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.

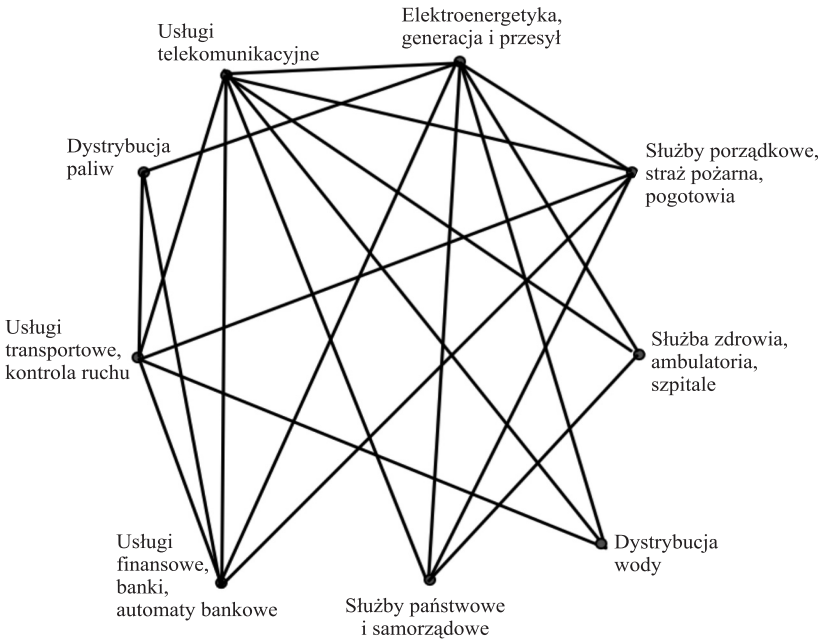
Już obecnie obserwuje się wzrastające uzależnienie od różnych urządzeń i systemów kontrolujących nasze życie. Poranny komunikat meteorologiczny w radiu decyduje o tym jak się ubierzemy. Sprawna winda w domu, w którym mieszkamy i sprawne światła regulujące ruch na skrzyżowaniu ulicy, którą idziemy decydują, 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.

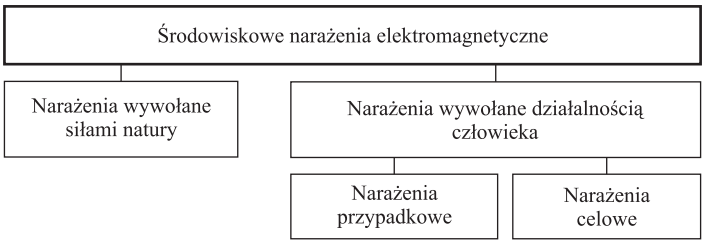
Zagrożenia i narażenia elektromagnetyczne

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

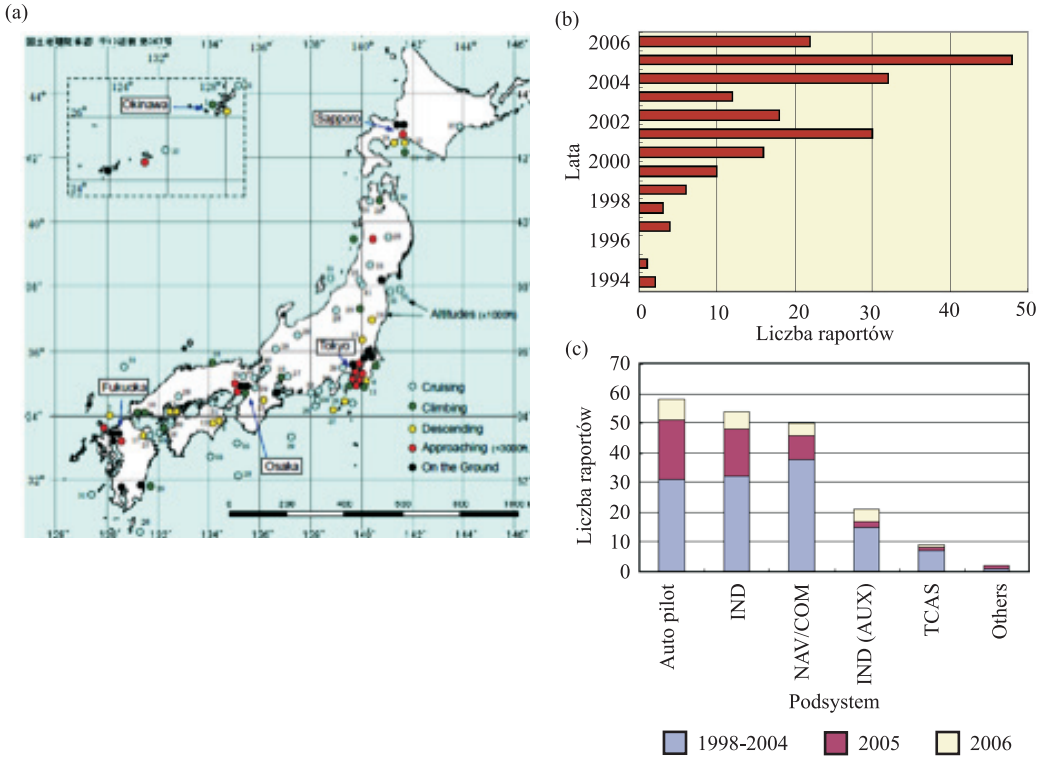
Sprawność transportu warunkuje efektywność wielu usług, jak pokazano na rysunku 1. Nawet prosta awaria sygnalizacji świetlnej w ruchu ulicznym może utrudnić akcje straży pożarnej i pogotowia; dużo poważniejsze następstwa może mieć awaria systemu kontroli lotów. Mimo wysiłków podejmowanych w celu zwiększenia 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)*

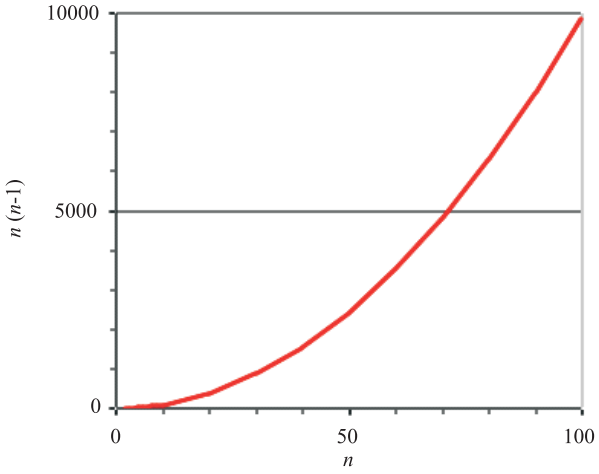
drzwi garażu. Komentował ten fakt następująco (w swobodnym przekładzie): „To jest dość niewygodne w czasie pracy w ogrodzie, ale naprawdę uciążliwe podczas odprawiania nabożeństwa”[①].

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

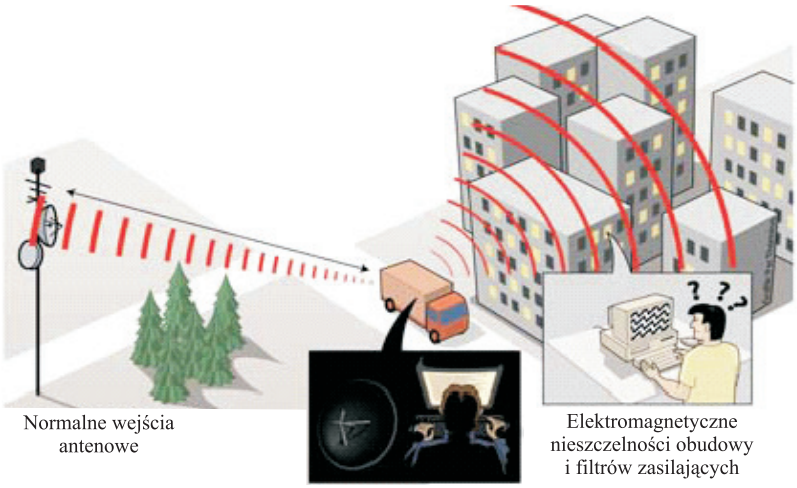
Niezamierzone narażenia elektromagnetyczne mogą prowadzić do poważnych następstw. Występują one wskutek zbiegu okoliczności, w przypadkowych miejscach i przypadkowych momentach. Tutaj zostaną omówione narażenia zamierzone, które mogą mieć następstwa jeszcze bardziej poważne; mogą być celowo wywoływane 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.

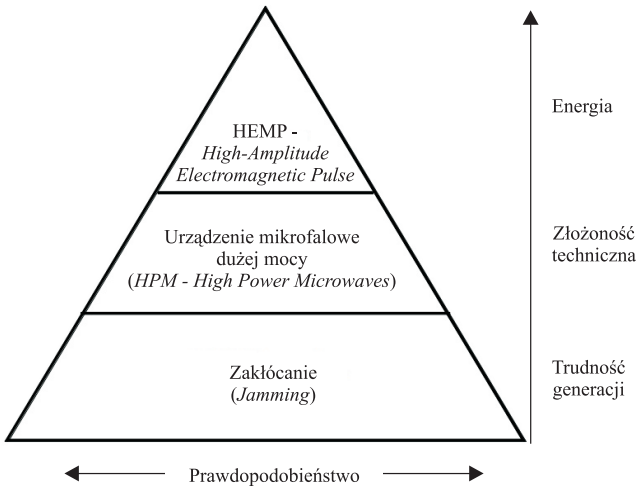
Atak elektromagnetyczny jest łatwiejszy w sieciach bezprzewodowych niż w sieciach kablowych, ponieważ może być dokonany na odległość. To dotyczy także przechwytywania informacji (*Intelligence, Signals Intelligence* (SIGINT), *Electronics Intelligence* (ELINT), *Foreign Instrumentation Signals Intelligence* (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.

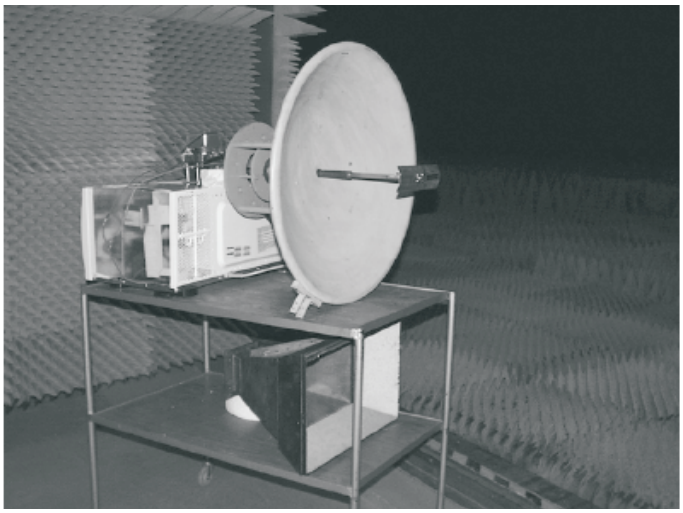
Składa się ono z elementów domowej kuchenki mikrofalowych i anteny do odbioru telewizji satelitarnej, łatwo dostępnych na rynku. Urządzenie to wytwarza energię elektromagnetyczną wystarczającą do zakłócenia lub zniszczenia na odległość wrażliwych elementów infrastruktury teleinformatycznej: układy scalone 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.*

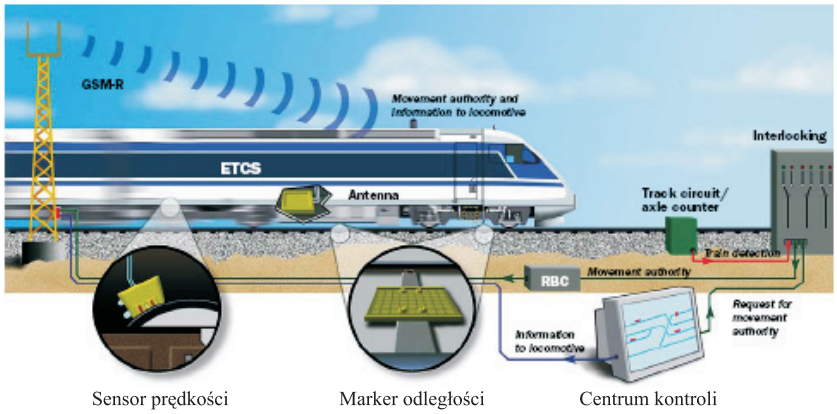
– modulacja CW, AM.

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

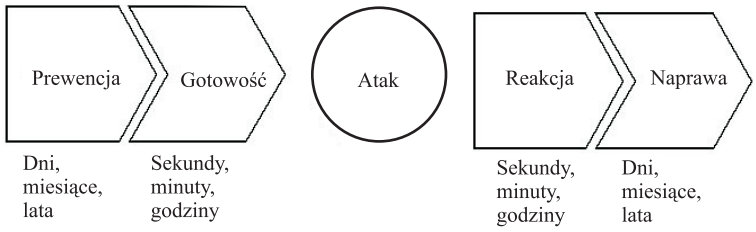
Ochrona przed narażeniami elektromagnetycznymi to problem holistyczny, w którym przeplatają się elementy techniczne, organizacyjne, ekonomiczne i socjalne (rysunek 10).

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.

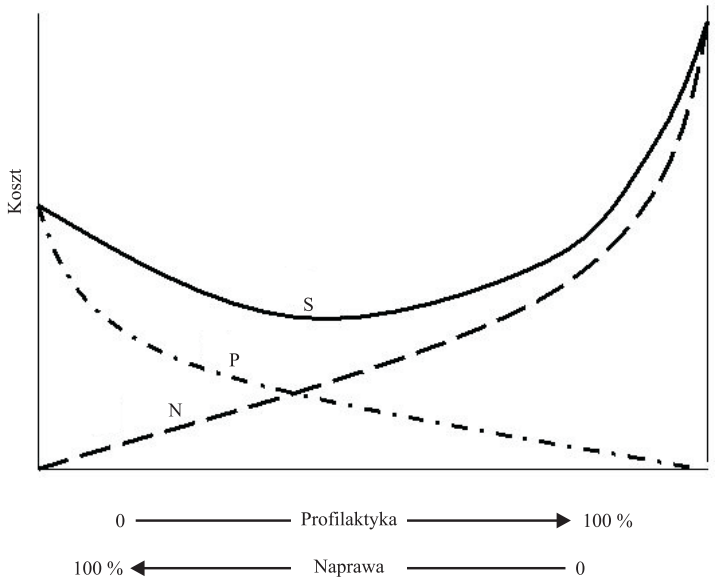
Proces obejmuje różne fazy: prewencję (uodpornienie), przygotowania na wypadek ataku, protekcję w czasie ataku, oraz ratunek i naprawę szkód po ataku, jak pokazano na rysunku 11.

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.

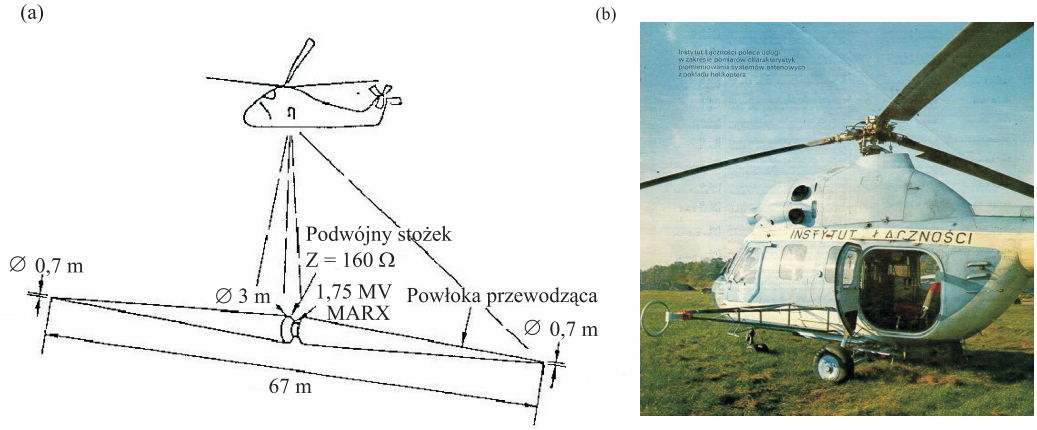
Odporność na atak

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]

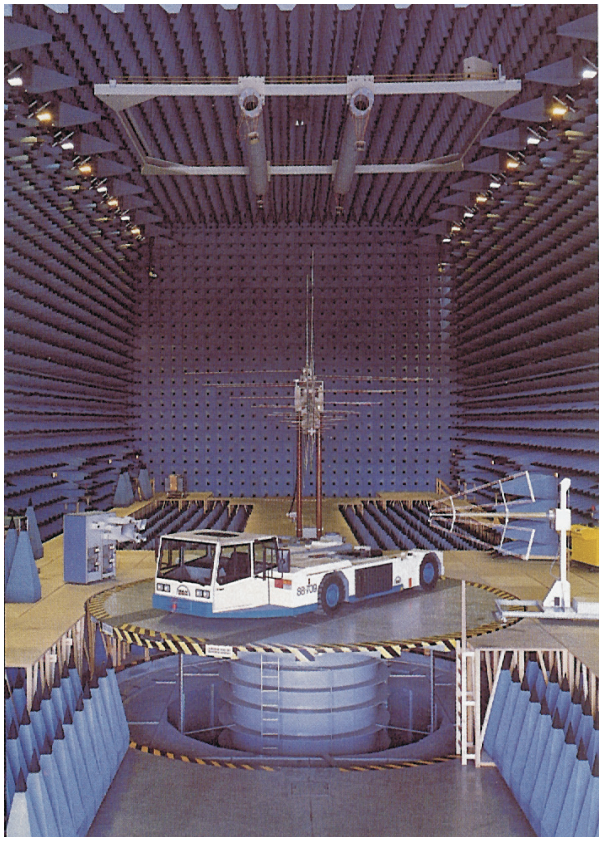
Rysunek 15 przedstawia widok jednego z amerykańskich stanowisk pomiarowych do oceny odporności stacji bazowych telefonii komórkowej na narażenia elektromagnetyczne, a rys. 16 widok stanowiska pomiarowego do badania odporności aparatury elektronicznej w samolocie na narażenia elektromagnetyczne[①]. Przedmiot 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

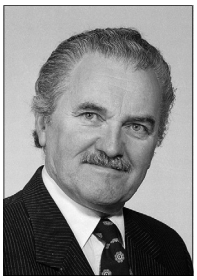
[37] Wik M. W.: *What is Network-Based Defence (NBD) and the Impact on the Future Defence?* Royal Swedish Academy of War Sciences, October 2003

[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