsługę dotychczasowych klientów, będą odsuwać swoją infrastrukturę coraz bardziej od klienta i przejmować jego ruch na wyższych poziomach sieci [10, s. 422].

Regulacja opłat hurtowych

Główna koncepcja regulacji opłat za usługi dostępowe w sieci NGA jest związana z uwzględnieniem w opłatach **poziomu ryzyka** podejmowanego przez inwestora. Ryzyko to zwiększa się wraz z zanikaniem w inwestycji elementu modernizacyjnego, a narastaniem czynników zmiany generacji dostępu. Inwestycje w elementy światłowodowe, które nie prowadzą do zasadniczej zmiany charakterystyki usług, powinny być traktowane pod względem poziomu ryzyka tak jak istniejąca infrastruktura miedziana [11, pkt 14].

Opłaty hurtowe powinny być nadal zorientowane kosztowo. Komisja różnicuje jednak zasady ustalania opłat za dostęp do infrastruktury technicznej, za dostęp do segmentu końcowego w sieci FTTH,

do uwolnionej pętli światłowodowej oraz za dostęp do podpętli miedzianej w sieci hybrydowej. Zastosowanie sieci FTTH wiąże się z najwyższym ryzykiem, ze względu na wysokie koszty tego rozwiązania przypadające na każde zakończenie sieci. Komisja wymaga szacowania różnych ryzyk, w szczególności ryzyka dotyczącego popytu hurtowego i detalicznego, kosztów prac, niepewności technologicznej, poziomu konkurencyjności rynku i niepewności makroekonomicznej. Zaleca się uwzględnienie wyższego poziomu ryzyka wariantu FTTH w koszcie kapitału operatora.

Rozpraszanie ryzyka inwestycyjnego w fazie przygotowania inwestycji poprzez długoterminowe umowy sprzedaży usług lub transakcje dotyczące znacznych przepływności powiązane z rabatami może prowadzić do obniżenia poziomu opłat dla operatorów podejmujących takie zobowiązania. Zmniejszają one ryzyko inwestora związane z liniami nieaktywnymi, ale prowadzą do dyferencjacji opłat, co może powodować kolizję z obowiązkiem niedyskryminacji. Z obawy przed takim blokującym efektem obowiązku niedyskryminacji Komisja wyraźnie dopuszcza różnicowanie opłat hurtowych w wyniku przejęcia części ryzyka inwestycyjnego przez innych operatorów, zastrzegając jednak konieczność zachowania wystarczającej marży dla wszystkich nabywców hurtowych [11, pkt 25].

Metodę orientacji kosztowej można uzależnić od tego, czy zasoby objęte obowiązkiem udostępnienia nadają się do powielenia, czy też jest to niewykonalne z punktu widzenia ekonomicznego. Można również różnicować parametry kalkulacji kosztów (np. koszt kapitału) dla tych dwóch kategorii zasobów. W zaleceniach Komisji widać jednak skłonność do **odchodzenia od kosztowej orientacji opłat** w miarę poprawy konkurencyjności rynku. Narastanie konkurencji na detalicznych rynkach usług szerokopasmowych powinno uzasadniać szersze stosowanie zasady „cena detaliczna minus", z zachowaniem odpowiednich różnic pomiędzy opłatami za poszczególne usługi hurtowe. Również inne efektywne rozwiązania regulacyjne, w szczególności zastosowanie rozdziału funkcjonalnego może prowadzić do rezygnacji z ustalania opłat na podstawie orientacji kosztowej i ograniczenia kontroli opłat do testu zawężenia marży.

Warunki wycofywania regulacji

Inwestycje w sieci NGA mogą prowadzić do tak istotnej zmiany warunków konkurencji na rynku, że uzasadnione będzie **ograniczenie lub wycofanie obowiązków regulacyjnych** na niektórych poziomach drabiny inwestycyjnej lub na niektórych rynkach. Generalna zasada interwencji regulatora przewiduje wprowadzanie konkurencji na jak najniższych poziomach infrastruktury i sieci, w szczególności na poziomie dostępu fizycznego. Udane wprowadzenie obowiązków dostępowych na poziomie fizycznym (linia abonencka) może prowadzić do ograniczenia lub zniesienia obowiązków dotyczących usług dostępu szerokopasmowego. Regulator może to jednak uzależnić od zastosowania wariantu punkt – punkt, jako najbardziej prokonkurencyjnego rozwiązania FTTH. Ograniczenie regulacji może polegać na utrzymaniu obowiązku świadczenia usług dostępu szerokopasmowego, przy jednoczesnym wycofaniu kosztowej kontroli opłat hurtowych za te usługi, pod warunkiem zastosowania testów zawężenia marży. Ograniczenie lub wycofanie regulacji może być również następstwem wspólnej inwestycji operatorów w sieć NGA. Zaleca się, aby uwzględnić w takim przypadku liczbę zaangażowanych operatorów i warunki współdziałania.

Problem zestawu usług hurtowych niezbędnych do podtrzymania i rozwoju konkurencji komplikuje się w okresie przechodzenia od sieci miedzianej do sieci światłowodowej. Zakłada się okres współistnienia obydwu infrastruktur (*Overlay*) oraz fazę substytucji. W fazie współistnienia sieć miedziana będzie nadal wykorzystywana przez operatorów alternatywnych. W **fazie substytucji** sieć miedziana będzie usuwana, a operatorzy alternatywni będą przenosić się do nowych punktów dostępu. Zaprojektowanie uniwersalnych rozwiązań usługowych w tym okresie jest w zasadzie niemożliwe,

ze względu na niepowtarzalność przedsięwzięć migracyjnych. Dlatego Komisja zaleca w tym przypadku rozwiązania typu negocjacyjno-procesowego polegające na współpracy między dysponentem sieci i operatorami alternatywnymi. Współpraca ta powinna prowadzić w miarę możliwości do wypracowania **uzgodnionych rozwiązań**. Wymagania dostępowe dotyczące sieci miedzianej pozostawałyby w mocy do czasu osiągnięcia porozumienia między operatorem dominującym i operatorami alternatywnymi korzystającymi z usług w sieci miedzianej. W razie braku porozumienia co do ścieżki produktowej i czasowej takiej migracji należy ustalić obowiązkowy **okres przejściowy**, w którym wcześniejsze usługi będą kontynuowane. Okres ten powinien być dostosowany do standardowego okresu inwestycyjnego dla uwolnionych pętli lokalnych w wymiarze około 5 lat. Jego skrócenie jest możliwe w przypadku zapewnienia w pełni równoważnego dostępu na poziomie przełącznicy głównej.

Szczególny przypadek wycofania wymagań regulacyjnych wystąpi na obszarach objętych nowymi inwestycjami w sieci FTTH, na których brak jest sieci miedzianej. Operator nie jest zobowiązany na tych obszarach do spełnienia wymagań związanych z usługami detalicznymi, w szczególności z usługami powszechnymi, realizowanymi za pomocą miedzianej sieci telefonicznej (usługa faksowa, komutowany dostęp do internetu). Wprowadzając sieć światłowodową na takim obszarze operator jest uprawniony do zaoferowania równoważnych usług, realizowanych za pomocą innych technologii.

Podsumowanie

Projektowanie polityki regulacyjnej w sprawach sieci NGA to proces oparty na rozstrzygnięciach unijnych, ale uwarunkowany sytuacją krajowego sektora telekomunikacyjnego. Krajowa polityka regulacyjna powinna być dostosowana do wariantu inwestycyjnego przyjętego przez operatora zasiedziałego, gdyż przygotowanie uniwersalnej koncepcji uwzględniającej wszystkie znane rozwiązania jest mało realistyczne. Ze względu na współzależność decyzji inwestycyjnych i regulacyjnych konieczne jest zapewnienie warunków do wymiany informacji między inwestorami i organem regulacyjnym, co zapewni z jednej strony stabilność regulacyjną, z drugiej zaś przewidywalność działań inwestycyjnych operatora zasiedziałego. Próba utrzymania zakresu i intensywności regulacji dotyczących sieci miedzianej w odniesieniu do sieci światłowodowych NGA będzie blokować większe inwestycje w te sieci.

W warunkach krajowych uzasadnione jest przygotowanie odrębnych warunków regulacyjnych dla przyjętego wariantu modernizacji sieci miedzianych oraz dla nowych, w pełni światłowodowych sieci dostępowych. W przypadku sieci FTTH regulacja powinna być ograniczona do dostępu fizycznego (kanalizacja, ciemne światłowody), oparta w jak najszerszym zakresie na zasadzie symetrii, ewentualna zaś kontrola opłat hurtowych musi uwzględniać zwiększone ryzyko ponoszone przez inwestora. W przypadku modernizowanych sieci światłowodowo-miedzianych utrzymanie dalej idących środków regulacyjnych jest uzasadnione dokonanymi już inwestycjami operatorów alternatywnych i niewątpliwą substytucyjnością usług świadczonych przed i po modernizacji. W sprawach sieci NGA regulator powinien w maksymalnym stopniu wykorzystać niedawno uzyskany instrument w postaci porozumienia regulacyjnego.

Bibliografia

[1] BEREC 2010. *Next generation access – implementation issues and wholesale products*. Berec Report, marzec 2010, BoR (10) 08

[2] Bijl P. de, Peitz P.: *Innovation, convergence and the role of regulation in the Netherlands and beyond.* Telecommunications Policy, 2008, nr 32

[3] Borzycki K.: *Światłowodowe sieci dostępowe.* Telekomunikacja i Techniki Informacyjne, 2008, nr 1-2

[4] Cave M.: *Snakes and ladders: Unbundling in a next generation world.* Telecommunications Policy, 2010, nr 34

[5] Elixmann D., Ilic D., Neumann K.-H., Plueckebaum T.: *The economics of next generation access – final report*. WIK Consult, wrzesień 2008

[6] Elixmann D., Kuehling J., Markus S., Neumann K.-H., Plueckebaum T., Vogelsang I.: *Anforderungen der Next Generation Networks an Politik und Regulierung*. WIK Consult, kwiecień 2008

[7] ERG 2007. *ERG opinion on regulatory principles of NGA*. ERG (07) 16rev2, www. erg.eu.int/documents/docs/index_en.htm

[8] ERG 2009. *Report on next generation access – economic analysis and regulatory principles*. (09) 17, czerwiec 2009

[9] Gavosto A., Ponte G., Scaglioni C.: *Investment in next generation networks and the role of regulation: a real option approach.* School of Economics and Management, Technical University of Lisbon, Working Papers WP 031/2007/DE

[10] Helmesl P., Schoof J., Geppert M.: *Herausforderungen der ALL-IP-Netzmigration: zur Balance zwischen Effizienzgewinn und Migrationsnachteilen.* Computer und Recht, 2008, nr 7

[11] Komisja 2010. *Zalecenie z dnia 20 września 2010 r. w sprawie regulowanego dostępu do sieci dostępu nowej generacji.* C(2010) 6223

[12] Marcus J.S., Elixmann D.: *Regulatory approaches to NGNs: an international comparison.* Communications & Strategies, 2008, nr 69(1)

[13] Michalski W.: *Strategie migracji sieci telekomunikacyjnych w kierunku sieci NGN w wybranych krajach.* Telekomunikacja i Techniki Informacyjne, 2008, nr 1-2, s. 51-57

[14] UKE 2008. *Opinia regulatora dotycząca procesu budowania i eksploatacji infrastruktury NGA w Polsce*. Warszawa, 17 grudnia 2008, www.uke.gov.pl

Stanisław Piątek

Dr hab. Stanisław Piątek (1951) – absolwent Wydziału Prawa i Administracji Uniwersytetu Warszawskiego (1973), pracownik naukowo-dydaktyczny Uniwersytetu Warszawskiego (od 1973), wykładowca akademicki i profesor Wydziału Zarządzania Uniwersytetu Warszawskiego; konsultant Krajowej Rady Radiofonii i Telewizji (1993–2000) oraz Urzędu Regulacji Telekomunikacji i Poczty (2001–2005); członek Krajowej Komisji Uwłaszczeniowej (1991–1998) oraz Rady Legislacyjnej (1998–2001); autor 120 publikacji krajowych i zagranicznych; zainteresowania naukowe: regulacja działalności infrastrukturalnej, ekonomiczne skutki regulacji.

e-mail: piatek@supermedia.pl

Systemy InHousePLC – charakterystyka ogólna, kierunki rozwoju i zastosowań

Henryk Gut-Mostowy

W artykule zamieszczono charakterystykę ogólną współczesnych systemów łączności elektronicznej opartych na technologii InHousePLC. Omówiono elementy składowe tych systemów, używane medium transmisyjne i wykorzystywane zakresy częstotliwości, a także stosowane metody modulacji i protokoły komunikacyjne warstwy drugiej. Scharakteryzowano zagadnienia kompatybilności elektromagnetycznej, przedstawiono głównych dostawców urządzeń składowych, a także nakreślono kierunki dalszego rozwoju i zastosowań tych systemów.

systemy BPLC, systemy InHousePLC, domowe sieci multimedialne, inteligentne budynki

Wprowadzenie

Jednym z podstawowych warunków funkcjonowania społeczeństwa informacyjnego z gospodarką opartą na wiedzy jest dobrze rozwinięta infrastruktura szerokopasmowej abonenckiej sieci dostępowej. W aglomeracjach wielkomiejskich sieci te realizują obecnie zarówno operatorzy PSTN (*Public Swiched Telephone Network*), dysponujący w obszarze abonenckim parami przewodów miedzianych oraz włóknami światłowodowymi, jak i operatorzy sieci telewizji kablowej. Sieci te są tam rozwijane przy wykorzystaniu istniejących kabli miedzianych z zastosowaniem technik transmisyjnych xDSL (*x Digital Subscriber Line*) [1], [17], [20], kabli światłowodowych z użyciem technik FITL (*Fiber in The Loop*) [30] lub sieci CATV (*Cable TV*) opartych na technice HFC (*Hybrid Fibre - Coaxial*) [18]. Zapewnienie usług teleinformatycznych w obszarach wielkomiejskich nie stanowi zatem istotnego problemu. Inaczej sprawa wygląda w regionach o słabo rozwiniętej infrastrukturze telekomunikacyjnej. Wprowadzanie usług informatycznych w tych obszarach, to nie kwestia wyboru optymalnej techniki transmisyjnej (xDSL, FITL, HFC), lecz przede wszystkim problem braku medium transmisyjnego dla którejkolwiek z nich. Jednym ze sposobów szybkiego i taniego rozwiązania tego problemu jest wykorzystanie, powszechnie tam występujących, linii energetycznych niskiego napięcia jako medium transmisyjnego i użycie szerokopasmowych systemów dostępowych BPLC (*Broadband Power Line Communications*) [4÷9], [11], [19], [23].

W początkowym okresie (lata dziewięćdziesiąte XX wieku) systemy BPLC były rozwijane głównie jako systemy dostępowe z tzw. jednostopniową komunikacją BPLC [6], [9], [19]. Jako medium transmisyjne wykorzystywano jedynie obszar zewnętrznej sieci energetycznej, obejmujący linie magistralne, przyłącza oraz część wewnętrznych linii zasilających (od przyłącza do bezpieczników głównych). W tym obszarze sieci transmisja sygnałów BPLC odbywała się w paśmie częstotliwości od 1,0 do 10,0 MHz. W obszarze budynku zaś lub mieszkania prowadzono oddzielną instalację telekomunikacyjną kablami informatycznymi lub koncentrycznymi.

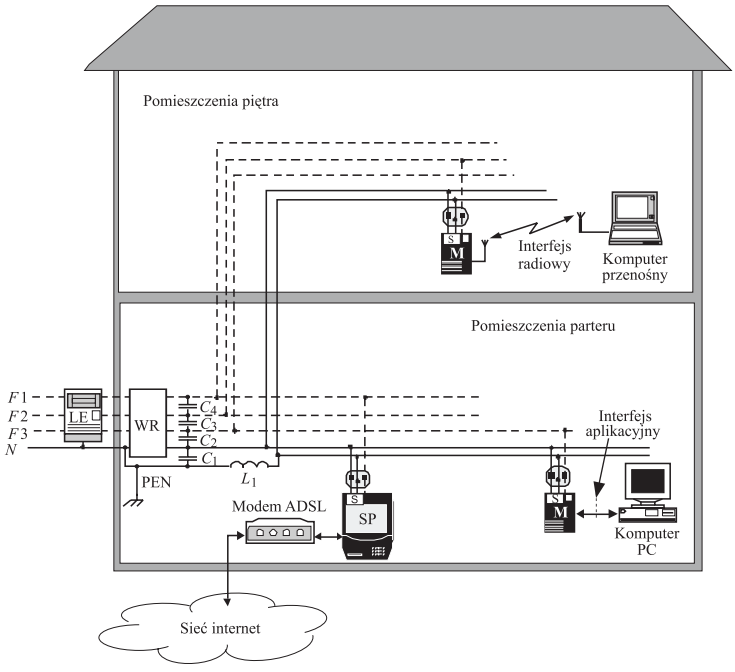
Problemy z zasięgiem i kompatybilnością elektromagnetyczną pierwszych zastosowań BPLC sprawiły, że na początku XXI wieku zaczęto stosować nowe architektury systemów dostępowych po liniach energetycznych z tzw. komunikacją dwustopniową BPLC. W systemach tej klasy wykorzystuje się zarówno płaszczyznę zewnętrzną, jak i wewnętrzną sieci energetycznej, a do transmisji sygnałów uży-

wa się dwóch zakresów częstotliwości. Pasmo od 1,0 do 10,0 MHz w obszarze zewnętrznej sieci energetycznej, natomiast w obszarze sieci wewnątrzbudynkowej od 10 do 30 MHz. Systemy tej klasy, ze względu na sposób dołączania urządzeń końcowych abonenta (modemów BPLC), określane są często jako *internet w gniazdku energetycznym*. Taką architekturę sieciową ma np. system E-PLC SD V1 szwajcarskiej firmy *Ascom*, czy też system PLUS izraelskiej firmy *MainNet Communications*.

Obecnie w systemach z komunikacją dwustopniową BPLC szczególnie dynamicznie rozwija się warstwa komunikacji wewnątrzbudynkowej, tzw. komunikacji *InHousePLC*. W krajach rozwiniętych (USA, Japonia, kraje UE) jest ona wykorzystywana do tworzenia platformy komunikacyjnej mieszkaniowych (domowych) sieci komputerowych, czy też systemów multimedialnych w tzw. inteligentnych budynkach nowej generacji. Jako wygodna i tania platforma komunikacyjna, integrująca dostęp szerokopasmowy do sieci internet w budynkach wielorodzinnych, blokach mieszkalnych, czy też obiektach użyteczności publicznej, warstwa ta stanowi także przedmiot rozważań tego artykułu.

Elementy konstrukcyjne i zasada działania

Obecnie wiele czołowych firm telekomunikacyjnych świata pracuje nad ciągłym udoskonalaniem systemów *InHousePLC* . Różnorodne rozwiązania tych systemów są oparte na trzech elementach składowych: sprzęgaczu, stacji pośredniczącej i module komunikacyjnym, połączonych w sposób pokazany przykładowo na rys. 1. Linią ciągłą zaznaczono tor przesyłania sygnałów w.cz. między elementami systemu (modemy, stacja pośrednicząca), linią przerywaną zaś obwody fazowe instalacji wewnątrzbudynkowej do zasilania tych elementów. Elementy reaktancyjne: L_1, $C_1 \div C_4$ tworzą filtr górnozaporowy, blokujący przenikanie sygnałów w.cz. do zewnętrznej sieci energetycznej



Rys. 1. *Architektura systemów InHousePLC. Oznaczenia: F1, F2, F3 – przewody fazowe, LE – licznik energii elektrycznej, M – moduł komunikacyjny (modem PLC), N – przewód neutralny (wspólna ziemia sygnałowa), PEN – przewód ziemi ochronnej, S – sprzęgacz, SP – stacja pośrednicząca (ruter PLC), WR – wyłącznik różnicowy*

Sprzęgacz jest układem złożonym z filtru biernego górnoprzepustowego, transformatora oraz elementów zabezpieczających przed przepięciami i/lub przetężeniami, powstającymi w instalacji elektrycznej mieszkania lub budynku. Zapewnia on częstotliwościową separację układów nadawczo-odbiorczych stacji pośredniczącej i modemów PLC od obwodów instalacji elektrycznej, a także sprzężenie tych układów z przewodami, które tworzą tor transmisyjny systemu. Zastosowane dwa filtry (górno- i środkowoprzepustowy) oraz transformator o dobranej transmitancji, gwarantują efektywne sprzężenie z jednoczesnym dopasowaniem impedancyjnym jedynie w zakresie częstotliwości roboczych systemów *InHousePLC*. Poza tym zakresem tłumienność sprzęgacza wynosi ok. 60 dB. W podkładowej instalacji elektrycznej sprzęgacze wydzielają zatem podkładowy kanał telekomunikacyjny z pasmem od 10 do 30 MHz, który jest wykorzystywany jedynie do transmisji sygnałów PLC. Charakteryzuje się on zmniejszonym poziomem zakłóceń wytwarzanych przez domowe urządzenia elektryczne. Zasadnicza część energii tych zakłóceń (ok. 90 %) jest bowiem skoncentrowana w zakresie pasma zaporowego filtru górnoprzepustowego sprzęgacza (poniżej 1 MHz).

Stacja pośrednicząca, zwana także ruterem PLC, będąca głównym elementem systemów *InHousePLC*, jest na ogół dołączana do gniazda energetycznego, znajdującego się najbliżej licznika energii elektrycznej, lub w pobliżu modemu dostępowego, stanowiącego port wyjściowy do sieci *WWW*. Nie są normalnie wyznaczone miejsca lokalizacji tej stacji, jednak ze względu na to, że miejsce przyłączenia stacji do torów transmisyjnych domeny komunikacyjnej *InHousePLC* zmienia topologię tej domeny, wydaje się najlepszy wybór gniazda, przy którym uzyskuje się największą przepływność binarną w domenie[①]. Można tego dokonać metodą „prób i błędów" lub za pomocą stosunkowo taniego zestawu instalacyjnego, złożonego z nadajnika i odbiornika testowego systemu. W strukturze funkcjonalnej systemu *InHousePLC*, stacja pośrednicząca wykonuje funkcje węzła pośredniczącego, obsługującego jedynie ten ruch informatyczny przychodzący z sieci zewnętrznej, który jest kierowany do modemów PLC z obsługiwanej przez nią domeny komunikacyjnej, a także ten ruch od modemów PLC własnej domeny, który jest kierowany do sieci zewnętrznej. Komunikacja między modemami PLC w ramach domeny nadzorowanej przez stację pośredniczącą odbywa się bez udziału tej stacji. Inaczej mówiąc, stacja ta pełni funkcję „pomostu" między zewnętrzną siecią telekomunikacyjną a domową siecią LAN z warstwą fizyczną opartą na technologii *InHousePLC*.

Moduł komunikacyjny, zwany także modemem PLC, tak jak i stacja pośrednicząca, może być dołączony do dowolnego gniazda instalacji elektrycznej mieszkania lub budynku. Jest on sprzężony z torem transmisyjnym domeny komunikacyjnej PLC za pośrednictwem sprzęgacza, wbudowanego na ogół w ten moduł. Od strony interfejsu aplikacyjnego jest on zwykle wyposażony w złącze interfejsu transmisji danych (USB, lub 10/100BaseT), chociaż znane są rozwiązania z interfejsem radiowym typu *Bluetooth*. W niektórych systemach jest specjalne złącze interfejsu do dołączenia liczników zużycia energii elektrycznej, gazu oraz wody, a także urządzeń sygnalizacji alarmowej, czy też urządzeń wyposażenia inteligentnego domu.

W strukturze funkcjonalnej systemów *InHousePLC*, na ogół, moduł komunikacyjny ma wbudowane funkcje dwóch najniższych warstw (fizycznej i łącza danych) zastosowanego protokołu komunikacyjnego. Wiadomości dyskretne odbierane na interfejsie aplikacyjnym modułu z urządzenia terminalowego (np. komputera PC) są zamieniane na sekwencje odpowiednio uformowanych ramek, które są przekształcane na ciąg sygnałów symbolowych odpowiedniej modulacji i wprowadzane do toru transmisyjnego domeny komunikacyjnej PLC w sposób określony przez podwarstwę MAC (*Medium Access Control*) zastosowanego protokołu komunikacyjnego. W przeciwnym kierunku transmisji, sygnały

① *Chodzi o taką lokalizację, przy której jest uzyskiwana maksymalna średnia arytmetyczna przepływności binarnych od stacji pośredniczącej do poszczególnych gniazdek sieciowych (i na odwrót), w których mogą być instalowane modemy InHousePLC.*

symbolowe modulacji odbierane z toru transmisyjnego domeny są najpierw poddawane procesom demodulacji i detekcji, w wyniku czego są przekształcane na sekwencje ramek zastosowanego protokołu komunikacyjnego. Zdekodowane ramki są następnie analizowane pod kątem zgodności części adresowej z adresem MAC modemu. Jeśli jest taka zgodność, poddawane są one dalszemu przetwarzaniu (deszyfracja, składanie[①], detekcja i korekcja błędów) i są przekształcane na wiadomości dyskretne, wyprowadzane na interfejs aplikacyjny modemu w postaci zgodnej z formatem danego interfejsu. W przypadku przeciwnym zdekodowane ramki są odrzucane przez warstwę łącza danych modemu.

Medium transmisyjne i wykorzystywane pasma częstotliwości

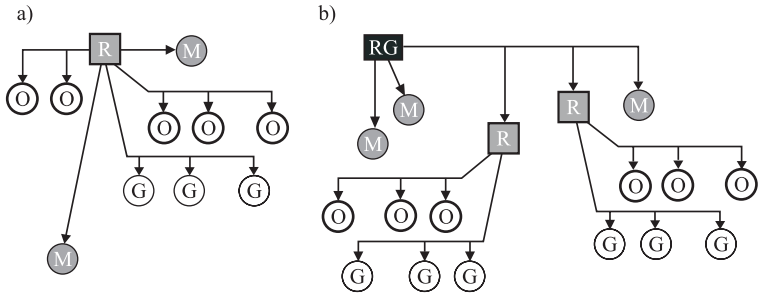
W systemach *InHousePLC* jako medium transmisyjne są wykorzystywane fragmenty domowych lub mieszkaniowych instalacji elektrycznych, a mówiąc ściślej – obwody zasilania gniazdek energetycznych w tych instalacjach. W instalacjach elektrycznych wykonanych zgodnie z obowiązującymi normami europejskimi i krajowymi, w obwodach tych są prowadzone trzy przewody: przewód fazowy F, neutralny N oraz przewód uziemienia ochronnego PE. Dysponując trzema przewodami, można utworzyć trzy różne tory transmisyjne do przesyłania sygnałów roboczych systemu. Jednak praktycznie tory takie mogą tworzyć jedynie pary przewodów: F-N lub N-PE, ponieważ kombinacja F-PE jest niedozwolona ze względów bezpieczeństwa. W pierwszych rozwiązaniach *InHousePLC* medium transmisyjne tworzono powszechnie na parze przewodów F-N. Jednak w [11] wykazano, że dużo lepszym rozwiązaniem jest stosowanie pary przewodów N-PE zarówno ze względu na niższy poziom emisji radiowych od sygnałów PLC, jak i mniejszy poziom szumu i zakłóceń wprowadzanych do tak utworzonego toru transmisyjnego przez urządzenia elektryczne zasilane z obwodów F-N.

Na ogół, obecne instalacje elektryczne wewnątrzbudynkowe są tworzone z przewodów instalacyjnych, zawierających trzy izolowane żyły miedziane, prowadzone równolegle w powłoce z tworzywa sztucznego. Średnica tych żył zależy od przeznaczenia fragmentu instalacji i może wynosić od 1,0 do 3,5 mm. Tory transmisyjne tworzone przy wykorzystaniu takich instalacji charakteryzują się strukturą odcinkami jednorodną, co jest bardzo ważne, i stosunkowo dobrymi właściwościami transmisyjnymi w zakresie częstotliwości roboczych systemów *InHousePLC*. Jednak te same tory przesyłowe, wydzielone w instalacjach elektrycznych występujących w budynkach starszych, mają dużo gorsze parametry transmisyjne. Instalacje te nie są bowiem utworzone z miedzianych przewodów instalacyjnych, lecz z oddzielnych żył (często aluminiowych i to nie trzech, a tylko dwóch), z izolacją papierową, które są prowadzone w rurkach instalacyjnych, bez zachowania jakiejkolwiek geometrii toru transmisyjnego.

Instalacje elektryczne (wykorzystywane przez systemy *InHousePLC* jako medium transmisyjne) są projektowane i wykonywane przede wszystkim pod kątem optymalnej dystrybucji energii elektrycznej prądu przemiennego małej częstotliwości (50 Hz) i dużej mocy, a nie w celu przesyłania w nich sygnałów wielkiej częstotliwości. Instalacje te bywają różnie wykonane zarówno w sensie topologicznym, jak i konstrukcyjnym. Zdecydowanie inną strukturę mają instalacje w mieszkaniach niż w budynkach jednorodzinnych, czy wielorodzinnych. Ze względu na minimalizację strat energii elektrycznej i niezawodność systemu zasilania, jako generalną zasadę stosuje się rozdzielanie obwodów zasilających gniazda od obwodów zasilających punkty oświetlenia, czy też od obwodów zasilających urządzenia o dużym poborze mocy. W zależności od obiektu (mieszkanie lub budynek), obwody te są rozdzielane w jednej lub kilku szafkach rozdzielczych, instalowanych zwykle pośrodku obszarów zasilania. W ogólnym przypadku prowadzi to do instalacji elektrycznej o topologii rozbudowanego drzewa, z gałęziami o strukturze magistrali prostej (rys. 2), do których są dołączane odbiorniki energii elektrycznej (gniazda elektryczne, punkty oświetlenia, obwody ogrzewania itp.).

① *Składanie (ang. de-interleaving) jest operacją odwrotną do operacji przeplotu (ang. interleaving).*

W instalacji elektrycznej o takiej topologii jest tworzony tor transmisyjny (dla sygnałów w.cz. od modemów *InHousePLC*) z licznymi odgałęzieniami. Jeśli tor ten jest na obwodach N-PE, wówczas tylko te odgałęzienia, do których są dołączone modemy są dopasowane do impedancji falowej odgałęzień. Odgałęzienia pozostałe, mimo dołączonych do nich odbiorników energii elektrycznej, reprezentują odcinki toru transmisyjnego rozwarte na końcach. Konsekwencją takiej struktury toru transmisyjnego jest występowanie licznych odbić sygnałów w.cz. zarówno od punktów połączenia odgałęzień z torem magistralnym, jak i od końców tych odgałęzień. Prowadzi to do bardzo dużych zniekształceń charakterystyki amplitudowej i fazowej toru. Jednak, w odróżnieniu od torów transmisyjnych na obwodach N-F, zniekształcenia te nie zmieniają się w czasie i dlatego można je łatwo korygować.



***Rys. 2**. Topologia przykładowej instalacji elektrycznej niskiego napięcia dla: (a) mieszkania, (b) domu jednorodzinnego. Oznaczenia: G – punkt odbioru z gniazdem energetycznym, M – punkt odbioru mocy, O – punkt odbioru oświetlenia, RG – rozdzielnia główna, R – rozdzielnia*

We współczesnych systemach *InHousePLC* do transmisji sygnałów użytkowych jest wykorzystywane pasmo częstotliwości roboczych od 10 do 30 MHz, w zależności od stosowanej metody modulacji, w sposób ciągły lub tylko niektóre jego podzakresy. W sposób ciągły wykorzystuje się gdy w warstwie fizycznej systemów *InHousePLC* do kodowania sygnału cyfrowego zastosowano którąkolwiek z metod modulacji z tzw. rozpraszaniem widma sygnału. Niektóre podzakresy pasma zaś wówczas, gdy w warstwie fizycznej jest stosowana modulacja z ortogonalnym częstotliwościowym zwielokrotnieniem kanałów.

Warstwa fizyczna i łącza danych

W systemach *InHousePLC* warstwą fizyczną są przekazywane sygnały cyfrowe (będące zakodowanymi sygnałami: audio-wideo, danymi binarnymi i/lub sygnałami kontrolno-sterującymi) między komunikującymi się bezpośrednio modemami PLC, od stacji pośredniczącej do tych modemów i na odwrót. W pierwszych rozwiązaniach w warstwie fizycznej stosowano modulacje jednotonowe, takie jak np. binarne kluczowanie częstotliwości z przesunięciem minimalnym i gaussowskim kształtowaniem impulsów GMSK (*Gaussian Minimum Shift Keying*), uzyskując stosunkowo niewielkie przepływności kanału, rzędu pojedynczych megabitów na sekundę. W związku z dynamicznym rozwojem technologii układów ASIC *(Application Specific Integrated Circuit)* o bardzo dużym stopniu integracji, na początku XXI wieku pojawiły się w produkcji masowej układy specjalizowane z kompletną warstwą fizyczną dla systemów *InHousePLC*, opartą na modulacjach szerokopasmowych z rozpraszaniem widma sygnału CDMA (*Code Division Multiply Access*) przez kluczowanie bezpośrednie DS-CDMA (*Direct Sequence*) lub skakanie po częstotliwościach FH-CDMA (*Frequency Hopping*), czy też z ortogonalną modula-

cją wielotonową OFDM (*Orthogonal Frequency Division Multiplex*). Po licznych próbach eksploatacyjnych, jako najbardziej odpowiednie rozwiązanie dla warstwy fizycznej systemów *InHousePLC* uznaje się obecnie modulację OFDM. Wynika to przede wszystkim z adaptacyjnych właściwości tej modulacji zarówno w kontekście wymagań na kompatybilność elektromagnetyczną systemów, jak i możliwości idealnego dopasowywania się do warunków panujących w podkładowym kanale transmisyjnym.

W systemach *InHousPLC*, w warstwie łącza danych przekazywane sygnały cyfrowe są formowane w ramki, które po obróbce kryptograficznej są poddawane kodowaniu korekcyjnemu, operacji przeplotu i kodowaniu liniowemu. Wszystkie te operacje są wykonywane w celu zabezpieczenia transmisji zarówno przed podsłuchem, jak i przed błędami. Różne firmy stosują różne formaty ramek, a także odmienne zasady kryptograficzne i metody zabezpieczania transmisji przed błędami. Tak uformowane ramki są przekazywane przez warstwę fizyczną na drugi koniec kanału ziarnistego. Procesem tego transferu steruje na ogół stacja pośrednicząca. Transmisja przez kanał ziarnisty z reguły jest symetryczną transmisją dupleksową. W zależności od konkretnej implementacji systemu *InHousePLC* jest ona realizowana albo z częstotliwościowym, albo czasowym rozdziałem kierunków transmisji. W systemach stosujących modulację z rozpraszaniem widma, kierunki transmisji są rozdzielane metodą kodową.

Istotnym elementem warstwy łącza protokołu komunikacyjnego stosowanego w systemach *InHousePLC*, w których wspólne medium transmisyjne (instalacja elektryczna mieszkania lub budynku) jest dzielone przez wielu użytkowników, jest podwarstwa MAC. Podwarstwa ta służy do bezkolizyjnego przepływu ramek (w obydwu kierunkach transmisji) między stacją pośrednicząca a modułami komunikacyjnymi, zwanymi także modemami *InHousePLC*. Również i w tym obszarze brak jest jakiejkolwiek normalizacji międzynarodowej. Jednak najczęściej stosuje się tu protokół CSMA CD/CA (*Carrier Sense Multiple Access Collision Detection / Collision Avoidance*) wielodostępu ze śledzeniem fali nośnej oraz wykrywaniem i rozstrzyganiem kolizji lub unikaniem kolizji. Zasada ta jest powszechnie stosowana między innymi w lokalnych sieciach komputerowych LAN (*Local Area Network*), a także w niektórych wcześniejszych systemach z dostępem radiowym. W tym obszarze sieci, ze względu na stosunkowo nieliczną grupę modemów BPLC „walczących" o dostęp do wspólnego medium transmisyjnego, zasada ta funkcjonuje wystarczająco dobrze. Przeniesienie tej zasady do obszaru sieci zewnętrznej jest raczej niewskazane, głównie ze względu na rozmiary tego obszaru i wynikające stąd duże opóźnienia transmisji, skutkujące większym prawdopodobieństwem wystąpienia kolizji i znacznym zmniejszeniem szybkości przekazu danych.

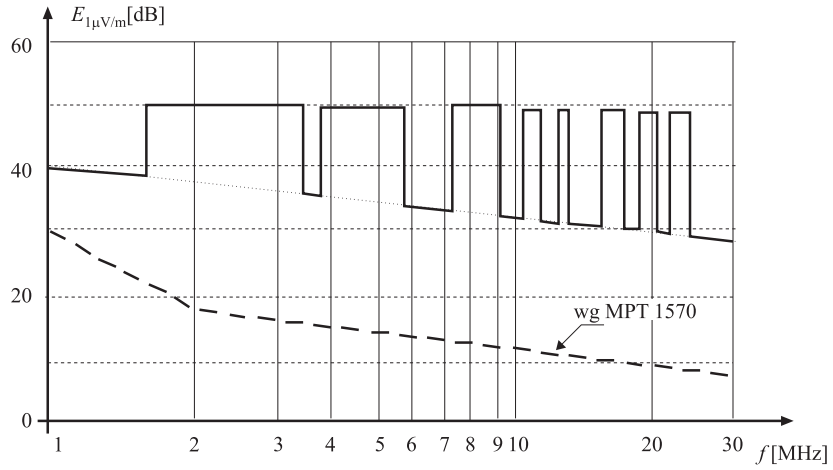
Kompatybilność elektromagnetyczna

We współczesnych systemach *InHousePLC* jest wykorzystywany zakres częstotliwości roboczych, który od dawna jest używany przez różne służby radiowe, takie jak: rozgłośnie radiowe, komunikacja lotnicza i morska, stała i ruchoma służba cywilna oraz wojskowa, a także przez amatorów krótkofalowców. Wobec problemów z kompatybilnością elektromagnetyczną, jakie występowały przy pierwszych zastosowaniach praktycznych techniki PLC, jest zrozumiałe żądanie dotychczasowych użytkowników tego zakresu częstotliwości, aby nowy sposób użytkowania linii energetycznych nie zakłócał dotychczasowej działalności tych służb. Żądanie to musi być respektowane przez producentów systemów *InHousePLC*, gdyż inaczej technika ta, skądinąd atrakcyjna, skazana zostanie na zagładę. Spełnienie tych żądań i bezkonfliktowy rozwój systemów tej klasy jest możliwy przy zachowaniu zasady separacji przestrzennej, albo częstotliwościowej.

Zasada separacji przestrzennej dotyczy ochrony całego pasma częstotliwości radiowych, wykorzystywanego przez systemy *InHousePLC* (10÷30 MHz). Wprowadza ona ograniczenie natężenia pola

elektromagnetycznego, wytwarzanego w odległości 3m od dowolnego punktu instalacji elektrycznej w czasie przesyłania w niej sygnałów PLC [11], [12]. Tymi punktami pomiarowymi mogą być: gniazda zasilania, przewody instalacji elektrycznej, licznik energii elektrycznej, szafka rozdzielcza oraz inne elementy konstrukcyjne wchodzące w skład instalacji elektrycznej wewnątrzobiektowej. Taka zasada separacji jest zdefiniowana między innymi w normie angielskiej MPT1570 *Radiation Limits and Measurement Standard. Electromagnetic radiation from telecommunications systems operating over material substances in the frequency range 9 kHz to 300 MHz* (rys. 3).

Zasada separacji częstotliwościowej zakłada użytkowanie przez systemy *InHousePLC* jedynie tych podzakresów częstotliwości z pasma od 1 do 30 MHz, które nie są wykorzystywane przez istniejące służby radiowe. Jest to tzw. koncepcja kominów, która w tych wolnych podzakresach① częstotliwości dopuszcza występowanie szkodliwej emisji od transmisji PLC, o natężeniu pola elektromagnetycznego ok. 50 dB w stosunku do pola odniesienia o natężeniu 1μV/m, w odległości 3m od instalacji energetycznej przenoszącej sygnały BPLC [11], [12], [14], [15]. Propozycje takich ograniczeń zakłóceń interferencyjnych od systemów PLC pokazano na rys. 3.



Rys. 3. *Dopuszczalne poziomy natężenia pola elektromagnetycznego, występującego w odległości 3m od instalacji elektrycznej w czasie transmisji sygnałów PLC, według zasady separacji częstotliwościowej*

Producenci i asortyment produkcji

Atrakcyjność systemów *InHousePLC* wynika z ich możliwości telekomunikacyjnych, powszechności medium transmisyjnego wykorzystywanego przez te systemy, a także z prostoty ich wdrażania w środowisko sieci energetycznej, porównywalnej z wdrażaniem radiowych systemów dostępowych. Nic więc dziwnego, że nad rozwojem tych systemów, w obszarze sprzętu i oprogramowania, pracuje wiele czołowych firm świata zaangażowanych w wytwarzanie zarówno podzespołów elektronicznych i specjalizowanych układów scalonych do tych systemów, jak i gotowych rozwiązań systemów. Zestawienie wybranych producentów podzespołów elektronicznych do PLC i kompletnych urządzeń systemów *InHousePLC* zamieszczono w tablicach 1 i 2.

① *Ponieważ przedzielane pasma łączności krótkofalowej są różne w różnych krajach świata, dlatego też współczesne modemy InHouse PLC mają wbudowane mechanizmy do automatycznego wykrywania tych zabronionych pasm częstotliwości.*

Tabl. 1. Zestawienie wybranych producentów układów modemowych do systemów InHousePLC

L.p.	Nazwa firmy: adres WWW	Asortyment produkcji
1	***Cogency:*** www.cogency.com	Układy scalone oraz urządzenia zgodne ze standardem *HomePlug 1.0*
2	***DS2:*** www.ds2.es	Układy scalone oraz urządzenia zgodne ze standardem *HomePlug 1.0*
3	***Inari***	Układy scalone do PLC (12 Mbit/s)
4	***Atheros Corp:*** www.atheros.com	Układy scalone oraz urządzenia zgodne ze standardami: *HomePlug 1.0*, *HomePlug 1.0 Turbo*, *HomePlug AV*
5	***ST&T:*** www.stt.com.tw	Układy scalone oraz urządzenia zgodne ze standardami: *HomePlug 1.0*, *HomePlug 1.0 Turbo*, *HomePlug AV*
6	***Yitrancomm:*** www.yitran.com	Układy scalone do PLC (2,5, 24 Mbit/s)

Tabl. 2. Zestawienie wybranych producentów urządzeń do systemów InHousePLC

L.p.	Nazwa firmy: adres WWW	Asortyment produkcji
1	***Ambient Corp:*** www.ambientcorp.com	Urządzenia systemu oparte na układach scalonych firmy *DS2*
2	***Asoka USA:*** www.asokausa.com	Urządzenia (rutery, adaptery z interfejsami: USB, Ethernet, radiowy)
3	***China Gridcom Co.:*** www.gridcom.cn	Urządzenia (rutery, pomosty i adaptery z interfejsami: USB, Ethernet) zgodne ze standardami: *HomePlug 1.0* (14 Mbit/s) lub *HomePlug AV* (200 Mbit/s)
4	***Corinex Global Corp.:*** www.corinex.com	Urządzenia (rutery, pomosty i adaptery z interfejsami: USB, Ethernet, radiowy) zgodne ze standardami: *HomePlug 1.0* (14 Mbit/s) lub *HomePlug AV* (200 Mbit/s)
5	***Devolo AG:*** www.devolo.de	Urządzenia (rutery, pomosty i adaptery z interfejsami: USB, Ethernet, radiowy) zgodne ze standardami: *HomePlug 1.0* (14 Mbit/s) lub *HomePlug AV* (200 Mbit/s)
6	***Edimax:*** www.edimax.pl	Adaptery (z interfejsami: USB, Ethernet), zgodne ze standardem *HomePlug AV* (200 Mbit/s)
7	***GigaFast:*** www.gigafast.com	Adaptery (z interfejsami: USB, Ethernet), zgodne ze standardem *HomePlug AV* (200 Mbit/s)
8	***MainNnet Communications:*** www.mainnet-plc.com	Rozwiązania kompleksowe dla systemu i sieci dostępowych *BPLC*
9	***NETGEAR, Inc.:*** www.netgear.com	Adaptery (z interfejsami: USB, Ethernet), zgodne ze standardem *HomePlug 1.0* (14 Mbit/s) lub *HomePlug 1.0 Turbo* (85 Mbit/s)
10	***PolyTrax Information:*** www.polytrax.com	Adaptery z interfejsem radiowym *Bluetooth*
11	***Powernet Israel:*** www.powernetsys.com	Urządzenia zgodne ze standardami: *HomePlug 1.0* (14 Mbit/s) lub *HomePlug AV* (200 Mbit/s)
12	***ST&T:*** www.stt.com.tw	Adaptery (z interfejsami: USB, Ethernet), zgodne ze standardem *HomePlug 1.0* (14 Mbit/s) lub *HomePlug AV* (200 Mbit/s)
13	***TELKONET:*** www.telkonet.com	Urządzenia (rutery, pomosty i adaptery z interfejsami: USB, Ethernet) zgodne ze standardem: *HomePlug 1.0* (14 Mbit/s) lub *HomePlug AV* (200 Mbit/s)

Wymienione w tablicach firmy stanowią zaledwie niewielki procent producentów sprzętu elektronicznego, dostawców usług i urządzeń telekomunikacyjnych, promujących rozwój systemów domowej, szerokopasmowej łączności elektronicznej z wykorzystaniem istniejących wewnątrzbudynkowych instalacji elektrycznych niskiego napięcia. Podmioty te tworzą globalne stowarzyszenie o nazwie *HomePlug Powerline Alliance* (HPPA) [22], odpowiedzialne za normalizację systemów *InHousePLC*, badanie zgodności wyrobów z normami, a także za testowanie współpracy wyrobów różnych producentów. Stowarzyszenie to zrzesza obecnie ponad 70 podmiotów gospodarczych związanych z techniką *InHousePLC* z różnych krajów świata i liczba ich ciągle się powiększa. Niewątpliwym osiągnięciem stowarzyszenia jest uzgodnienie (w skali globalnej) jednolitych specyfikacji dla inteligentnego budynku/mieszkania, opartych na technice *InHousePLC*, takich jak: dystrybucja sygnałów IP TV, dostęp do gier interaktywnych i szerokopasmowego internetu, a także zdalnego monitoringu, kontroli stanu liczników (energii elektrycznej, gazu i poboru wody) oraz nadzoru i sterowania urządzeniami szeroko rozumianego gospodarstwa domowego (lodówki, piece gazowe, oświetlenie, itp.). Stowarzyszenie to wydało także ponad 200 świadectw certyfikacyjnych różnych elementów systemów *InHousePLC*, wytwarzanych przez członków tego stowarzyszenia.

Obecny asortyment rozwiązań obejmuje konwertery, przełączniki i rutery *InHousePLC*, zgodne ze standardami: *HomePlug 1.0*, *HomePlug AV*, *HomePlug AV2* oraz *HomePlug GreenPhy*. Wszystkie te standardy zostały opracowane przez stowarzyszenia HPPA.

Standard HomePlug 1.0 jest historycznie pierwszą specyfikacją, opracowaną przez stowarzyszenie HPPA. Standard ten, opublikowany w czerwcu 2001 r., dotyczy systemów *InHousePLC* 1-generacji, o przepływnościach binarnych (dla obu kierunków transmisji) do 14 Mbit/s. Obejmuje on również specyfikację urządzeń 2-generacji, znanych jako *HomePlug1.0 Turbo*, o maksymalnej przepływności 85,0 Mbit/s. W maju 2008 r. standard ten został zatwierdzony przez ANSI (*American National Standards Institute*), stając się w ten sposób pierwszym standardem dotyczącym łączności elektronicznej po liniach energetycznych, zatwierdzonym przez amerykańską instytucję normalizacyjną.

Standard HomePlug AV opracowano we wrześniu 2005 r. w celu specyfikacji systemów *InHousePLC* wykorzystywanych w inteligentnych domach/mieszkaniach do domowych aplikacji multimedialnych, takich jak: wideo-telefonia internetowa VoIP (*Voice over Internet Protocol*), telewizja internetowa wysokiej rozdzielczości HDTVoIP (*High Definition TV over Internet Protocol*), czy interaktywne gry sieciowe wysokiej rozdzielczości. W systemach tej klasy, dzięki zastosowaniu: 1155-kanałowej adaptacyjnej metody modulacji OFDM, turbo kodowania splotowego do korekcji błędów pierwotnych kanału oraz dwupoziomowego ramkowania w warstwie MAC z automatyczną regulacją jakości przekazu ARQ [28], uzyskano maksymalną przepływność binarną 200 Mbit/s. Zgodnie z tą specyfikacją urządzenia tej klasy mogą opcjonalnie współpracować z urządzeniami standardu *HomePlug 1.0*; przy czym, jeśli współpraca ta nie jest zapewniona, wówczas obligatoryjnie jest wymagana bezkolizyjna praca systemów obydwu standardów w środowisku tego samego medium transmisyjnego.

Standard HomePlug AV2 jest obecnie w trakcie opracowywania i dotyczy urządzeń *InHousePLC* następnej generacji, o ponad gigabitowej przepływności w warstwie fizycznej kanału (w jednym kierunku transmisji) oraz o wynikowej przepływności binarnej w warstwie MAC (przy czasowym rozdziale kierunków transmisji) do 600 Mbit/s. W standardzie tym zakłada się ponadto pełną kompatybilność urządzeń transmisyjnych tego standardu z urządzeniami standardu *HomePlug AV*. Przewiduje się [22], że prace normalizacyjne dla tej kategorii urządzeń *InHouse PLC* zostaną zakończone pod koniec 2010 r., pierwsze urządzenia tej klasy będą dostępne na rynku w 2011 r.

Standard HomePlug GreenPhy jest nową specyfikacją, przeznaczoną głównie do tzw. inteligentnych, domowych systemów zasilania energią elektryczną (*smart grid market*). Maksymalna przepływ-

ność w systemach tej klasy nie przekracza 10 Mbit/s, przy poborze energii elektrycznej przez te urządzenia mniejszym o 75% niż przez urządzenia standardu *HomePlugAV*, stąd przyrostek do nazwy *GreenPhy*. Zgodnie z tym standardem, urządzenia tej klasy stanowić będą wyposażenie komunikacyjne liczników poboru energii elektrycznej, zużycia gazu i wody, a także innych urządzeń elektrycznych gospodarstwa domowego, takich jak np.: lodówki, termostaty, elektryczne piece centralnego ogrzewania, wewnętrzne i zewnętrzne systemy oświetlenia budynku oraz wiele innych odbiorników energii elektrycznej. Zakłada się pełną kompatybilność urządzeń tej klasy z urządzeniami *HomePlug AV*, a także ich wysoką niezawodność działania, niewielkie rozmiary i łatwość integracji z odbiornikami energii elektrycznej oraz małe koszty wytwarzania w stosunku do kosztów produkcji urządzeń elektrycznych, w których będą one instalowane.

Kierunki rozwoju i zastosowań – aspekty ekonomiczne

Obserwując poczynania nauki, techniki i technologii w zakresie łączności *InHouse PLC* można powiedzieć, że technologia ta znajduje się w fazie ciągłego ulepszania. Ulepszanie, a przez to i dynamiczny rozwój systemów tej klasy, dzieje się w dwóch, wzajemnie przenikających się obszarach, którymi są:

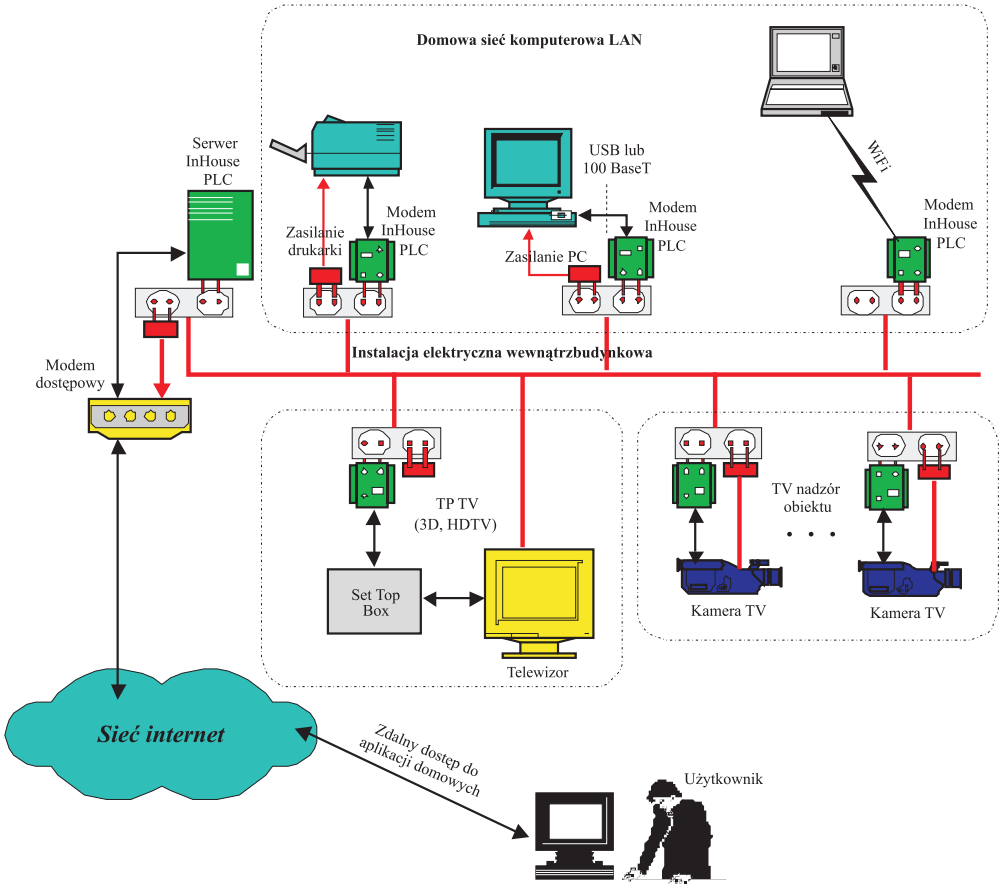
- zwiększanie przepływności binarnej w domenie komunikacyjnej,
- powiększanie obszaru zastosowań.

Zwiększanie przepływności binarnej w domenie komunikacyjnej *InHousePLC* jest realizowane przez stosowanie modulacji OFDM z coraz większą liczbą nośnych, w połączeniu z różnicowymi modulacjami DQPSK (*Differential Quarternary Phase Shift Keying*) i DQAM (*Differential Quadrature Amplitude Modulation*), lub przez stosowanie tzw. turbo-kodów, a więc algorytmów z adaptacyjną detekcją miękką. W tym obszarze działań są także prowadzone prace badawczo-wdrożeniowe w zakresie tworzenia warstwy fizycznej *InHousePLC* opartej na algorytmach sztucznych sieci neuronowych, zaangażowanych zarówno w proces detekcji sygnałów cyfrowych, jak i w rozpoznawanie i eliminację zakłóceń impulsowych z sygnału przed właściwym procesem detekcji. Najnowsze badania dotyczą także zastosowania tzw. technologi MIMO (*Multiply Input Multiply Output*) [30], znanej z szerokopasmowych systemów dostępu radiowego najnowszej generacji, w celu dalszego powiększania przepływności binarnej aż do magicznych 0,6 Gbit/s w warstwie MAC, tj. kilka razy większej niż przepływność binarna systemów domowej łączności elektronicznej na światłowodach plastikowych, co wydaje się być warte podkreślenia.

Powiększanie obszaru zastosowań techniki *InHousePLC* jest ściśle związane ze zwiększaniem przepływności binarnej systemów i jest uzyskiwane przez wzbogacanie interfejsów, głównie w obszarze oprogramowania, o nowe protokoły komunikacyjne, stosowane przez urządzenia stanowiące wyposażenie budynków inteligentnych nowej generacji. W budynkach takich, oprócz zastosowań wąskopasmowych związanych np. ze sterowaniem i kontrolą urządzeń gospodarstwa domowego, z odczytem stanu liczników energii elektrycznej, wody i gazu, coraz częściej są wdrażane różnego rodzaju platformy informatyczne z szerokopasmową komunikacją multimedialną. Obecnie, przy praktycznie uzyskiwanych przepływnościach w domenie komunikacyjnej systemów *InHousePLC* rzędu kilkuset megabitów na sekundę [24], [26], [27], [30], oprócz wymienionych zastosowań wąskopasmowych, systemy te są wykorzystywane do tworzenia zunifikowanej platformy komunikacyjnej (rys. 4):

- w mieszkaniowych lub budynkowych sieciach komputerowych z szerokopasmową bramą wyjściową do sieci internet;
- do dystrybucji sygnałów audio-wideo wysokiej rozdzielczości w obrębie mieszkania lub budynku, odbieranych od interaktywnych usług multimedialnych typu: telegry, telezakupy, zdalne nauczanie, audio i/lub wideo na żądanie itd.;

- w zintegrowanych systemach ochrony obiektów prywatnych lub użyteczności publicznej, z wizyjnym nadzorem tych obiektów.



Rys. 4. *Przykład domowych zastosowań multimedialnych system InHousePLC*

Główną zaletą współczesnych systemów *InHousePLC* jest możliwość szybkiego i prostego tworzenia szerokopasmowej, przewodowej platformy łączności elektronicznej, opartej na istniejącym okablowaniu instalacji elektrycznej budynku lub mieszkania. Oznacza to, że dla zapewnienia takiej łączności nie trzeba ponosić dodatkowych wydatków, związanych z instalacją medium transmisyjnego, poza przypadkiem, kiedy warstwa fizyczna wewnątrzobiektowej, szerokopasmowej sieci teleinformatycznej jest tworzona techniką światłowodową, czy Ethernet. W tych obydwu przypadkach są kosztowne i komponenty tworzące medium transmisyjne (światłowody lub kable informatyczne, gniazda, rozgałęźniki) i wykonanie instalacji w pomieszczeniach obiektu. Nakłady te są wielokrotnie wyższe① od kosztu zastosowanych urządzeń sieciowych (konwerterów, przełączników, ruterów). Ponieważ ceny urządzeń sieciowych techniki *InHousePLC* są tego samego rzędu② co ceny odpowiadających im urządzeń tech-

① *Całkowity koszt wykonania instalacji opartej na miedzianych kablach informatycznych w przeciętnym dwupoziomowym domu jednorodzinnym kształtuje się na poziomie około 5000 PLN, przy założeniu, że w każdym pomieszczeniu tego domu występuje jedno gniazdo tej instalacji.*

② *Cena detaliczna modemów InHouse PLC standardu HomePlug AV wynosi około 200 PLN, a cena modemów standardu HomePlug 1.0 Turbo nie przekracza 100 PLN.*

niki światłowodowej, czy też techniki *Ethernet*, to konkurencyjność cenowa techniki *InHousePLC* w stosunku do innych technik przewodowych jest niepodważalna. Biorąc jako kryterium oceny maksymalne teoretyczne przepływności binarne uzyskiwane w domenie komunikacyjnej należy zauważyć, że i w tym obszarze technika *InHousePLC* nie jest rozwiązaniem gorszym od innych technik przewodowych. Przepływność binarna w warstwie fizycznej domeny *InHousePLC* zgodnej ze standardem *HomePlug AV2* wynosi bowiem 1,2 Gbit/s, co odpowiada przepływności binarnej w warstwie fizycznej sieci *GbitEthernet* i jest kilka razy większa od przepływności domeny światłowodowej ze światłowodami plastikowymi①.

Porównując atrakcyjność techniki *InHousePLC* i systemów radiowych zgodnych ze standardami 802.11.b/g można stwierdzić, że:

- obydwa rozwiązania są proste w obsłudze (z punktu widzenia użytkownika) i umożliwiają prawie tak samo szybkie utworzenie wewnątrzbudynkowej sieci LAN, z niewielką przewagą na korzyść techniki *InHousePLC*;
- obydwa rozwiązania nie wymagają tworzenia dodatkowej instalacji wewnątrz budynku do realizacji warstwy fizycznej sieci LAN;
- ceny urządzeń sieciowych zastosowanych w obydwu rozwiązaniach są tego samego rzędu, nieco tańsze są systemy radiowe (cena detaliczna zakupu stacji bazowej, zwanej powszechnie *access point*, zawiera się w przedziale 100÷150 PLN);
- maksymalna teoretyczna przepływność binarna dla warstwy fizycznej domeny w technice *InHousePLC*, w przypadku standardu *HomePlug AV2*, wynosi 1,2 Gbit/s i jest kilkadziesiąt razy większa niż maksymalna przepływność systemów radiowych standardu 802.11.g, wynosząca 54 Mbit/s.

Podsumowanie

Wiele projektów europejskich koncentruje się obecnie na tworzeniu nowych architektur i mechanizmów sieciowych nowej generacji, zwanych potocznie internetem przyszłości. Architektury te są oparte na mechanizmach wirtualizacji elementów sieciowych i jako takie są odpowiedzią na obecne i przyszłe potrzeby użytkowników szeroko rozumianej telekomunikacji w zakresie niezawodnego zapewniania (przez tę samą sieć) różnorodnych form przekazu wiadomości od prostych, wąskopasmowych transmisji danych alfanumerycznych do zaawansowanych platform łączności elektronicznej z pełną gwarancją jakości przekazu, wykorzystywaniem w łączności multimedialnej czasu rzeczywistego, np. w: wideotelefonii wysokiej rozdzielczości, trójwymiarowej szerokopasmowej telewizji internetowej, trójwymiarowych grach interaktywnych wysokiej rozdzielczości, zdalnym nauczaniu, zdalnych zakupach itp. Zastosowania te są przedmiotem zainteresowania zarówno grupy użytkowników mobilnych, jak i stacjonarnych, a także użytkowników mobilno-stacjonarnych, a efektywne korzystanie z nich wymaga „istnienia" infrastruktury telekomunikacyjnej zapewniającej łączność szerokopasmową w bezpośredniej bliskości użytkownika. Nie ulega wątpliwości, że dla użytkownika mobilnego rozwiązaniami takimi są techniki szerokopasmowej łączności radiowej WiFi (*Wireless Fidelity*), WiMax (*Worldwide Interoperability for Microwave Access*), czy techniki łączności pseudosatelitarnej HAP (*Hight Altitude Platformas*). Użytkownicy stacjonarni zaś mogą być efektywnie dołączani do internetu przyszłości z wykorzystaniem wyżej omówionej technologii *InHousePLC*. Oczywiście połączenie to może być zrealizowane techniką łączności światłowodowej, opartej na światłowodach plastikowych. Wymaga to jednak rozprowadzenia światłowodu w obrębie domu lub

① *Z uwagi na wymagany mały promień gięcia, w domowych instalacjach światłowodowych raczej nie stosuje się kabli z jednomodowymi włóknami kwarcowymi o parametrach transmisyjnych, pozwalających na uzyskanie przepływności binarnych ok. 10 Gbit/s.*

mieszkania, co wiąże się z koniecznością poniesienia dodatkowych kosztów instalacyjnych, których nie ma w przypadku zastosowania technik *InHousePLC*. Dodatkowo, ponieważ praktycznie wszystkie oferowane obecnie na rynku modemy *InHousePLC* są wyposażone w szerokopasmowy interfejs radiowy, to technika ta wydaje się być rozwiązaniem optymalnym również dla grupy użytkowników mobilno-stacjonarnych.

Bibliografia

[1] Aprille T. at al.: *Interactive broadband services and PCS network architecture*. Bell Labs Techn. J., vol. 1, no 1, summer 1996

[2] Arzberger M. at al.: *Fundamental properties of the low voltage power distribution grid*. Proc. Int. Symp. Power-line Communications and its Applications, Essen, 1997

[3] Barnes J.S.: *A physical multi-path model for power distribution network propagation*, Proc. Int. Symp. Power-line Communications and its Applications, Tokyo, 1998

[4] Brandt F.: *BEWAG case study: Examining and evaluating the dune project's success in power line communications*. Proc. Int. Symp. Power-line Communications, London, September 1998

[5] Brown P.: *Telecommunication services and local access provision*. http.//www.nortel.com/powerline/report2.htm

[6] Brown P. A.: *Overcoming the technical challenges of sending high-speed data over power line*. Proc. Int. Symp. Power-line Communications, London, September 1998

[7] Brown P.: *Multi-media communication over the electricity networks*. http.//www.nortel.com/powerline/report3.htm

[8] Brown P.: *High frequency conditioned power networks*. http.//www.nortel.com/powerline/report4.htm

[9] Brown P. Linge N.: *A multi-media architecture facilitating advanced inter-active customer services*. http.//www.nortel.com/powerline/report1.htm

[10] Cogency : *White paper : CS1102 Ethernet to homeplug bridge*. http://www.cogency.com/B_Support/CS1102_DS_PN_0118_01.pdf

[11] Dosert K.: *Powerline communications*. Prentice Hall, Upper Saddle River, 2001

[12] Dosert K.: *EMC aspects of high speed powerline communications*. Proc. Int. Symp. Electromagnetic Compatibility, Wrocław, Poland, 2002

[13] DS2: *Products catalog*. http://www.ds2.es/products/pcatalog.pdf

[14] ETSI TS 101 867 V1.1.1 (2000-11). *Powerline telecommunications (PLT);Coexistence of access and in-house powerline systems*

[15] ETSI TS 101 896 V1.1.1 (2001-02). *Powerline telecommunications (PLT); Reference network architecture model*

[16] Fenton F., Sipes J.: *Architectural and technological trends in access: An overview*. Bell Labs Techn. J., vol. 1, no 1, Summer 1996

[17] Gagen P. E., Pugh W. E.: *Hybrid fiber-coax access networks*. Bell Labs Techn. J., vol. 1, no 1, Summer 1996

[18] Gut-Mostowy H.: *Techniki transmisyjne w multimedialnych, abonenckich sieciach dostępowych*. Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, 1998, nr 9

[19] Gut-Mostowy H.: *Szerokopasmowe techniki dostępowe wykorzystujące linie energetyczne niskiego napięcia*. Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, 1999, nr 6

[20] Gut-Mostowy H., Kowalewski M.: *Wykorzystanie linii energetycznych jako lokalnych sieci dostepowych – szansą na szybką integrację wsi polskiej ze społecznością globalnej wioski informacyjnej*. Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, 2000, nr 6

[21] Gut-Mostowy H.: *Wykorzystanie linii energetycznych jako lokalnych sieci dostepowych. Badanie właściwości propagacyjnych linii*. Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, 2000, nr 6

[22] *HomePlug powerline alliance*: http://en.wikipedia.org/wiki/HomePlug_Powerline_Alliance, August 2010

[23] Hrasnica H., Haidine A. and Lehnert R.: *Broadband powerline communications networks. Network design*. Wiley, England, 2004

[24] Intellon : *HomePlug AV*. http://www.intellon.com/products/homeplugav/

[25] Intellon : *HomePlug with turbo*. http://www.intellon.com/products/homeplug_turbo

[26] Intellon : *INT5200 Product brief*. http://www.intellon.com/pdfs/INT5200_Product_Brief.pdf

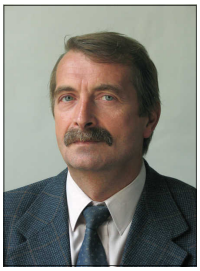
[27] Katar S., Krishnam M., Newman R. and Latchman H.: *Harnessing the potential of powerline communications using the HomePlug AV standard.* http://rfdesign.com/mag/608RFDF1.pdf. July 2008

[28] Katar S., Yonge L., Newman R. and Haniph L.: *Efficient framing and ARQ for high-speed PLC systems*. http://www.cise.ufl.edu/~nemo/papers/ISPLC2005-framing.pdf. Jan. 2008.

[29] Okada K. at al.: Overview of full services optical access networks. Proc. Conf. Full Services Access Netw. London, 1996

[30] *Revolutionary powerline communications technology with MIMO announced by sigma designs*: http://www.marketwire.com/press-release/

Henryk Gut-Mostowy



Mgr inż. Henryk Gut-Mostowy (1951) – absolwent Wydziału Elektroniki Politechniki Warszawskiej (1975); długoletni pracownik Instytutu Łączności w Warszawie (od 1976); starszy wykładowca w Wyższej Szkole Techniczno-Ekonomicznej w Warszawie (od 2002); promotor prac inżynierskich z dziedziny informatyki stosowanej; autor i współautor kilkudziesięciu publikacji i referatów na konferencjach krajowych; redaktor kwartalnika Telekomunikacja i Techniki Informacyjne; zainteresowania naukowe: Internet Przyszłości oparty na wirtualizacji zasobów sieciowych, modelowanie numeryczne warstwy fizycznej systemów InHousePLC i metody predykcji przepływności binarnej tych systemów, systemy inteligentnego transportu samochodowego w tym system e-call.

e-mail: H.Gut@itl.waw.pl

Wymagania na rozdzielczość i nieliniowość przetwornika C/A dla sygnału OFDM

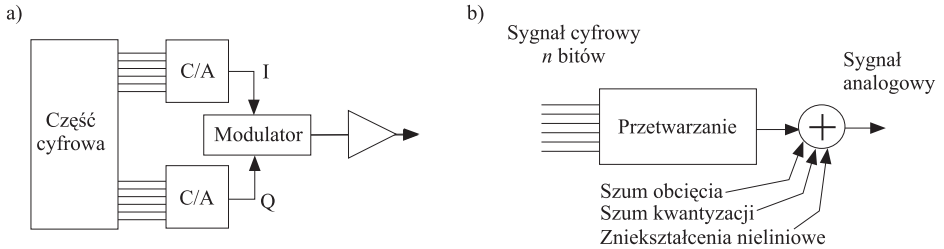
Adam Rudziński
Sebastian Kozłowski

Przedstawiono model analityczny, umożliwiający wyznaczenie błędów wnoszonych do sygnału OFDM w procesie przetwarzania cyfrowo-analogowego. Zaproponowano wyrażenia do oszacowania wymaganej rozdzielczości i dopuszczalnych nieliniowości przetwornika C/A, gwarantujących utrzymanie zniekształceń sygnału poniżej założonego poziomu.

przetwornik cyfrowo-analogowy, modulacja OFDM, szum kwantyzacji, nieliniowość całkowa, nieliniowość różniczkowa

Wprowadzenie

Przetworniki cyfrowo-analogowe (C/A) są obecnie jednymi z niezbędnych elementów każdego radiowego urządzenia nadawczego [1]. Przykładem ich zastosowania jest typowa konstrukcja nadajnika radiowego z modulacją kwadraturową, której uproszczony schemat jest przedstawiony na rys. 1. Układy przetworników C/A stanowią interfejs między częścią cyfrową, w której generowane są dane do transmisji, a częścią analogową, w której następuje przemiana częstotliwości i wzmocnienie sygnału. Dlatego bardzo istotny jest wybór przetwornika o odpowiednio dobrych parametrach, zapewniającego poprawne przetwarzanie i utrzymującego założoną jakość sygnału. Zagadnienie to jest szczególnie istotne w przypadku stosowania modulacji OFDM – *Orthogonal Frequency Division Multiplexing* (modulacji na wielu ortogonalnych podnośnych), która sprawia, że przebieg czasowy przesyłanego sygnału staje się bardzo skomplikowany.



Rys. 1. *a) Uproszczony schemat blokowy typowego nadajnika radiowego z modulacją kwadraturową. b) Model funkcjonalny przetwornika C/A*

Proces przetwarzania sygnału z postaci cyfrowej do analogowej, podobnie jak każdy inny proces fizyczny, nie jest wolny od zjawisk mających negatywny wpływ na przetwarzany sygnał. Można wyróżnić kilka mechanizmów degradacji sygnału przez przetwornik C/A [1, 2], których nie można pominąć przy projektowaniu urządzeń. Są to m.in. ograniczenie sygnału wyjściowego do skończonego zakresu (obcinanie), kwantyzacja oraz zniekształcenia przez nieliniowości (różniczkową i cał-

kową) – przedstawione w modelu funkcjonalnym przetwornika, przedstawionym schematycznie na rys. 1b. Wyboru przetwornika można dokonać przeprowadzając symulacje i analizując ich wyniki [3, 4], co jest jednak czasochłonne i nie ukazuje jawnie zależności, które wpływają na wynik przetwarzania. O wiele wygodniej jest skorzystać z modelu analitycznego, oczywiście gdy taki model istnieje. Spośród wymienionych mechanizmów degradacji sygnału najdokładniej został przeanalizowany wpływ obcięcia sygnału [5]. Ograniczony model, umożliwiający wyznaczenie wymaganej rozdzielczości (liczbę bitów) przetwornika, można znaleźć w [6], natomiast wydaje się, że model analityczny opisujący wpływ nieliniowości na sygnał z modulacją na wielu podnośnych nie został jeszcze przez nikogo opublikowany.

W niniejszej pracy podjęto próbę stworzenia modelu analitycznego, umożliwiającego wyznaczenie wymaganej rozdzielczości i dopuszczalnej nieliniowości przetwornika C/A, zapewniających przetwarzanie sygnału OFDM z degradacją poniżej założonego poziomu. W dostępnych obecnie przetwornikach następuje bardzo szybkie ustalanie się poziomu sygnału wyjściowego, dlatego skoncentrowano się na parametrach statycznych, zakładając, że przetwarzany sygnał jest wolnozmienny, a więc na wyjściu przetwornika występuje sygnał schodkowy o idealnie stromych zboczach. Otrzymane wyniki pokrywają się z przeprowadzonymi symulacjami numerycznymi i są istotnie różne od przedstawionych w [6], według których wymagana rozdzielczość przetwornika zależy od konstelacji i liczby podnośnych.

Przedstawione dalej zależności są ogólniejsze i umożliwiają powiązanie wymaganej rozdzielczości z poziomem obcięcia sygnału, liczbą podnośnych, liczbą próbek sygnału oraz dopuszczalnym błędem przetwarzania, co pośrednio wprowadza zależność od modulacji zastosowanej dla podnośnych. W szczególności, uzyskane wyniki wskazują na istotny wpływ gęstości dyskretyzacji, tj. stosunku liczby próbek do liczby podnośnych. Według Autorów, przedstawione rozważania, dotyczące wpływu nieliniowości przetwornika, wykraczają poza wszelkie dostępne w literaturze światowej.

Założenia modelu i definicje

Cyfrowy sygnał OFDM (z modulacją na wielu ortogonalnych podnośnych) jest podawany do przetwornika C/A. Przetwarzany sygnał może stanowić całość przesyłanych przez urządzenie danych lub być jedynie ich częścią, np. w przypadku, gdy jest to jeden ze strumieni wejściowych modulatora kwadraturowego, co jednak nie jest istotne w badanym zagadnieniu. Zostaną pominięte efekty dynamiczne, takie jak skończony czas ustalania się poziomu sygnału na wyjściu przetwornika czy jitter (czasu lub fazy), zakładając, że sygnał zmienia się na tyle wolno, że proces przemiany można wystarczająco dobrze opisać za pomocą parametrów statycznych. W wyprowadzeniach ograniczono się do pojedynczego symbolu OFDM, którego ogólną postać cyfrową można zapisać jako:

$$x_i \equiv x(iT) = \frac{1}{\sqrt{N_S}} \sum_{k \in K} A_k \cos(\omega_k iT + \phi_k), \tag{1}$$

gdzie:

- i – indeksuje kolejne próbki,
- T – jest okresem próbkowania,
- N_S – liczbą próbek „właściwego” symbolu, po usunięciu wszelkiego rodzaju okresów ochronnych, prefiksów cyklicznych itp.

Symbol jest złożony z K podnośnych, indeksowanych przez k, dla których założono jednakowe schematy modulacji. Nie nałożono dodatkowych warunków na wartości N_S i K, dopuszczając dowolnie gęstą dyskretyzację, określaną stosunkiem N_S/K. Pulsacje podnośnych ω_k są dobrane w taki sposób, aby odpowiadające im przebiegi były ortogonalne w przedziale równym czasowi trwania symbolu $T_S = N_S T$:

$$\frac{1}{N_S}\sum_i \exp(j\omega_k iT)\exp(-j\omega_{k'} iT) = \delta_{kk'}, \tag{2}$$

gdzie:

$\delta_{kk'}$ – delta Kroneckera.

Symbole na poszczególnych podnośnych koduje się poprzez ich amplitudy A_k lub fazy ϕ_k, które są stałe w czasie trwania symbolu OFDM. Przyjęto, że symbol ma zerową składową stałą, która jest szczególnie podatna na przesunięcie przez przetwornik i nie nadaje się do przesyłania informacji. Dodatkowo (dla ustalenia uwagi) założono, że wszystkie $\omega_k > 0$. Średnia moc symbolu OFDM wynosi

$$\sigma^2 = K\langle C^2\rangle, \tag{3}$$

gdzie:

$\langle C^2\rangle$ – średnia moc konstelacji, wyznaczana ze wzoru:

$$\langle C^2\rangle = \sum_{k\in C}\frac{A_k^2}{2M}, \tag{4}$$

w którym:

k – przebiega konstelację (zbiór symboli) C,

M – liczba symboli w konstelacji.

Do opisu przetwarzania przez przetwornik C/A o rozdzielczości n bitów jest wygodnie przyjąć jako jednostkę dla sygnału wyjściowego LSB (*Least Significant Bit*), tj. różnicę między idealnie rozłożonymi poziomami wyjściowymi, wynoszącą $1/(2^n-1)$ część pełnego zakresu wyjściowego. Wówczas sygnał na wyjściu przetwornika przyjmuje wartości całkowite ze zbioru $\{-2^{n-1},\ldots,2^{n-1}-1\}$, zwane dalej poziomami (dla przejrzystości zapisu jednostka LSB nie będzie jawnie wskazywana). Dzięki temu sygnał wyjściowy można wprost (bez dodatkowych przeskalowań i przesunięć) porównywać z sygnałem wejściowym. Amplituda sygnału wyjściowego jest ograniczona do wartości $2^{n-1}-1$, co powoduje obcinanie fragmentów sygnału wejściowego przekraczających tę wartość. Przebieg symbolu wejściowego poddawany jest kwantyzacji, która przekształca go do postaci schodkowej

$$x_i^q = x_i + \Delta_i^q, \tag{5}$$

gdzie:

Δ_i^q – błąd (szum) kwantyzacji,

x_i^q – przyjmuje wartości z zakresu wyjściowego przetwornika.

Uwzględniono również nieliniowości, czyli zniekształcenia sygnału spowodowane przez przesunięcia poziomów na wyjściu względem wartości idealnych (błędy odwzorowania poziomów). Ponieważ o jakości przetwarzania decyduje możliwość poprawnego odbioru sygnału w odbiorniku, założono, że sygnał przetworzony jest sprowadzany ponownie do postaci cyfrowej przez idealny przetwornik A/C

i analizowany bez dalszych zniekształceń. Przy przyjętych założeniach sygnał wyjściowy można opisać wyrażeniem

$$y_i = x_i^{\mathrm{q}} + \Delta\left(x_i^{\mathrm{q}}\right), \tag{6}$$

gdzie:
$\Delta(p)$ – błąd odwzorowania poziomu p przez rozważany przetwornik C/A.

Błędy wnoszone przez system można scharakteryzować za pomocą EVM (*Error Vector Magnitude*), którą to wielkość definiuje się jako pierwiastek ze stosunku średniej mocy wektora błędu do mocy odniesienia. W przypadku modulacji na wielu podnośnych jako moc odniesienia można wybrać średnią moc sygnału [7]. Zgodnie z tą definicją

$$\mathrm{EVM} = \sqrt{\frac{\langle \mathrm{ev}^2 \rangle}{\sigma^2}}, \tag{7}$$

gdzie:
ev – wektor błędu.

Wartość EVM wyraża się zazwyczaj w procentach. Przyjęta definicja pozwala łatwo obliczyć stosunek mocy sygnału do mocy szumu $\mathrm{SNR} = \mathrm{EVM}^{-2}$.

Traktując wszystkie trzy uwzględniane źródła szumu i zniekształceń sygnału jako niezależne można napisać:

$$\left\langle \mathrm{ev}^2 \right\rangle = \left\langle \mathrm{ev}_{\mathrm{c}}^2 \right\rangle + \left\langle \mathrm{ev}_{\mathrm{q}}^2 \right\rangle + \left\langle \mathrm{ev}_{\mathrm{nl}}^2 \right\rangle, \tag{8}$$

gdzie:
$\left\langle \mathrm{ev}_{\mathrm{c}}^2 \right\rangle$ – średnia moc wektora błędu obcięcia,
$\left\langle \mathrm{ev}_{\mathrm{q}}^2 \right\rangle$ – średnia moc wektora błędu kwantyzacji,
$\left\langle \mathrm{ev}_{\mathrm{nl}}^2 \right\rangle$ – średnia moc wektora błędu zniekształceń nieliniowych.

Na wartość EVM wpływają wówczas trzy wielkości: $\mathrm{EVM_c} = \sqrt{\left\langle \mathrm{ev}_{\mathrm{c}}^2 \right\rangle / \sigma^2}$ pochodzący od szumu obcięcia, $\mathrm{EVM_q} = \sqrt{\left\langle \mathrm{ev}_{\mathrm{q}}^2 \right\rangle / \sigma^2}$ pochodzący od szumu kwantyzacji oraz $\mathrm{EVM_{nl}} = \sqrt{\left\langle \mathrm{ev}_{\mathrm{nl}}^2 \right\rangle / \sigma^2}$ pochodzący od zniekształceń nieliniowych. Są to funkcje parametrów przetwornika i sygnału, zatem, jeżeli interpretować EVM jako dopuszczalną wartość całkowitego błędu, można napisać warunek:

$$\mathrm{EVM_c^2} + \mathrm{EVM_q^2} + \mathrm{EVM_{nl}^2} < \mathrm{EVM}^2, \tag{9}$$

który umożliwia oszacowanie wymagań na parametry przetwornika. Dalej są przedstawione wyprowadzenia wyrażeń opisujących poszczególne składniki.

Weryfikacja numeryczna

W celu weryfikacji modelu porównano jego przewidywania z wynikami obliczeń numerycznych. Przyjęte założenia i ograniczenie się do efektów statycznych umożliwiły wykorzystanie w tym celu prostego algorytmu, złożonego z następujących kroków:

1. Losowanie K punktów z założonej konstelacji C definiujących pojedynczy symbol OFDM.
2. Generacja N_{S} próbek przebiegu sygnału wejściowego (za pomocą IFFT).

3. Wprowadzenie odpowiednich zniekształceń, tj. obcięcia sygnału, kwantyzacji lub błędów odwzorowania poziomów.
4. Obliczenie punktów w założonej konstelacji w sygnale wyjściowym (za pomocą FFT).
5. Obliczenie mocy wektorów błędu i obliczenie EVM dla wylosowanego symbolu OFDM.
6. Wielokrotne powtórzenie poprzednich kroków, co odpowiada przetworzeniu założonej liczby symboli OFDM.
7. Uśrednienie EVM dla wszystkich wylosowanych symboli OFDM, dające ostateczny wynik obliczeń.

Przedstawiane w niniejszej pracy wyniki numeryczne pochodzą z obliczeń wykonywanych dla 1000 symboli OFDM z modulacją 64-QAM na każdej podnośnej.

Szum obcięcia

Do oceny wpływu obcięcia sygnału zastosowano metodę opisaną w [5], uproszczoną przez pominięcie korelacji między kolejnymi próbkami wynikającego z tego szumu. Sygnał x_i można z dobrym przybliżeniem traktować jako proces stochastyczny, którego próbki są niezależnymi zmiennymi losowymi. Z centralnego twierdzenia granicznego wynika, że gęstość prawdopodobieństwa przyjęcia przez próbkę wartości x dana jest rozkładem Gaussa z wariancją σ^2, określoną przez średnią moc sygnału (3):

$$f_x(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{x^2}{2\sigma^2}\right). \tag{10}$$

Poziom progu obcięcia można określić za pomocą parametru

$$\alpha = \frac{2^{n-1}-1}{\sigma}, \tag{11}$$

wówczas obcięcie polega na ograniczeniu wartości sygnału do zakresu $[-\alpha\sigma, \alpha\sigma]$, próbki szumu obcięcia zaś są zmiennymi losowymi o gęstości prawdopodobieństwa

$$f_c(x) = \begin{cases} f_x(|x| + \alpha\sigma), & \text{gdy } x \neq 0, \\ \int_{-\alpha\sigma}^{\alpha\sigma} \mathrm{d}x\, f_x(x), & \text{gdy } x = 0. \end{cases} \tag{12}$$

Stosunek wariancji tego rozkładu σ_c^2 do wariancji σ^2 (czyli moc szumu do mocy sygnału wejściowego przetwornika) wynosi

$$\frac{\sigma_c^2}{\sigma^2} = \left(1+\alpha^2\right) \operatorname{erfc}\left(\frac{\alpha}{\sqrt{2}}\right) - \alpha\sqrt{\frac{2}{\pi}} \exp\left(-\frac{\alpha^2}{2}\right), \tag{13}$$

gdzie komplementarna funkcja błędu

$$\operatorname{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty \mathrm{d}t\, e^{-t^2}. \tag{14}$$

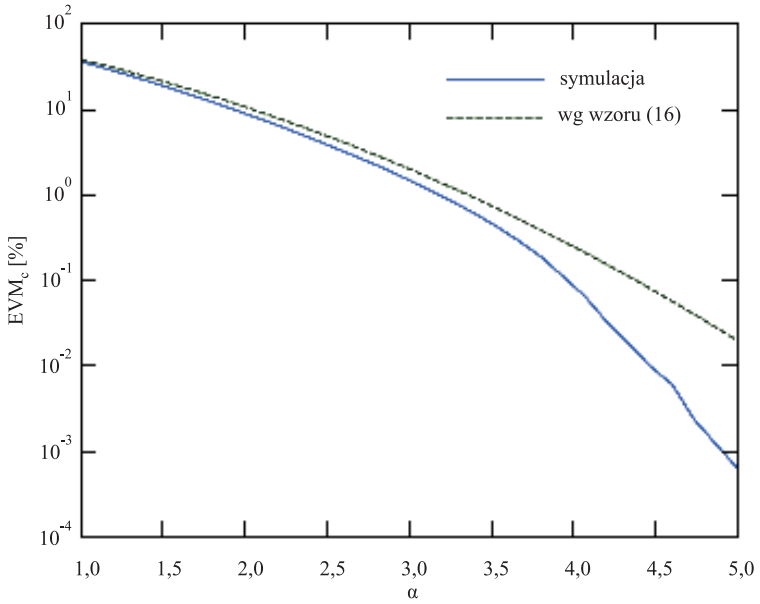
Moc wektora błędu wynosi

$$\left\langle \mathrm{ev}_c^2 \right\rangle = \sigma_c^2, \tag{15}$$

a zatem:

$$\mathrm{EVM}_c = \frac{\sigma_c}{\sigma}. \tag{16}$$

Wykresy stanowiące porównanie wyniku teoretycznego (16) i symulacji przedstawiono na rys. 2. Wyprowadzone wyrażenie stanowi górne ograniczenie wartości $\mathrm{EVM_c}$, które wraz ze wzrostem α staje się coraz mniej dokładne. Pozwala jednak poprawnie przewidzieć czy obcięcie sygnału będzie istotne,



Rys. 2. $\mathrm{EVM_c}$ *w funkcji* α

w szczególności zauważyć, że wybór $\alpha = 4$ ogranicza w zadowalającym stopniu jego wpływ [5, 6]. W związku z tym wartość ta jest przyjęta w dalszych obliczeniach. Przedstawione oszacowanie jest wystarczająco dobre do zastosowania w niniejszej pracy, w której skoncentrowano się na wpływie kwantyzacji i nieliniowości.

Szum kwantyzacji

Jeżeli wartość skuteczna sygnału OFDM jest znacznie większa niż 1 LSB, szum kwantyzacji jest z dobrym przybliżeniem szumem białym o jednorodnym rozkładzie wartości próbek [8]. W wyprowadzeniu zatem próbki szumu kwantyzacji Δ_i^{q} będą traktowane jako niezależne zmienne losowe o rozkładzie jednorodnym w przedziale $\left[-\frac{1}{2}, \frac{1}{2}\right]$, z wariancją równą $\frac{1}{12}$. W takim przypadku, moc szumu rozkłada się jednakowo na wszystkie N_{S} próbek widma, z których jedynie $2K$ odpowiada zaszumianemu sygnałowi OFDM. Dlatego, średnia moc wektora błędu w paśmie sygnału wynosi

$$\left\langle \mathrm{ev}_{\mathrm{q}}^2 \right\rangle = \frac{2K}{N_{\mathrm{S}}} \left\langle \left(\Delta_i^{\mathrm{q}}\right)^2 \right\rangle = \frac{K}{6N_{\mathrm{S}}}, \tag{17}$$

skąd wynika, że

$$\mathrm{EVM_q} = \sqrt{\frac{2K}{3N_{\mathrm{S}}}} \frac{\alpha}{2^n - 2}. \tag{18}$$

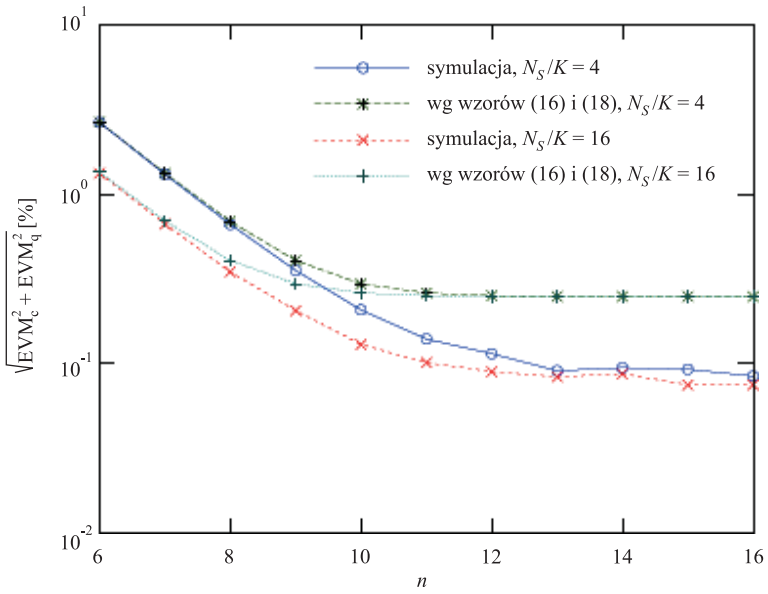
Uwzględniając szumy obcięcia oraz kwantyzacji, warunek (9) przyjmuje postać:

$$\mathrm{EVM} > \sqrt{\frac{\sigma_c^2}{\sigma^2} + \frac{2K}{3N_S}\frac{\alpha^2}{(2^n-2)^2}}. \tag{19}$$

Wynika stąd wymagana rozdzielczość przetwornika

$$n > \log_2\left(2 + \sqrt{\frac{2K}{3N_S}}\frac{\alpha}{\sqrt{\mathrm{EVM}^2 - \sigma_c^2/\sigma^2}}\right). \tag{20}$$

Prawa strona (19) wyznacza teoretyczną wartość EVM, porównaną z wynikami symulacji na rys. 3. Widać, że obie wartości są zgodne przy małej rozdzielczości n. Przy większych rozdzielczościach dominuje błąd obcięcia sygnału, dany przeszacowanym wyrażeniem (16), stąd wyniki symulacji



Rys. 3. EVM *wynikający z obcięcia sygnału i kwantyzacji w funkcji n dla różnych stosunków* N_S/K

są korzystniejsze niż wartości teoretyczne, jednak zgodność przebiegów krzywych jest wyraźna i wskazuje na poprawność wyrażenia (18). Wynika z niego (co znajduje pokrycie w wynikach symulacji), że szum kwantyzacji zależy wprost jedynie od: gęstości dyskretyzacji N_S/K, poziomu obcięcia α oraz rozdzielczości przetwornika. W szczególności, otrzymana zależność od gęstości dyskretyzacji wskazuje, że poprawę jakości przetwarzania C/A można otrzymać zwiększając gęstość dyskretyzacji N_S/K, co nie wynika np. ze wzorów przedstawionych w pracy [6].

Zniekształcenia nieliniowe

Analiza wpływu zniekształceń nieliniowych jest bardziej złożona. Zniekształcenia te mają swoje źródło w błędzie odwzorowania poziomów $\Delta(p)$, będącego różnicą między rzeczywistą a nominalną

wartością sygnału na poziomie p na wyjściu przetwornika. Przebieg błędu $\Delta\left(x_i^{\mathrm{q}}\right)$ odpowiadający sygnałowi x_i^{q} można rozdzielić na cztery składniki

$$\Delta\left(x_i^{\mathrm{q}}\right) = \Delta_0 + (G-1)x_i^{\mathrm{q}} + \Delta_{\mathrm{d}}\left(x_i^{\mathrm{q}}\right) + \Delta_{\mathrm{s}}\left(x_i^{\mathrm{q}}\right). \tag{21}$$

Pierwsze dwa składniki definiują przesunięcie charakterystyki przetwornika i jej nachylenie (wzmocnienie). Nie mają one znaczenia dla dalszych rozważań. Pozostałe składniki opisują zniekształcenia nieliniowe: $\Delta_{\mathrm{d}}\left(x_i^{\mathrm{q}}\right)$ jest ich częścią wolnozmienną, potraktowaną jako deterministyczna, natomiast $\Delta_{\mathrm{s}}\left(x_i^{\mathrm{q}}\right)$ jest częścią szybkozmienną (pseudolosową), traktowaną jako ergodyczny, stacjonarny proces stochastyczny o zerowej wartości średniej i właściwościach szumu białego:

$$\overline{\Delta_{\mathrm{s}}\left(x_i^{\mathrm{q}}\right)} = \langle \Delta_{\mathrm{s}} \rangle = 0 \tag{22}$$

oraz

$$\overline{\Delta_{\mathrm{s}}\left(x_i^{\mathrm{q}}\right)\Delta_{\mathrm{s}}\left(x_{i+l}^{\mathrm{q}}\right)} = \left\langle \Delta_{\mathrm{s}}^2 \right\rangle \delta_{l0} = \sigma_{\mathrm{s}}^2 \delta_{l0}, \tag{23}$$

gdzie:

$\overline{f_i}$ – wartość średnia przebiegu f_i,

δ_{l0} – delta Kroneckera przyjmująca wartość 1 dla $l = 0$.

Przy założeniu, że obydwie składowe są wzajemnie ortogonalne i nieskorelowane:

$$\overline{\Delta_{\mathrm{d}}\left(x_i^{\mathrm{q}}\right)\Delta_{\mathrm{s}}\left(x_{i+l}^{\mathrm{q}}\right)} = 0, \tag{24}$$

średnia moc wektora błędu staje się sumą średnich mocy pochodzących od obydwu składowych oddzielnie

$$\left\langle \mathrm{ev}_{\mathrm{nl}}^2 \right\rangle = \left\langle \mathrm{ev}_{\mathrm{nld}}^2 \right\rangle + \left\langle \mathrm{ev}_{\mathrm{nls}}^2 \right\rangle. \tag{25}$$

Składowe pseudolosową i deterministyczną można powiązać z parametrami katalogowymi, którymi są nieliniowości różniczkowa DNL (*Differential Nonlinearity*) i całkowa INL (*Integral Nonlinearity*) [9].

Wektor błędu składowej pseudolosowej

Składowa pseudolosowa (tj. szybkozmienna) błędu odwzorowania poziomów przypomina pod pewnymi względami szum kwantyzacji. Do sygnału dodawane jest nieregularne zniekształcenie, zależne od chwilowej wartości sygnału. Zatem, podobnie jak przy kwantyzacji, moc tego błędu rozkłada się równomiernie w pewnym pasmie częstotliwości, do pasma sygnału zaś trafia tylko jej część. W przypadku kwantyzacji stanowi ona $2K/N_{\mathrm{S}}$ całej mocy szumu. Jednakże błąd kwantyzacji przyjmuje wartości ze zbioru ciągłego, dlatego prawdopodobieństwo tego, że kolejne próbki tego błędu przyjmują jednakową wartość, jest równe zeru. Natomiast błąd odwzorowania poziomu jest określony na zbiorze dyskretnym, wobec tego dla niego takie zdarzenie ma niezerowe prawdopodobieństwo. Pojawianie się w realizacji szumu ciągów próbek o tej samej wartości prowadzi do zawężenia jego pasma. W efekcie, ułamek mocy szumu przypadający na pasmo sygnału można zapisać jako $2K/N_{\mathrm{eff}}$, w którym definiuje się efektywną liczbę próbek

$$N_{\mathrm{eff}} = \frac{N_{\mathrm{S}}}{\langle L \rangle}, \tag{26}$$

gdzie:

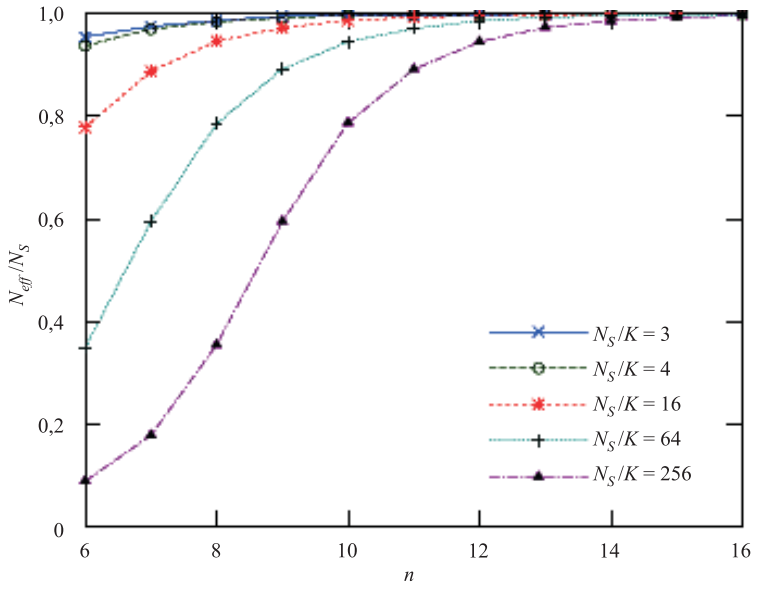
$\langle L \rangle$ – średnia długość ciągu kolejnych próbek o jednakowej wartości w skwantowanym sygnale x_i^{q}.

W niniejszej pracy $\langle L \rangle$ jest wyznaczane za pomocą symulacji numerycznej. Można jednak wskazać dwa mechanizmy wpływające na wartość $\langle L \rangle$:

1. „Przypadkowa" redukcja efektywnej liczby próbek, mająca miejsce, gdy kilka kolejnych próbek skwantowanego sygnału x_i^{q} przyjmuje taką samą wartość, mimo że w ogólności kolejne próbki przebiegu x_i mogą znacznie się różnić. Wyprowadzenie wyrażenia na $\langle L \rangle$ należy w tym przypadku oprzeć na rozkładzie prawdopodobieństwa wartości próbek sygnału skwantowanego. Z pobieżnej analizy wynika, że dla tego mechanizmu $\langle L \rangle$ jest malejącą funkcją n i rosnącą funkcją N_{S}.
2. „Bezwładnościowa" redukcja efektywnej liczby próbek, która zachodzi, gdy zmiany wartości kolejnych próbek w całym przebiegu x_i są nieznaczne (o mniej niż jeden poziom). Mechanizm ten dominuje, gdy dyskretyzacja przebiegu jest bardzo gęsta, czyli stosunek N_{S}/K jest odpowiednio duży. W tym przypadku $\langle L \rangle = \tau/T$, gdzie τ oznacza średni czas przejścia x_i^{q} między poziomami. Wydaje się, że czas ten można wyznaczyć szacując odwrotność charakterystycznego nachylenia sygnału, na które naturalnym kandydatem wydaje się być pierwiastek ze średniego kwadratu pochodnej. Wówczas, $\langle L \rangle \sim 2^{-n} \alpha N_{\mathrm{S}}/K$.

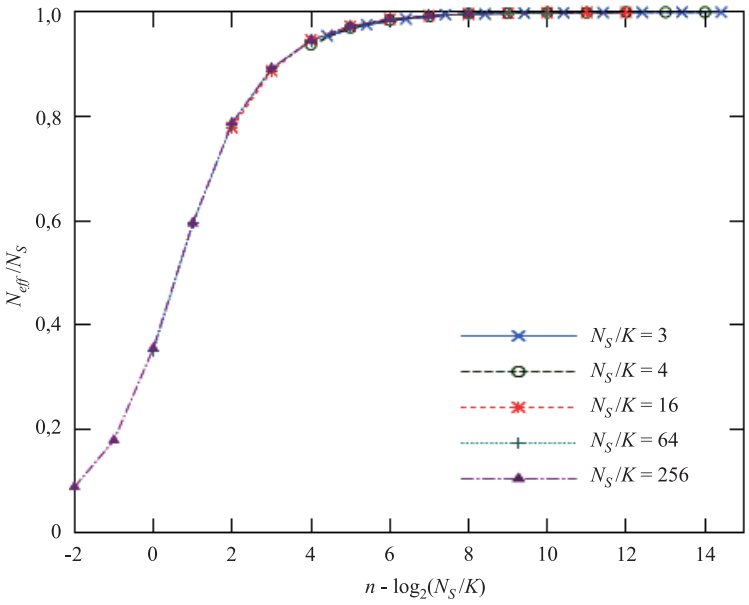
Dominujący jest ten mechanizm, który prowadzi do większej wartości $\langle L \rangle$.

Z przeprowadzonych obliczeń wynika, że stosunek $N_{\mathrm{eff}}/N_{\mathrm{S}}$ nie zależy od liczby podnośnych, zależy natomiast od gęstości dyskretyzacji N_{S}/K. Wyniki obliczeń numerycznych tak znormalizowanej liczby próbek znajdują się na rys. 4. Daje się zauważyć, że przy dużym nadpróbkowaniu i małej



Rys. 4. *Znormalizowana efektywna liczba próbek błędu odwzorowania poziomu $N_{\mathrm{eff}}/N_{\mathrm{S}}$ w funkcji rozdzielczości przetwornika n*

rozdzielczości n punkty określające efektywną liczbę próbek układają się wzdłuż krzywej o innym charakterze niż pozostałe – jest to obszar, w którym dominuje drugi, czyli „bezwładnościowy", mechanizm redukcji N_{eff}. Można także zauważyć, co obrazuje rys. 5, że wszystkie krzywe można



Rys. 5. *Znormalizowana efektywna liczba próbek błędu odwzorowania poziomu* $N_{\text{eff}}/N_{\text{S}}$ *w funkcji różnicy rozdzielczości przetwornika n i logarytmu z nadpróbkowania* N_{S}/K

„dopasować", przesuwając je o $\log_2(N_{\text{S}}/K)$ wzdłuż osi odciętych, a na dominujący mechanizm redukcji N_{eff} wskazuje znak różnicy $n - \log_2(N_{\text{S}}/K)$.

W rezultacie przedstawionych rozważań wynika, że dla składowej pseudolosowej

$$\left\langle \text{ev}_{\text{nls}}^2 \right\rangle = \frac{2K}{N_{\text{eff}}} \overline{\left(\Delta_{\text{s}}\left(x_i^{\text{q}}\right)\right)^2} = \frac{2K}{N_{\text{eff}}} \sigma_{\text{s}}^2. \tag{27}$$

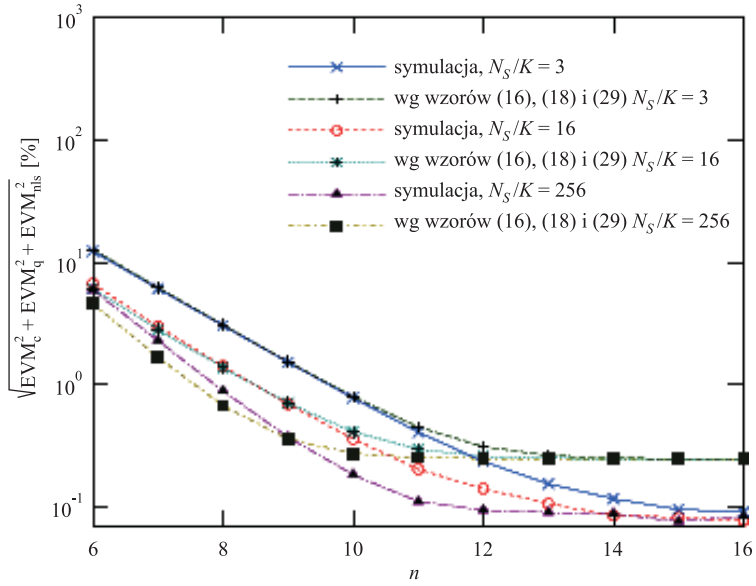
Producenci przetworników zazwyczaj podają nieliniowość różniczkową w najgorszym przypadku, czyli jej wartość maksymalną, co odpowiada $\text{DNL} = 2\max_p |\Delta_{\text{s}}(p)|$. Przy założeniu, że składowa pseudolosowa błędu ma rozkład jednostajny, $\sigma_{\text{s}}^2 = \text{DNL}^2/12$, to

$$\left\langle \text{ev}_{\text{nls}}^2 \right\rangle = \frac{K}{6N_{\text{eff}}} \text{DNL}^2, \tag{28}$$

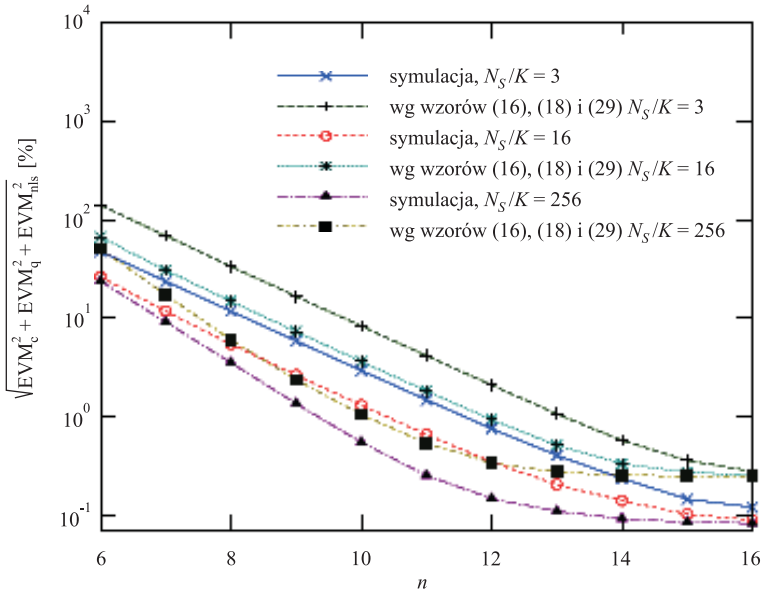
stąd:

$$\text{EVM}_{\text{nls}} = \sqrt{\frac{\left\langle \text{ev}_{\text{nls}}^2 \right\rangle}{\sigma^2}} = \sqrt{\frac{2K}{3N_{\text{eff}}}} \frac{\alpha \text{DNL}}{2^n - 2}. \tag{29}$$

Wprawdzie tak prosty model teoretyczny nie daje wyników pokrywających się z wynikami symulacji aż tak dokładnie, jak w przypadku błędu kwantyzacji, ale zapewnia zadowalającą zgodność oraz dobrze oddaje wpływ parametrów przetwornika i sygnału na jakość przetwarzania. Przykładowe wykresy, stanowiące porównanie wyników teoretycznych i numerycznych, znajdują się na rys. 6, rys. 7 i rys. 8. Widać z nich, że utworzony model daje wartości bardzo dobrze pokrywające się z wynikami symulacji przy mniejszych wartościach DNL, jednakże wciąż na tyle dużych, aby można było go

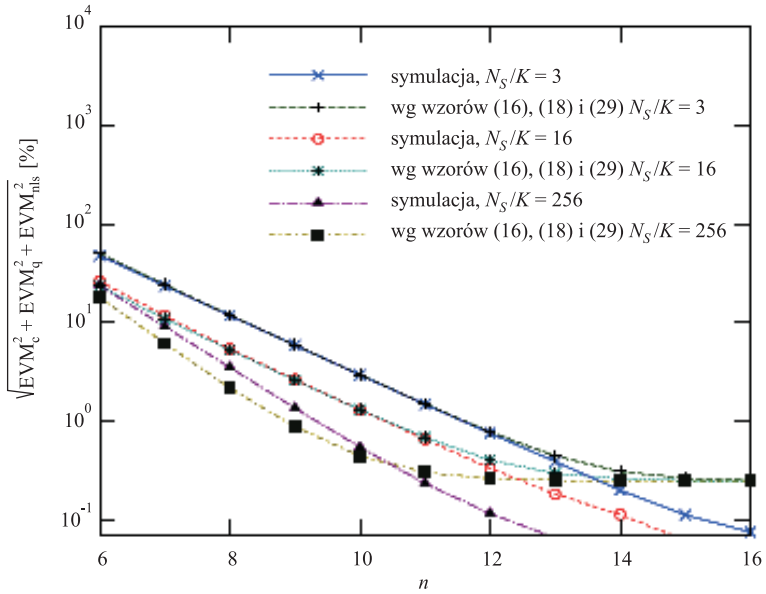


Rys. 6. EVM *wynikający z obcięcia sygnału, kwantyzacji i nieliniowości różniczkowej* DNL = 4 *w funkcji n dla różnych stosunków* N_S/K, *przy* $K = 2048$



Rys. 7. EVM *wynikający z obcięcia sygnału, kwantyzacji i nieliniowości różniczkowej* DNL = 16 *w funkcji n dla różnych stosunków* N_S/K, *przy* $K = 2048$

wykorzystać w praktyce. Daje się zauważyć, że przy większej liczbie podnośnych błędy szacowane wyrażeniem (29) zależą od K, co jest sprzeczne z wynikami symulacji. Natomiast w każdym przypadku krzywe teoretyczne i symulacyjne charakteryzują się takimi samymi nachyleniami. Oznacza to,



Rys. 8. EVM *wynikający z obcięcia sygnału, kwantyzacji i nieliniowości różniczkowej* DNL = 16 *w funkcji n dla różnych stosunków* N_S/K, *przy* $K = 256$

że wyrażenie (29) jest oparte na poprawnych założeniach i uwzględnia w odpowiedni sposób efekty składające się na błędy przetwarzania, dzięki czemu pozwala precyzyjnie określać, do jakich zmian prowadzą modyfikacje parametrów przetwornika lub sygnału (o zadanej liczbie podnośnych).

Wektor błędu składowej wolnozmiennej

Zniekształcenia sygnału (z pominięciem przesunięcia składowej stałej) pochodzące od składowej wolnozmiennej wynikają z różnic między błędami poziomów odpowiadających kolejnym próbkom sygnału skwantowanego. Dlatego, średnią moc wektora błędu tych zniekształceń można zapisać jako:

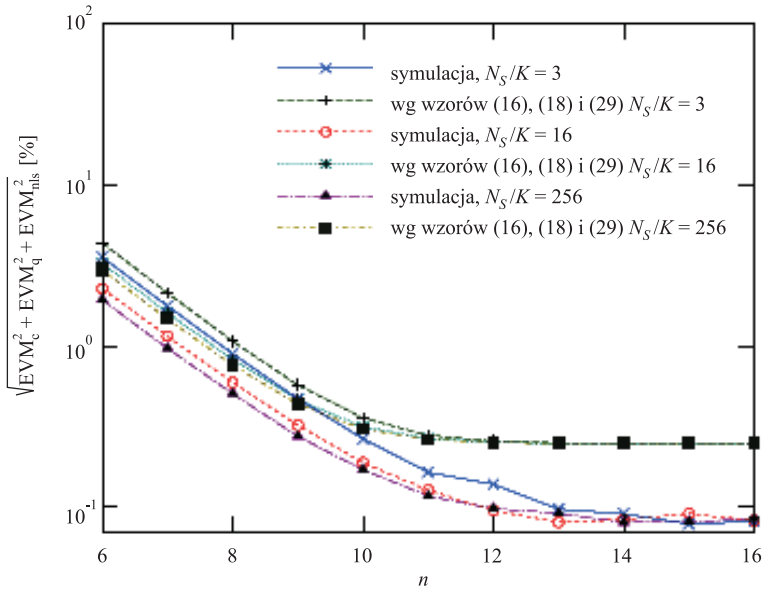
$$\left\langle \mathrm{ev}_{\mathrm{nld}}^2 \right\rangle = \overline{\left(\Delta_{\mathrm{d}}\left(x_{i+1}^{\mathrm{q}}\right) - \Delta_{\mathrm{d}}\left(x_i^{\mathrm{q}}\right)\right)^2}. \tag{30}$$

Błąd ten można powiązać z obydwiema nieliniowościami. Traktując wartość nieliniowości całkowej jako najgorszy przypadek, czyli maksymalne odchylenie od idealnej charakterystyki liniowej, $\mathrm{INL} = \max_p |\Delta(p)| = \max_p |\Delta_{\mathrm{d}}(p)| + \mathrm{DNL}/2$. Rozkład widmowy mocy błędu pochodzącego od składowej wolnozmiennej zależy od jej charakterystyki, dlatego w ogólnym oszacowaniu należy przyjąć, że cała moc błędu przypada na pasmo sygnału. Otrzymuje się wtedy wyrażenie:

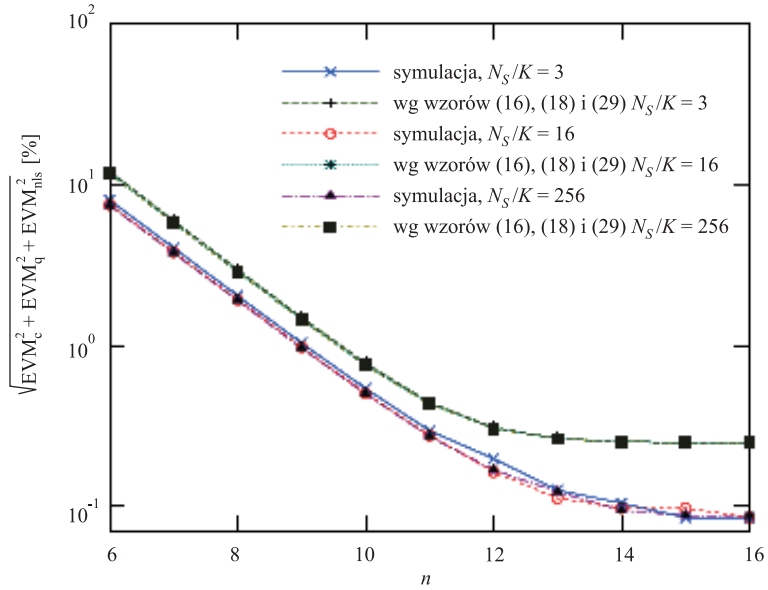
$$\mathrm{EVM}_{\mathrm{nld}} = \sqrt{\frac{\left\langle \mathrm{ev}_{\mathrm{nld}}^2 \right\rangle}{\sigma^2}} = S\left[x_i^{\mathrm{q}}\right] \frac{\alpha\,(2\,\mathrm{INL} - \mathrm{DNL})}{2^n - 2}, \tag{31}$$

z zależnym od przebiegu $\Delta_{\mathrm{d}}\left(x_i^{\mathrm{q}}\right)$ współczynnikiem

$$S\left[x_i^{\mathrm{q}}\right] = \sqrt{\frac{\overline{\left(\Delta_{\mathrm{d}}\left(x_{i+1}^{\mathrm{q}}\right) - \Delta_{\mathrm{d}}\left(x_i^{\mathrm{q}}\right)\right)^2}}{\max_p |\Delta_{\mathrm{d}}(p)|^2}}. \tag{32}$$



Rys. 9. EVM *wynikający z obcięcia sygnału, kwantyzacji i nieliniowości całkowej* INL = 2 *w funkcji n dla różnych stosunków* N_S/K



Rys. 10. EVM *wynikający z obcięcia sygnału, kwantyzacji i nieliniowości całkowej* INL = 8 *w funkcji n dla różnych stosunków* N_S/K

Przykładowe wyniki obliczeń numerycznych i teoretycznych porównane są na rys. 9 i rys. 10. Szacunki za pomocą opisanego modelu prowadzą do wartości przewyższających trochę wyniki symulacji. Aby uzyskać poprawę dokładności należy wyrażenie (31) uzupełnić o czynnik wskazujący jaki

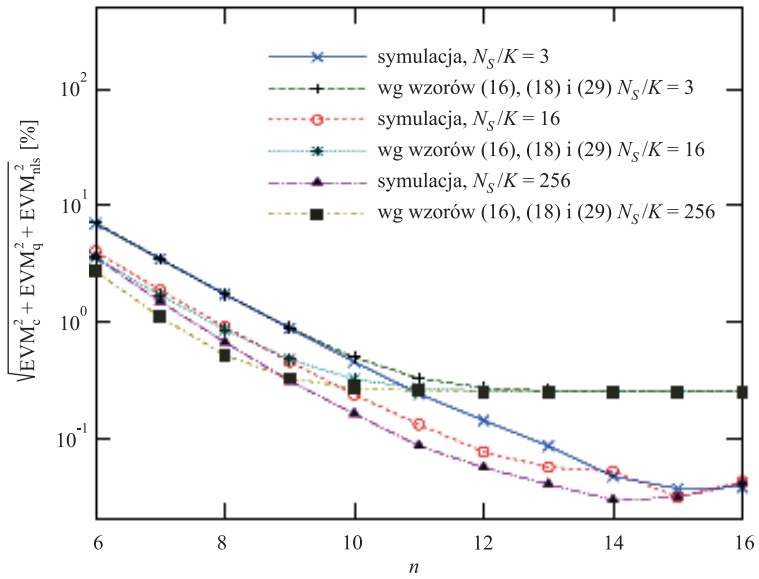
ułamek mocy wektora błędu przypada na pasmo sygnału. Widać jednak, że wyrażenie to zależy w poprawny sposób od uwzględnionych w nim parametrów przetwornika i sygnału. W szczególności można zauważyć, że symulacje przeprowadzone dla wartości INL = 8 (przy której błąd od składowej wolnozmiennej był dominującym błędem) potwierdzają, że gęstość dyskretyzacji nie ma wpływu na pogorszenie jakości przetwarzania przez deterministyczą część błędu $\Delta_{\mathrm{d}}\left(x_i^{\mathrm{q}}\right)$.

Całkowity błąd przetwarzania

Wyrażenia (16), (19), (29) oraz (31) umożliwiają wyznaczenie całkowitego błędu przetwarzania, co przy dopuszczalnej wartości EVM pozwala zapisać warunek na wymagane parametry przetwornika (9) w jawnej postaci:

$$\left(\frac{\alpha}{2^n-2}\right)^2\left[\frac{2K}{3N_{\mathrm{S}}}\left(1+\frac{N_{\mathrm{S}}}{N_{\mathrm{eff}}}\mathrm{DNL}^2\right)+S^2\left[x_i^{\mathrm{q}}\right](2\,\mathrm{INL}-\mathrm{DNL})^2\right]<\mathrm{EVM}^2-\mathrm{EVM}_{\mathrm{c}}^2. \tag{33}$$

Wynikają z niego dwa ważne wnioski. Pierwszy, że błąd przetwarzania można częściowo zmniejszyć przez zwiększenie liczby próbek sygnału. Wpływ na poprawę jakości przetwarzania jest największy, gdy charakterystyka błędu odwzorowania poziomu $\Delta(p)$ ma charakter przebiegu pseudolosowego (szybkozmiennego) i gdy rozdzielczość jest odpowiednio duża (co wynika z przeprowadzonej analizy zachowania się N_{eff}). Drugi, że zmiany progu obcięcia sygnału α wpływają nie tylko na poziom szumu obcięcia, ale także na pozostałe omawiane błędy. Jeżeli szum obcięcia jest pomijalny, aby utrzymać błąd przetwarzania na stałym poziomie, zmniejszenie rozdzielczości przetwornika wymaga zwiększenia amplitudy sygnału względem zakresu dynamicznego przetwornika, co odpowiada zmniejszeniu α i zwiększeniu błędu obcinania. W przybliżeniu zmiany te powinny być takie, aby stosunek $\alpha/2^n$ miał stałą wartość.



Rys. 11. EVM *przy obcięciu sygnału, kwantyzacji oraz nieliniowościach* DNL = 2 *i* INL = 2, *w funkcji n dla różnych stosunków* N_{S}/K, *przy* $K = 256$

Przykładowe wyniki otrzymane za pomocą utworzonego modelu oraz symulacji dla INL = 2 i DNL = 2 znajdują się na rys. 11. Widać, że wartości teoretyczne są bliskie wartościom pochodzącym z obliczeń numerycznych, a ponadto zachowanie krzywych jest identyczne, co świadczy o poprawności przewidywań modelu teoretycznego.

Podsumowanie

W niniejszej pracy przedstawiono prosty model analityczny do oszacowania ilościowego błędów wnoszonych do sygnału OFDM w procesie przetwarzania z postaci cyfrowej na analogową, jak też do określenia wymaganych parametrów, które zapewniają utrzymanie błędów przetwarzania poniżej założonego poziomu. Model ten stanowi narzędzie umożliwiające analizę dokładności przetwarzania i wybór optymalnego przetwornika C/A oraz odpowiednie dostosowanie parametrów samego sygnału. W konstrukcji modelu uwzględniono trzy składniki błędów: błąd obcięcia sygnału, błąd kwantyzacji oraz zniekształcenia nieliniowe. Do oszacowania błędu obcięcia sygnału przyjęto uproszczoną metodę opisaną w [5]. Wyprowadzone wyrażenie prowadzi do wartości malejących wolniej, niż pokazuje symulacja, jednakże znaczne rozbieżności występują dopiero, gdy szum obcięcia staje się bardzo mały ($EVM_c \ll 1\%$). Dla poprawy wyników należy zastosować dla tego składnika dokładniejsze wyrażenie lub wartości otrzymane numerycznie, jednakże w pierwszym przybliżeniu nie jest to konieczne.

Wyprowadzenie wyrażenia opisującego szum kwantyzacji oparto na założeniu, że jest to szum biały o próbkach z jednorodnym rozkładem prawdopodobieństwa, które jest bardzo dobrym przybliżeniem w przypadku sygnału OFDM. Dzięki temu, otrzymany wzór (18), pozwala bardzo dokładnie określić wielkość błędu kwantyzacji. Ze wzoru tego wynika, że wpływ kwantyzacji na dokładność przetwarzania zależy od rozdzielczości przetwornika, poziomu obcięcia sygnału, a także od nadpróbkowania sygnału. Jest to wniosek, którego nie można wyciagnąć na podstawie np. wyrażeń zamieszczonych w [6].

W przypadku ostatniego uwzględnionego źródła błędów przedtwarzania, tj. błędów odwzorowania poziomów przetwornika, rozróżniono błędy generowane przez regularną (wolnozmienną) i pseudolosową (szybkozmienną) część charakterystyki całkowitego błędu. Pokazano, że wpływ części wolnozmiennej zależy od jej przebiegu, natomiast część szybkozmienna ma wpływ podobny jak szum kwantyzacji, z tą różnicą, że w obliczeniach należy uwzględnić fakt, że kolejne próbki błędu mogą mieć jednakową wartość. Zdefiniowano w tym celu efektywną liczbę próbek, która pojawia się w ostatecznym wyrażeniu określającym stosowny składnik błędu przetwarzania.

Na podstawie wyprowadzonego wyrażenia (33) pokazano, że błędy przetwarzania można zmniejszać poprzez zwiększenie liczby próbek sygnału (nadpróbkowanie), otrzymując tym silniejszy efekt, im słabszy wpływ ma regularna część charakterystki błędu odwzorowania poziomu. Wyciągnięto także wniosek, że utrzymanie stałego poziomu błędów kwantyzacji i nieliniowych wymaga, z dobrym przybliżeniem, zachowania stałej wartości stosunku $\alpha/2^n$. Zdaniem Autorów, w literaturze światowej nie zostało dotychczas opublikowane podobne wyrażenie, opisujące proces przetwarzania C/A sygnału OFDM na takim poziomie ogólności.

Praca była współfinansowana ze środków Programu Operacyjnego Innowacyjna Gospodarka, projekt nr POIG.01.01.02-00-014/08.

Bibliografia

[1] *Analog-digital conversion*. Red. W. Kester, Analog Devices, 2004

[2] Colotti J.J.: *Dynamic evaluation of high-speed, high resolution D/A converters*. RF Design, November 1990, s. 51

[3] Come B. i in.: *Impact of front-end non-idealities on bit error rate performance of WLAN-OFDM transceivers*. Proc. 2000 IEEE RAWCON, 2000, s. 91–94

[4] Lee C., El-Tanany M.S., Goubran R.A.: *Impacts of non-ideal analog interfacing factors on OFDM baseband signals*. Proc. 2005 IEEE IMTC, 2005, s. 762–767

[5] Gross R., Veeneman D.: *SNR and spectral properties for a clipped DMT ADSL signal*. 1994 IEEE ICC Conf. Rec., 1994, z. 2, s. 843–847

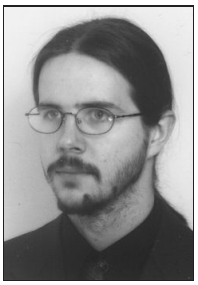
[6] Mehrnia A.: *Optimum DAC resolution for WMAN, WLAN and WPAN OFDM-based standards*. 2005 ICCE Dig. Techn. Papers, 2005, s. 355–356

[7] McKinley M.D. i in.: *EVM calculation for broadband modulated signals*. 64th ARFTG Conf. Dig., Orlando, grudzień 2004, s. 45–52

[8] *Spectrum of quantization noise and conditions of whiteness*. W: Widrow B., Kollár I.: *Quantization noise*. Cambridge, Cambridge University Press, 2008

[9] Maxim Integrated Products: *INL/DNL Measurements for High-Speed Analog-to-Digital Converter (ADCs)*. Nota aplikacyjna nr 283, wrzesień 2000

Adam Rudziński



Dr inż. Adam Rudziński (1980) – absolwent Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej (2004) oraz Wydziału Fizyki Uniwersytetu Warszawskiego (2009); praca zawodowa: projektowanie układów i urządzeń elektronicznych; zainteresowania naukowe: modelowanie układów elektronicznych i zjawisk w nich występujących, konstrukcje urządzeń elektronicznych, oddziaływanie promieniowania elektromagnetycznego z materią.
e-mail: arudzins@poczta.onet.pl
e-mail: adam.rudzinski@ire.pw.edu.pl

Sebastian Kozłowski

Mgr inż. Sebastian Kozłowski (1980) – absolwent Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej (2004); doktorant w Instytucie Radioelektroniki PW; zainteresowania naukowe: transmisja radiowa – systemy MIMO oraz OFDM.
e-mail: s.kozlowski@ire.pw.edu.pl

Wykaz ważniejszych konferencji – I półrocze 2011

Tytuł konferencji	Data	Miejsce	Adres internetowy
First International Conference on Computer Science and Information Technology (COSIT)	02.01–04.01	Bangalore, India	http://coneco2009.com/cosit/cosit.html
12th International Conference on Distributed Computing and Networking (ICDCN 2011)	03.01–05.01	Bangalore, India	http://icdcn.iitkgp.ac.in/
Third International Conference on Communication Systems and Networks (COMSNETS 2011)	04.01–08.01	Bangalore, India	http://www.comsnets.org/
International Conference on Systemic, Cybernetics and Informatics (ICSCI)	05.01–08.01	Hyderabad, India	http://www.icsci.net/
3rd International Conference on Computer Modeling and Simulation (ICCMS 2011)	07.01–09.01	Mumbai, India	http://www.iccms.org/cfp.htm
International Joint Conference on Information and Communication Technology	08.01–09.01	Bhubaneswar, India	http://www.interscience.ac.in/IJcICT-2011/ijcict2011.html
2nd International Conference on e-Education, e-Business, e-Management and e-Learning (IC4E 2011)	09.01–11.01	Mumbai, India	http://www.conferencealerts.com/seeconf.mv?q=ca16i8m8
IEEE Consumer Communications and Networking Conference (CCNC 2011)	09.01–12.01	Las Vegas, USA	http://www.ieee-ccnc.org/
IEEE Radio and Wireless Symposium	16.01–20.01	Phoenix, USA	http://rawcon.org/index.html
International Conference on e-Commerce, e-Administration, e-Society, e-Education, and e-Technology (e-CASE & e-Tech 2011)	18.01–20.01	Tokyo, Japan	http://www.e-case.org/2011/
Knowledge Management GigaCon	20.01	Warsaw, Poland	http://gigacon.org/knowledge_management
International Conference on Advanced Computing & Communication Technologies	21.01–23.01	Rohtak, India	http://rgconferences.com/acct11/
Interconnection World Forum	24.01–27.01	London, United Kingdom	http://www.iir-telecoms.com/event/interconnection

Tytuł konferencji	Data	Miejsce	Adres internetowy
2011 World Congress on Computer Science and Information Technology (WCSIT11)	24.01–27.01	Cairo, Egypt	http://www.conferencealerts.com/seeconf.mv?q=ca16sasm
DATA CENTER & STORAGE GigaCon	25.01	Warsaw, Poland	http://gigacon.org/datacenter_storage
6th Annual Prepaid Mobile Summit 2011	25.01–26.01	Bangkok, Thailand	http://www.prepaidmobilesummit.com/Event.aspx?id=383800
Systemy dla przedsiębiorstw GigaCon	26.01	Wrocław, Poland	http://gigacon.org/sdp_wroclaw_2011
DECT World & CAT-iq 2011	26.01–27.01	Amsterdam, The Netherlands	http://www.dectconference.com/
International Conference on Information Networking (ICOIN)	26.01–28.01	Kuala Lumpur, Malaysia	http://www.icoin.org/
8th International Conference on Wireless On-demand Network Systems and Services	26.01–28.01	Bardonecchia, Italy	http://conferenze.dei.polimi.it/wons2011/
International Conference on Health Informatics	26.01–29.01	Rome, Italy	http://www.healthinf.biostec.org/
International Conference On Telecommunication & Enabling Technologies	29.01–30.01	Islamabad, Pakistan	http://www.content2011.ioast.org/
5th WSEAS International Conference on Circuits, Systems, Signal and Telecommunications (CISST '11)	29.01–31.01	Puerto Morelos, Mexico	http://www.wseas.us/conferences/2011/mexico/cisst/
KARIERA IT GigaCon	05.02	Warsaw, Poland	http://gigacon.org/karierait
4th IFIP International Conference on New Technologies, Mobility and Security	07.02–10.02	Paris, France	http://ntms-conf.org/
IT w Ubezpieczeniach GigaCon	08.02	Warsaw, Poland	http://sdcenter.pl/ubezpieczenia
15th International Conference on Optical Networking Design and Modeling	08.02–10.02	Bologna, Italy	http://www.ondm2011.unibo.it/
International Conference on Communications and Signal Processing (ICCSP)	10.02–12.02	Kerala, India	http://iccsp2011.nitc.ac.in/
13th International Conference on Advanced Communication Technology	13.02–16.02	Gangwon-Do, Korea (South)	http://www.icact.org/
Baltic Congress on Future Internet Communications	16.02–18.02	Riga, Latvia	http://www.bcfic.org/
3rd International ICST Conference on Personal Satellite Services	17.02–18.02	Malaga, Spain	http://psats.eu/

Tytuł konferencji	Data	Miejsce	Adres internetowy
Second International Conference on Emerging Applications of Information Technology (EAIT 2011)	18.02–20.02	Kolkata, India	https://sites.google.com/site/csieait2011/
10th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications (EHAC '11)	20.02–22.02	Cambridge, United Kingdom	http://www.wseas.us/conferences/2011/cambridge/ehac/
World Congress on Internet Security (WorldCIS-2011)	21.02–23.02	London, United Kingdom	http://worldcis.org/
2011 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA 2011)	22.02–24.02	Miami Beach, USA	http://committees.comsoc.org/tco/
2011 International Conference on Communication and Electronics Information - ICCEI 2011	22.02–24.02	Haikou, China	http://www.iccei.org/
2nd International ICST Conference on Digital Business	23.02–24.02	London, United Kingdom	http://digibiz.org/
IEEE International Symposium on Wireless Pervasive Computing	23.02–25.02	Hong Kong, China	http://www.iswpc.org/2011/
8th European Conference on Wireless Sensor Networks (EWSN 2011)	23.02–25.02	Bonn, Germany	http://www.nes.uni-due.de/ewsn2011
International Conference on Devices and Communications	24.02–25.02	Ranchi, India	http://icdecom.bitmesra.ac.in/
3rd International Conference on Computer and Network Technology	26.02–28.02	Taiyuan, China	http://www.iccnt.org/
3rd International Conference on Wireless Information Networks & Business Information System (WINBIS)	27.02–01.03	Katmandu, Nepal	http://www.win-bis.com/
Kongres Bezpieczeństwa Sieci GigaCon	28.02	Warsaw, Poland	http://gigacon.org/kbs_2011
2nd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems	28.02–03.03	Chennai, India	http://www.wirelessvitaechennai.org/
1st National Conference on Soft Computing and Information Technology	03.03–04.03	Mahshahr, Iran	http://ncscit.ir/2011/
2011 International Conference on Communications, Computing and Control Applications (CCCA'11)	03.03–05.03	Hammamet, Tunisia	http://www.hypersciences.org/ccca11/
2011 International Conference on Software and Information Engineering (ICSIE 2011)	04.03–06.03	Kuala Lumpur, Malaysia	http://www.icsie.org/

Tytuł konferencji	Data	Miejsce	Adres internetowy
1st International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS)	05.03–07.03	Algarve, Portugal	http://www.peccs.org/
Optical Fiber Communication Conference	06.03–10.03	Los Angeles, USA	http://www.ofcnfoec.org/
Second International Conference on Recent Trends in Information, Telecommunication and Computing ITC 2011	10.03–11.03	Kochi, India	http://itc.engineersnetwork.org/2011/
5th International ICST Conference on Nano-Networks	14.03–16.03	Atlanta, USA	http://nanonets.org/
7th Annual CEM, CRM & Retention Conference	14.03–17.03	Vienna, Austria	http://www.iir-telecoms.com/event/CEM-CRM-Retention
2011 International Conference on Information and Computer Applications ICICA 2011	18.03–20.03	Dubai, UEA	http://www.icica.org/
2011 International Conference on Network Communication and Computer - ICNCC 2011	19.03–20.03	New Delhi, India	http://www.icncc.org/
Telecoms Fraud & Revenue Assurance	21.03–23.03	London, United Kingdom	http://www.iir-telecoms.com/event/fraudrev
Telecoms Regulation Forum	21.03–25.03	London, United Kingdom	http://www.iir-telecoms.com/event/regulation
IEEE International Conference on Pervasive Computing and Communications	21.03–25.03	Seattle, USA	http://www.percom.org/
4th International ICST Conference on Simulation Tools and Techniques	21.03–25.03	Barcelona, Spain	http://simutools.org/2011/
3rd International ICST Conference on IT Revolutions	23.03–25.03	Cordoba, Spain	http://itrevolutions.org/2011/
International Conference on Information Science and Technology	26.03–28.03	Nanjing, China	http://icist.mae.cuhk.edu.hk/
5th International Symposium on Medical Information and Communication Technology	27.03–30.03	Montreux, Switzerland	http://www.ismict2011.org/
IEEE Wireless Communications and Networking Conference (WCNC)	28.03–31.03	Cancun, Mexico	http://www.ieee-wcnc.org/2011/
International Conference on Communications and Information Technology ICCIT-2011	29.03–31.03	Aqaba, Jordan	http://iccit-conf.org/
2011 International Conference on Communications and Networking Application (ICCNA 2011)	01.04–02.04	Bali, Indonesia	http://www.grs-association.org/iccna2011/

Tytuł konferencji	Data	Miejsce	Adres internetowy
2011 International Conference on Computer and Communication Devices ICCCD 2011	01.04–03.04	Bali, Indonesia	http://www.icccd.org/
15th IEEE International Symposium on Power Line Communications and its Applications	03.04–06.04	Udine, Italy	http://www.ieee-isplc.org/
30th IEEE International Conference on Computer Communications (IEEE INFOCOM 2011)	10.04–15.04	Shanghai, China	http://www.ieee-infocom.org/2011/
8th IEEE International Conference on Networking, Sensing and Control - ICNSC 2011	11.04–13.04	Delft, The Netherlands	http://sinfras.com/conferences/icnsc2011/
IEEE International Conference on RFID	12.04–14.04	Orlando, USA	http://www.ieee-rfid.org
Wireless Telecommunications Symposium	13.04–15.04	New York, USA	http://www.csupomona.edu/~wtsi/
International Conference on Consumer Electronics, Communications and Networks (CECNet 2011)	16.04–18.04	Xianning, China	http://www.cecnetconf.org/
12th annual IEEE Wireless and Microwave Technology (WAMI) Conference	18.04–19.04	Clearwater, USA	http://www.wamicon.org/
Advances in Information Technology and Mobile Communication (AIM 2011)	21.04–22.04	Nagpur, India	http://aim.engineersnetwork.org/2011/
3rd International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC)	23.04–24.04	Wuhan, China	http://www.nswctc.org/
EUROCON 2011 - International Conference on Computer as a Tool	27.04–29.04	Lisbon, Portugal	http://www.eurocon2011.it.pt/
17th European Wireless Conference	27.04–29.04	Vienna, Austria	http://www.ew2011.org/
IEEE International Symposium on Dynamic Spectrum Access Networks (DYSPAN)	03.05–06.05	Aachen, Germany	http://www.ieee-dyspan.org/2011/
International Conference on E-Business and E-Government (ICEE2011)	06.05–08.05	Shanghai, China	http://www.submitpaper.org/icee/index.htm
7th International Conference on Web Information Systems and Technologies (WEBIST)	06.05–09.05	Noordwijkerhout, The Netherlands	http://www.webist.org/
18th International Conference on Telecommunications ICT 2011	08.05–11.05	Ayia Napa, Cyprus	http://www.ict2011.org/

Tytuł konferencji	Data	Miejsce	Adres internetowy
3rd International ICST Conference on Mobile Lightweight Wireless Systems	09.05–11.05	Bilbao, Spain	http://mobilight.org/
International Symposium of Modeling and Optimization of Mobile, Ad Hoc, and Wireless Networks	09.05–13.05	Princeton, USA	http://www.ourglocal.com/event/?eventid=5969
2011 International Conference on Network Computing and Information Security (NCIS'11) and the 2011 International Conference on Multimedia and Signal Processing (CMSP'11)	14.05–15.05	Guilin, China	http://ncis-cmsp2011.gxnu.edu.cn/
IEEE 73rd Vehicular Technology Conference	15.05–18.05	Budapest, Hungary	http://www.ieeevtc.org/vtc2011spring/
2011 IEEE International Conference on Electro/Information Technology	15.05–20.05	Mankato, USA	http://www.eit-conference.org/eit2011/
12th ACM International Symposium on Mobile Ad Hoc Networking and Computing	16.05–17.05	Paris, France	http://www.sigmobile.org/mobihoc/2011/
8th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON 2011)	17.05–20.05	Khon Kaen, Thailand	http://www.ecti-con2011.org/main/
36th International Conference on Acoustics, Speech and Signal Processing	22.05–27.05	Prague, Czech Republic	http://www.icassp2011.com/
TETRA World Congress	24.05–27.05	Budapeszt, Hungary	http://www.iir-telecoms.com/event/twc2011
10th WSEAS International Conference on Telecommunications and Informatics (TELE-INFO '11)	27.05–29.05	Lanzarote, Spain	http://www.wseas.us/conferences/2011/lanzarote/tele-info/
6th International ICST Conference on Cognitive Radio Oriented Wireless Networks	31.05–03.06	Yokohama, Japan	http://crowncom.org/2011/
IASTED International Conference on Wireless Communications (WC 2011)	01.06–03.06	Vancouver, Canada	http://www.iasted.org/conferences/home-730.html
International Conference on Recent Trends in Information Technology	03.06–05.06	Chennai, India	http://www.annauniv.edu/icrtit/
IEEE International Conference on Communications ICC2011	05.06–09.06	Kyoto, Japan	http://www.ieee-icc.org/2011/
10th TTCN-3 User Conference 2011	07.06–09.06	Bled, Slovenia	http://www.ttcn3uc.eu/

Tytuł konferencji	Data	Miejsce	Adres internetowy
2011 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting	08.06–10.06	Nuremberg, Germany	http://www.ieee-bmsb2011.org
4th IEEE International Conference on Computer Science and Information Technology (ICCSIT 2011)	10.06–12.06	Chengdu, China	http://www.iccsit.org/
Future Network and Mobile Summit 2011	15.06–17.06	Warsaw, Poland	http://www.futurenetworksummit.eu/2011/
9th International Conference on Wired/Wireless Internet Communications - WWIC 2011	15.06–17.06	Barcelona, Spain	http://www.craax.upc.edu/WWIC11/
9th International Navigational Symposium on Marine Navigation and Safety of Sea Transportation (TRANS-NAV 2011)	15.06–17.06	Gdynia, Poland	http://transnav.am.gdynia.pl/
11th International Conference on Telecommunications	15.06–17.06	Graz, Austria	http://www.contel.hr/2011
International Conference on Digital Information and Communication Technology and its Applications	21.06–23.06	Dijon, France	http://www.sdiwc.net/fr/
International Conference on Advances in Information and Communication Technologies	22.06–23.06	Bangkok, Tailand	http://ict.engineersnetwork.org/2011/
4th International ICST Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications (Mobilware 2011)	22.06–24.06	London, United Kingdom	http://mobilware.org/
13th International Conference on Transparent Optical Networks and 3rd Annual Conference of COST Action MP0702:Towards Functional Sub-Wavelength Photonic Structures	26.06–30.06	Stockholm, Sweden	http://www.itl.waw.pl/icton2011
International Conference on Computer Science and Service System	27.06–29.06	Nanjing, China	http://www.cssconf.org/
International Conference on Information Society (i-Society 2011)	27.06–29.06	London, United Kingdom	http://www.i-society.eu/
3rd International Conference on Immersive Telecommunications (IMMERSCOM 2009)	27.06–29.06	Istanbul, Turkey	http://immerscom.org/
16th IEEE Symposium on Computers and Communications (ISCC'11)	28.06–01.07	Kerkyra, Greece	http://www.ieee-iscc.org/2011/
International Symposium on Signals,	30.06–01.07	Iasi,	http://scs.etti.tuiasi.ro/isscs2011/

Opracowanie: mgr inż. Barbara Przyłuska

Protection of telecommunication/ information networks against electromagnetic terrorism and unintentional EMI

Ryszard Strużak

This article discusses protection of telecommunication/information networks against electromagnetic interference (EMI) from the viewpoint of potential terrorist threats and development of Information Society. Both unintentional and intentional interference cases are covered and critical infrastructures, threats, and recommendations are discussed. References are made both to literature and author's experience during work at the EMC Laboratories of National Institute of Telecommunications in Wrocław, Poland.

cybercrime, EM sabotage, EM terrorism, EMI, IEMI, EMC, EMP, EW, HMP, RFI, Information Society, Networked Information Systems

Environmental protection against electromagnetic non-ionizing radiation

Marta Macher

Marek Kałuski

Karolina Skrzypek

The paper describes the effects of electromagnetic fields from various sources on the human body and the magnitude of health risk. The authors have analyzed the rules for determining field limits in Poland and worldwide applicable to general public and people working near field sources. The paper presents activities of the National Institute of Telecommunications in the field of electromagnetic compatibility and measurements of electromagnetic fields for occupational health and safety or environmental protection.

electromagnetic field sources, non-ionizing radiation effects on humans, allowable levels of electromagnetic fields

Regulatory policy concerning next generation networks

Stanisław Piątek

The paper presents the process of formulating telecommunications policy of the European Union concerning next generation access (NGA) networks, as well as economic, technical and information factors forcing changes to existing regulation developed for copper networks. It also indicates fundamentals of new regulatory approach and network elements and hubs subject to regulation in NGA environment. Basic investment conditions for various types of FTTx networks are evaluated together with principles of wholesale price control and options for withdrawal of regulatory measures. Finally, the risks associated with dismantling of existing access points to incumbent operator's network and options for resolution of resulting disputes with alternative operators are discussed.

next generation networks, next generation access, FTTH, European Commission recommendation, ladder of investment

InHousePLC systems – overview, development trends and applications

Henryk Gut-Mostowy

In this paper a general overview of contemporary communication systems based on InHousePLC technology is presented. Components of these systems, as well as transmission medium and frequency bandwidth used are shortly described. The physical and link layers, as well electromagnetic compatibility issues of such systems are also discussed. Main suppliers of InHousePLC hardware are presented together with directions of development and possible application areas.

BPLC systems, InHousePLC systems, Multimedia Home Networking, smart buildings

Resolution and nonlinearity requirements for D/A converter for OFDM signal

Adam Rudziński

Sebastian Kozłowski

This paper presents an analytic model allowing to determine errors introduced into an OFDM signal by digital-to-analog (D/A) conversion. Expressions for evaluation of necessary resolution and acceptable nonlinearity to keep the signal's distortion below a required level have been proposed.

digital-to-analog converter, OFDM modulation, quantization noise, integral nonlinearity, differential nonlinearity