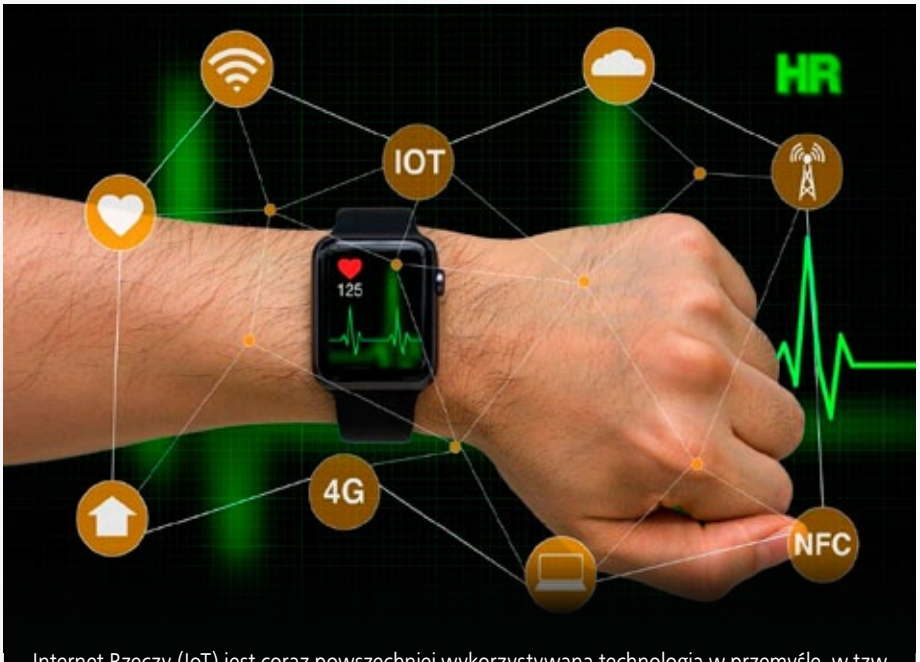
dr hab. inż. PATRYK ZRADZIŃSKI (ORCID: 0000-0001-8094-0761)
dr hab. inż. JOLANTA KARPOWICZ (ORCID: 0000-0003-2547-2728)
dr hab. inż. KRZYSZTOF GRYZ (ORCID: 0000-0001-5655-2187)
Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy
Kontakt: pazra@ciop.pl
DOI: 10.5604/01.3001.0014.8771

Charakterystyka emisji elektromagnetycznych związanych z użytkowaniem nasobnych urządzeń działających w technologii Internetu Rzeczy



Fot./Bigstockphoto

Internet Rzeczy (IoT) jest coraz powszechniej wykorzystywaną technologią w przemyśle, w tzw. inteligentnych miastach i domach czy w monitoringu stanu zdrowia. Artykuł prezentuje charakterystykę emisji elektromagnetycznych różnych technologii łączności bezprzewodowej wykorzystywanych w IoT (WiFi, Bluetooth, RFID, Zig-Bee, sieci komórkowe itp.). Przedstawiono w nim również kryteria i metody oceny zawodowych zagrożeń elektromagnetycznych związanych z użytkowaniem takich urządzeń.

Słowa kluczowe: urządzenia łączności bezprzewodowej, inżynieria środowiska, inżynieria biomedyczna, pole elektromagnetyczne, symulacje numeryczne, szybkość pochłaniania właściwego energii (SAR)

Characteristics of electromagnetic emissions related to the use of wearable devices operating within the Internet of Things technology

The Internet of Things (IoT) is an increasingly popular technology in industry, so-called smart cities and homes, or health monitoring. The article presents the characteristics of electromagnetic emissions of various wireless communication technologies used in IoT (WiFi, Bluetooth, RFID, Zig-Bee, cellular networks, etc.). It also presents criteria and methods for the assessment of occupational electromagnetic hazards related to the use of such devices.

Keywords: wireless communication devices, environmental engineering, biomedical engineering, electromagnetic field, numerical simulations, specific energy absorption rate (SAR)

Wstęp

Internet Rzeczy (*IoT, ang. Internet of Things*) to koncepcja sieci łączącej przewodowo lub bezprzewodowo urządzenia charakteryzujące się autonomicznym (niewymagającym zaangażowania człowieka) działaniem w zakresie pozyskiwania, udostępniania, przetwarzania danych lub wchodzenia w interakcje z otoczeniem pod wpływem tych danych [1, 2]. IoT, działający z wykorzystaniem sieci telekomunikacyjnych i systemów informatycznych o wysokim stopniu rozproszenia, ma służyć między innymi tworzeniu inteligentnych systemów kontrolno-pomiarowych, analitycznych, czy układów sterowania, praktycznie w każdej dziedzinie życia, gospodarki czy nauki. Z punktu widzenia architektury informatycznej, IoT jest koncepcją współpracujących warstw: sprzętowej, komunikacyjnej, aplikacyjnej i integracyjnej, która umożliwia współpracę (interoperacyjność) różnorodnych systemów teleinformatycznych wspierających rozmaite zastosowania dziedzinowe.

Zgodnie z ISO 19731:2017 IoT jest „infrastrukturą połączonych obiektów, ludzi, systemów i zasobów informacyjnych wraz z inteligentnymi usługami, aby umożliwić im przetwarzanie informacji o świecie fizycznym i wirtualnym oraz reagowanie na nie" [3].

Jedną z podstawowych funkcjonalności, rozwijanych w ramach IoT, jest komunikacja typu M2M (ang. Machine-to-Machine; Maszyna-z-Maszyną), obejmująca szeroką gamę rozwiązań komunikacyjnych służących do wymiany informacji, a także urządzenia nasobne (nazywane także ubieralnymi, ang. wearables, będące częścią odzieży lub zlokalizowane przy/na ciele użytkownika). Wśród zastosowań nasobnych urządzeń IoT znajdują się między innymi: urządzenia do zdalnego monitorowania parametrów medycznych; urządzenia do monitorowania lokalizacji pracowników, personelu medycznego, pacjentów, czy urządzenia do monitorowania parametrów środowiska pracy i ostrzegania pracowników przed zagrożeniami.

Dane przedstawione na portalu nowoczesnego przemysłu (Industry 4.0) wskazują, że szacunkowa liczba urządzeń połączonych do sieci w 2018 roku to ok. 35 miliardów, a do końca 2020 r. prognozowano około 50 miliardów, natomiast najnowsze dane opublikowane przez firmę Cisco szacują te liczby na ok. 18 miliardów w 2018 roku, 22 miliardy w 2020 roku i około 29 miliardów w 2023[1].

Celem artykułu jest scharakteryzowanie pola elektromagnetycznego emitowanego przez nasobne urządzenia działające w technologii IoT oraz przybliżenie tematyki dotyczącej kryteriów i metod oceny zawodowych zagrożeń elektromagnetycznych związanych z użytkowaniem takich urządzeń.

Zastosowania IoT w przemyśle, środowisku medycznym i życiu codziennym

Do przykładowych zastosowań IoT w przemyśle należą między innymi: inteligentna produkcja; identyfikacja materiału, produktu, towarów lub pogorszenia jakości produktu; zarządzanie magazynem, operacje zakupowe i szybka płatność; monitorowanie zakładów przemysłowych; diagnostyka pojazdu w czasie rzeczywistym, jazda wspomagana; zarządzanie bagażami na lotnisku, operacje wejścia na pokład samolotu, bilety mobilne; lokalizacja zwierząt, certyfikacja, kontrola handlu; zarządzanie gospodarstwem; nawadnianie, monitorowanie produkcji rolnej i pasz; kontrola produkcji rolnej; identyfikacja zarażonych zwierząt lub upraw w celu uniknięcia rozprzestrzeniania się chorób zakaźnych; globalna ogólnodostępna baza danych zwierząt hodowlanych zawierająca dane demograficzne, rodowód zwierzęcia, choroby, szczepienia, kontrole weterynaryjne; dostęp w czasie rzeczywistym do optymalizujących hodowlę danych o stanie zdrowia zwierząt, na przykład temperatury ciała.

IoT jest również szeroko wykorzystywane w środowisku medycznym i życiu codziennym między innymi do: monitorowania lokalizacji sprzętu medycznego, zapasów produktów jednorazowego użytku, procesu sterylizacji narzędzi, przedmiotów medycznych, leków i farmaceutyków, pacjentów i personelu; identyfikacji i monitorowania lokalizacji materiału biologicznego w badaniach diagnostycznych; kontroli dostępu do pomieszczeń i sektorów placówki medycznej; zdalnego monitorowania parametrów medycznych (np. pomiar temperatury, tętna, poziomu cukru - zarówno w placówkach medycznych jak i w domu); monitorowania funkcjonowania osób starszych i z niepełnosprawnościami (np. w celu podniesienia alarmu, gdy konieczna jest kontrola medyczna lub hospitalizacja w przypadku pogorszenia stanu zdrowia lub nagłego wypadku).

[1] http://przemysl-40.pl

Technologie i standardy komunikacji bezprzewodowej

Technologia IoT wykorzystuje różne technologie łączności i bezprzewodowej transmisji danych (np. WiFi, Bluetooth, RFID, Zig-Bee, sieci komórkowe itp.), [4-8]. Często poszczególne urządzenia IoT korzystają z dwóch technologii łączności bezprzewodowej, np. Bluetooth i WiFi w bezprzewodowych sieciach sensorowych (WSN, ang. *Wireless Sensor Network*) czy RFID i WiFi w systemach lokalizacji w czasie rzeczywistym (*RTLS, ang. Real-Time Locating System).* Źródłami pola elektromagnetycznego w technologii IoT są zarówno urządzenia wyposażone w czujniki (np. hałasu, temperatury, stężenia substancji chemicznych, ruchu, parametrów pracy organizmu żywego itp.) lub alarmujące (np. ostrzegające pracowników o wystąpieniu sytuacji awaryjnych), jak również moduły komunikacyjne (elementy sieci łączności bezprzewodowej) łączące elementy sieci IoT [5, 6].

Technologie, protokoły i standardy komunikacji bezprzewodowej o podstawowych parametrach przedstawionych w tabeli, które obecnie mogą być zastosowane w IoT, to: [4-8]:

- **WiFi** (ang. Wireless Fidelity) – technologia lokalnej sieci bezprzewodowej, bazująca na specyfikacjach IEEE 802.11x, jest w dużej mierze wykorzystywana przez urządzenia IoT w automatyce domowej (np. w tzw. inteligentnych domach). WiFi wykorzystuje pasma częstotliwości (2,400 – 2,4835; 5,150 – 5,350 i 5,470 – 5,725) GHz, od których popularnie oznacza się ją odpowiednio, jako WiFi 2G oraz WiFi 5G. W ostatnim czasie wprowadzono WiFi HaLow, które umożliwia łączność przy niskim zużyciu energii wymaganym w zastosowaniach wykorzystujących nasobne czujniki i urządzenia, w tzw. inteligentnych miastach i domach lub w pojazdach autonomicznych.
- **RFID** (ang. *Radio Frequency IDentification*) – technologia identyfikacji wykorzystująca fale radiowe do bezprzewodowego przesyłania danych lub zasilania pasywnego znacznika/taga (tj. elektronicznego układu stanowiącego etykietę identyfikującą obiekt włączony do systemu RFID). Stosowana jest w takich obszarach, jak: kontrola dostępu do przejść, budynków, pomieszczeń czy mebli, lokalizacja oznakowanych obiektów w systemach przeciwkradzieżowych w placówkach handlowych, bibliotecznych, magazynach, szpitalach itp., kontrola czasu pobytu, w systemach opłat drogowych, w zbliżeniowych kartach płatniczych i kartach komunikacji miejskiej, aż po identyfikację materiałów niebezpiecznych i lokalizację kontenerów w systemach magazynowych, lokalizację narzędzi budowlanych, lokalizację maszyn górniczych czy kontrolę czasu w sporcie, oznakowanie zwierząt, a nawet pacjentów. Ze względu na pasmo częstotliwości, systemy RFID można podzielić na: LF (ang. *Low Frequency*), HF (ang. *High Frequency*), UHF (ang. *Ultra-High Frequency*) oraz SHF (ang. *Super High Frequency*).
- **NFC** (ang. *Near Field Communication*) – protokół komunikacyjny, który umożliwia urządzeniom bezprzewodowe udostępnianie informacji przy ich bezpośredniej bliskości (przy oddaleniu nie przekraczającym 20 cm). NFC jest szeroko stosowany w aplikacjach do udostępniania danych osobowych (takich, jak: kontakty, wizytówki, zdjęcia, filmy), transakcji finansowych, dostępu do informacji w inteligentnych plakatach itp. Jest uważany za ewolucję technologii RFID, poprzez dodanie do niej możliwości komunikacji dwukierunkowej.
- **Bluetooth** – technologia bezprzewodowej komunikacji krótkiego zasięgu między różnymi urządzeniami elektronicznymi, opisana w specyfikacji IEEE 802.15.1, i nadal rozwijana. Specyfikacja techniczna Bluetooth obejmuje trzy klasy mocy nadawczej o zasięgu 100, 10 oraz 1 metra w otwartej przestrzeni. Do zróżnicowanych zastosowań IoT: medycznych, związanych z bezpieczeństwem, zdalnego odczytu liczników czy określania położenia, opracowano technologię Bluetooth LE (ang. *Low Energy*), w której znacząco obniżono pobór mocy oraz szybkość transmisji danych zwiększając jednocześnie zasięg do nawet 1000 m w otwartej przestrzeni.
- **ZigBee** – technologia cechująca się małą przepustowością i małym zużyciem energii w specyfikacji IEEE 802.15.4, opracowana głównie z myślą o sieciach sensorowych WSN (także w tzw. inteligentnych budynkach czy przemysłowych systemach kontrolnych) jako prostsza w zastosowaniu i tańsza alternatywa dla Bluetooth.
- **NB-IoT** (ang. *NarrowBand-Internet of Things*) – jest standardem technologii LPWAN (ang. *Low-Power Wide-Area Network*) umożliwiającym działanie szerokiej gamie usług, w szczególności dotyczących komunikacji między urządzeniami (M2M). NB-IoT znacząco ogranicza zużycie energii przez urządzenia użytkownika, zwiększa pojemność systemu i efektywność wykorzystania widma, szczególnie w przypadku pokrycia wewnętrznego (m.in. wnętrza budynków). Ma zastosowanie w tzw. inteligentnych miastach, domach, licznikach, detektorach zdarzeń czy w monitoringu przemysłowym.
- **LoRa** (*ang. Long Range)* – jest standardem technologii LPWAN przeznaczonym do zastosowań między urządzeniami IoT, a w szczególności M2M. LoRa ma zastosowanie w tzw. inteligentnych miastach, np. poprzez zdalny odczyt lub komunikację między daleko rozmieszczonymi czujnikami. Protokół ten dostosowuje moc nadajnika i szybkość transmisji do aktualnych warunków propagacyjnych sygnału radiowego. Z tego też względu LoRa nie jest odpowiednia dla usług czasu rzeczywistego, a jedynie dla tych aplikacji, w których można tolerować opóźnienia przesyłanych informacji.

Tabela. Parametry technologii, protokołów i standardów komunikacji bezprzewodowej stosowanych w IoT
Table. Parameters of wireless communication technologies, protocols and standards used in IoT

Technologia komunikacji bezprzewodowej	Wykorzystywane pasma częstotliwości	Przepustowość danych	Maksymalny zasięg	Maksymalna emitowana moc z anteny nadajnika (EIRP/ERP)*
WiFi 2G	(2400 – 2483,5) MHz	do 600 Mbps	do 70 m wewnątrz budynków do 1000 m w otwartej przestrzeni	100 mW ETSI EN 300-328 v2.1.1 (2016-11)
WiFi 5G	(5150 – 5350) MHz (5470 – 5725) MHz	do 3,5 Gbps		200 mW ETSI EN 301 893 V2.0.7 (2016-11)
WiFi HaLow	(863 – 868) MHz	do 347 Mbps	do 1000 m	do 10 mW
RFID LF	(120-140) kHz	do 5 kbps	do kilku cm	standaryzacja dotycząca poziomu pola elektromagnetycznego
RFID HF	typowo 13.56 MHz	do 424 kbps	do 1 m	standaryzacja dotycząca poziomu pola elektromagnetycznego
RFID UHF	(860 – 960) MHz 433 MHz	do 640 kbps do 250 kbps	do 32 m do 800 m	4000 mW, 2000 mW ETSI EN 302 208 V3.1.0 (2016-02)
RFIF SHF	(2400 – 2483,5) MHz	do 1-2 Mbps	do 100 m	4000 mW
NFC	13,56 MHz	do 424 kbps	do 20 cm	standaryzacja dotycząca poziomu pola elektromagnetycznego
GSM	(880 – 915) MHz (925 – 960) MHz (1710 – 1785) MHz (1805 – 1880) MHz	do 9,6 kbps	zasięg całej sieci	2000 mW ETSI TR 103 182 V1.1.1 (2016-09)
GPRS		do 115 kbps		
UMTS	(1885 – 2025) MHz (2110 – 2200) MHz	do 2 Mbps	zasięg całej sieci	2000 mW, 500 mW, 200 mW, 125 mW ETSI TS 125 101 V11.14.0 (2018- 04)
HSPA+		do 42 Mbps		
LTE	(791 – 821) MHz (832 – 862) MHz (1710 – 1785) MHz (1805 – 1880) MHz (1920 – 1980) MHz (2110 – 2170) MHz (2500 – 2690) MHz	do 300 Mbps	zasięg całej sieci	1250 mW, 400 mW, 200 mW ETSI TS 136 101 V15.9.0 (2020-02)
LTE-M		do 1 Mbps		200 mW, 100 mW ETSI TS 136 101 V15.9.0 (2020-02)
Bluetooth	(2400 – 2480) MHz	do 50 Mbps (do 2 Mbps – urządzenia nasobne)	do 100 m	100 mW, 2,5 mW, 1 mW ETSI EN 300 328 V2.2.2 (2019-07)
Bluetooth LE		do 2 Mbps	do 400 m wewnątrz budynków do 1000 m w otwartej przestrzeni	
ZigBee	(2400 – 2480) MHz dodatkowo w Europie 868 MHz	do 250 kbps do 100 kbps	do 100 m wewnątrz budynków do 300 m w otwartej przestrzeni	100 mW ETSI EN 300 328 V2.2.2 (2019-07)
NB-IoT	pasmo LTE,ograniczone do pojedynczego pasma o szerokości 200 kHz	do 235 kbps	do 15 km w obszarze niezurbanizowanym głębokie pokrycie wewnątrz budynków	200 mW, 100 mW, 25 mW ETSI TS 136 101 V15.9.0 (2020-02)
LoRa	433 MHz, 868 MHz	do 50 kbps	do 5 km w obszarze miejskim do 15 km w obszarze podmiejskim do 45 km w obszarze niezurbanizowanym	500 mW, 25 mW, 5 mW ETSI TR 103 526 V1.1.1 (2018-04)
Z-Wave	868 MHz	200 kbps	do 100 m	–

* EIRP (Equivalent Isotropically Radiated Power) – równoważna, ekwiwalentna moc wypromieniowana izotropowo; ERP (Effective Radiated Power) – efektywna wypromieniowana moc; EIRP [W] = 1,64*ERP [W]

- **Z-Wave** – protokół służący do połączenia różnych klas obiektów w jedną, zdalnie sterowaną sieć bezprzewodową, wykorzystywany w systemach inteligentnego zarządzania budynkiem (np. sterowanie ogrzewaniem, oświetleniem, oknami, roletami, żaluzjami, bramą, sprzętem RTV i AGD, systemy alarmowe, powiadamianie pożarowe czy monitoring video).
- **Systemy publicznej łączności komórkowej** – głównie standardy dostępu do Internetu, między innymi GSM (ang. *Global System for Mobile Communications*), GPRS (ang. General Pocket Radio Services), UMTS (ang. *Universal Mobile Telecommunication System*), HSPA+ (ang. *High Speed Packet Access*), LTE (ang. *Long Term Evolution*) czy LTE-M, przeznaczony szczególnie dla aplikacji z zakresu IoT (w tym M2M).

Wielkości charakteryzujące pole elektromagnetyczne od urządzeń IoT

Pole elektromagnetyczne związane z użytkowaniem urządzeń IoT, występuje w środowisku pracy, jak i środowisku ogólnym, ze względu na wykorzystywanie przez te urządzenia łączności bezprzewodowej. Wielkościami stosowanymi do jego scharakteryzowania są: natężenie pola elektrycznego, E – wyrażane w woltach na metr (V/m); natężenie pola magnetycznego, H – wyrażane w amperach na metr (A/m).

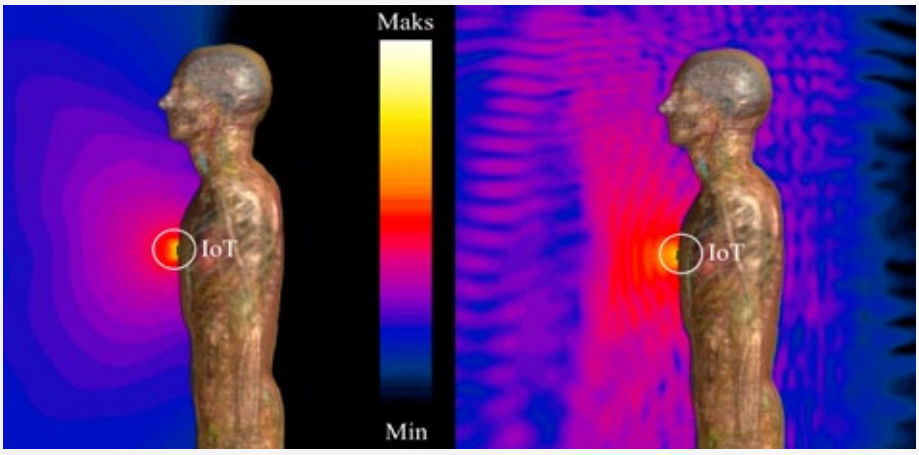
Nasobne urządzenia IoT wykorzystują obecnie technologie łączności bezprzewodowej pracujące w paśmie częstotliwości (0,01-5,7) GHz. Bezpośrednie oddziaływanie pola elektromagnetycznego o takich częstotliwościach powoduje oddziaływanie termiczne wynikające z pochłaniania w organizmie energii, które może skutkować ogrzaniem tkanek. Miarą takiego oddziaływania jest szybkość pochłaniania właściwego energii, tzw. SAR, wyrażany w watach na kilogram (W/kg).

Ocena narażenia na pole elektromagnetyczne

Do oceny takich zagrożeń prawo pracy określa Graniczne Poziomy Oddziaływania (GPO), rozumiane jako miary zagrożeń elektromagnetycznych, związane ze skutkami oddziaływania bezpośredniego pola elektromagnetycznego na ludzi (tj. w omawianym przypadku oddziaływania termicznego pola o częstotliwości z pasma (0,01-5,7) GHz w organizmie człowieka) następująco [9]:

- SARcc (wartość SAR uśredniana względem całego ciała pracownika) – 0,4 W/kg
- SARgt (miejscowa wartość SAR w głowie i tułowiu, uśredniona w 10 g tkanki) – 10 W/kg
- SARk (miejscowa wartość SAR w kończynach uśredniona w 10 g tkanki) – 20 W/kg.

W zaleceniach międzynarodowych określono 5-krotnie niższe limity SAR do oceny ekspozycji ludności.



Rys. 1. Natężenie pola elektrycznego, emitowanego przez nasobne urządzenie IoT zlokalizowane na klatce piersiowej, pracujące w technologii WiFi (wyniki symulacji komputerowych rozkładu przestrzennego pola elektrycznego uzyskane przy częstotliwości emitowanego promieniowania elektromagnetycznego: z lewej – 2,4 GHz; z prawej – 5,5 GHz), (skala logarytmiczna)

Fig. 1. The electric field strength emitted by the IoT device located on the chest, working in the WiFi technology (results of computer simulations of the spatial distribution of the electric field obtained at the frequency of the emitted electromagnetic radiation: on the left – 2.4 GHz; on the right – 5.5 GHz), (logarithmic scale)

Uzupełnieniem są zależne od częstotliwości Interwencyjne Poziomy Narażenia (IPN), rozumiane jako miary narażenia w miejscu pracy na pole elektromagnetyczne (wyrażone jako: natężenie pola elektrycznego i natężenie pola magnetycznego), określające poziomy operacyjne, umożliwiające uproszczoną ocenę, czy narażenie spełnia wymagania określone przez limity GPO, lub konieczne jest stosowanie odpowiednich środków ochronnych [10].

Metody oceny zagrożeń elektromagnetycznych pochodzących od IoT

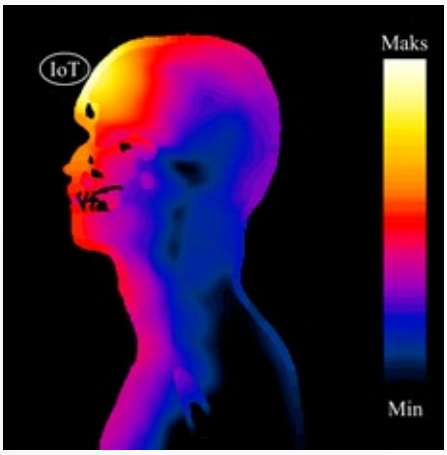
Parametry pola elektromagnetycznego oddziałującego na pracownika ocenia się na podstawie obliczeń (rys. 1.) lub pomiarów natężenia pola elektrycznego i magnetycznego w miejscu przebywania człowieka. Pomiary te powinny być wykonane zgodnie z zasadami określonymi w rozporządzeniu MRPiPS [8]. Wykonuje się je w minimalnej odległości co najmniej 10 cm od źródła pola elektromagnetycznego. Z tego względu ocena zagrożeń elektromagnetycznych przy nasobnych urządzeniach IoT, znajdujących się bezpośrednio przy ciele użytkownika, wymaga przeprowadzenia oceny SAR. Działanie to zaleca się wtedy, gdy człowiek przebywa w odległości mniejszej niż 20 cm od źródła pola elektromagnetycznego.

Wartości SAR oceniane są najczęściej na drodze symulacji numerycznych z zastosowaniem wysokorozdzielczych, antropomorficznych modeli ciała człowieka i źródła pola elektromagnetycznego (rys. 2.). Ocena wyników symulacji numerycznych na potrzeby oceny ich zgodności z limitami wiąże się z koniecznością uwzględnienia licznych wymagań dotyczących cech antropometrycznych oraz rozdzielczości przestrzennej modelu pracownika, jego pozycji ciała czy parametrów dielektrycznych tkanek [11].

Zagrożenia elektromagnetyczne pochodzące od urządzeń IoT

Badania prowadzone przez wiodące ośrodki badawcze na świecie wykazały możliwość występowania przy urządzeniach IoT (w odległości mniejszej od 50 cm) pola elektrycznego o natężeniach, przy których w razie narażenia pracownika konieczne jest stosowanie środków ochronnych określonych przez prawo pracy [5, 9]. Narażenie na pole elektromagnetyczne generowane przez nasobne urządzenia IoT ma często charakter lokalny, charakteryzujący się znaczną różnicą maksymalnych wartości miejscowego SAR i SAR uśrednionego w ciele.

Zgodnie z dyrektywą 2013/35/UE taki rodzaj narażenia powinien być oceniany indywidualnie dla każdego przypadku. Podejście takie zawarto również w dyrektywie 2014/53/UE (RED): ocena narażenia na pole elektromagnetyczne od urządzeń radiowych powinna obejmować wszystkie przewidywane warunki eksploatacji urządzań. Przykładowe symulacje numeryczne oddziaływania pola elektromagnetycznego emitowanego przez anteny nasobnych urządzeń IoT wskazują na możliwość występowania wartości miejscowego SAR przekraczających limity określone dla ogółu ludności i pracowników [12, 13]. Badania te wskazują na konieczność oceny bezpieczeństwa przy nasobnych urządzeniach IoT – pole elektromagnetyczne emitowane z takiego urządzenia do zapewnienia połączenia z odbiornikiem systemu zarządzającego informacjami jest absorbowane również przez ciało jego użytkownika. Stąd, dobre, a więc bezpieczne urządzenie IoT, to takie, którego działanie charakteryzuje się małymi wartościami SAR w ciele użytkownika. Z tego względu wiodące ośrodki badawcze pracują nad nowymi rozwiązaniami technicznymi (nowe konstrukcje anten, nowe materiały i konstrukcje urządzeń IoT) pozwalającymi na ograniczenie wartości SAR w ciele użytkownika, przy równoczesnej poprawie parametrów łączy radiowych tworzonych z udziałem tego urządzenia [12, 13].



Rys. 2. Współczynnik SAR w modelu głowy, prezentujący wyniki symulacji komputerowych rozkładu przestrzennego skutków biofizycznych pochłaniania promieniowania elektromagnetycznego (2,4 GHz), emitowanego przez nasobne urządzenie IoT zlokalizowane przy głowie (np. na opasce), pracujące w technologii WiFi lub Bluetooth (skala logarytmiczna)

Fig. 2. SAR coefficient in the model of the head, presenting the results of computer simulations of the spatial distribution of the biophysical effects of the absorption of electromagnetic radiation (2.4 GHz), emitted by the IoT device located at the head (e.g. on a headband), working in the WiFi or Bluetooth technology (logarithmic scale)

Ograniczanie elektromagnetycznego oddziaływania urządzeń IoT na użytkowników jest istotne również w kontekście ograniczania zagrożenia związanego z wieloletnim oddziaływaniem na człowieka radiofalowego pola elektromagnetycznego, które Międzynarodowa Agencja Badań nad Rakiem (IARC) zakwalifikowała do grupy 2B, czyli czynników środowiskowych przypuszczalnie rakotwórczych dla ludzi [14-16]. Ponadto przyczynia się również do ograniczania zagrożeń pośrednich, które mogą wystąpić pod wpływem oddziaływania pola radiofalowego, które może spowodować nieobojętne dla bezpieczeństwa i zdrowia dysfunkcje w działaniu aktywnych implantów medycznych (AIMD), zarówno u użytkowników nasobnych IoT, jak i osób znajdujących się w ich pobliżu [17]. Najczęściej użytkowane AIMD to stymulatory i kardiowerter-defibrylatory serca, implanty słuchowe oraz nasobne pompy insulinowe.

Podsumowanie

IoT jest technologią coraz powszechniej wykorzystywaną w wielu gałęziach gospodarki, w pracy, a także w życiu codziennym. Przeprowadzona analiza emisji elektromagnetycznych związanych z zastosowaniem technologii IoT wykazała, że nasobne urządzenia IoT wykorzystują obecnie głównie takie technologie, protokoły i standardy łączności bezprzewodowej, jak: Bluetooth, Wi-Fi, RFID, czy łącza publicznych systemów telefonii komórkowej, korzystające z łączy radiowych za pośrednictwem pola elektromagnetycznego o częstotliwości (0,01-5,7) GHz.

Ocena zagrożeń elektromagnetycznych związanych z użytkowaniem nasobnych urządzeń działających w technologii IoT na podstawie pomiarów rozkładów natężenia pola elektrycznego i magnetycznego w ich otoczeniu nie jest miarodajna ze względu na małą odległość źródła pola elektromagnetycznego od ciała człowieka (użytkownika nasobnego urządzenia IoT lub osoby znajdującej się w pobliżu). Prawo pracy wymaga w takim przypadku oceny współczynnika SAR z wykorzystaniem symulacji numerycznych z zastosowaniem wysokorozdzielczych modeli ciała człowieka i możliwie szczegółowych modeli źródła pola elektromagnetycznego [8,9,11].

Takie kompleksowe badania i ocena zagrożeń elektromagnetycznych (z wykorzystaniem symulacji numerycznych i technik pomiarowych) są przedmiotem realizowanych obecnie w Pracowni Zagrożeń Elektromagnetycznych CIOP-PIB badań, których wyniki zostaną zaprezentowane w kolejnych publikacjach.

BIBLIOGRAFIA

[1] Raport Grupy Roboczej do Spraw Internetu Rzeczy przy Ministerstwie Cyfryzacji, IoT w Polskiej gospodarce. Ministerstwo Cyfryzacji 2019, www.gov.pl/cyfryzacja

[2] VERMESAN, O., FRIESS, P. Digitising the Industry. Internet of Things Connecting the Physical, Digital and Virtual Worlds, River Publishers: Gistrup, Denmark, 2016.

[3] ISO 19731:2017. Digital analytics and web analyses for purposes of market, opinion and social research – Vocabulary and service requirements.

[4] ILNAS, Internet of Things (IoT) Technology. Economic View and Technical Standardization, ILNAS, Luxemburg, 2018.

[5] AERTS, S., VERLOOCK, L., VAN DEN BOSSCHE, M., VERGARA, X., MARTENS, L., WOUT, J. Characterization of the exposure due to smart-home devices and other esidential RF sources. Abstract Collection. The Joint Annual Meeting of The Bioelectromagnetics Society and the European BioElectromagnetics Association, BioEM June 25-29, Piran, Portoroz, Slovenia 2018.

[6] CHOPRA, N., ADDISON, D., CALDERON, C., MASLANYJ, M., PEYMAN, A. Exposure to electromagnetic fields from smart meter technologies in Great Britain (Phase 3): On-site measurements in homes. Abstract Collection. The Joint Annual Meeting of The Bioelectromagnetics Society and the European BioElectromagnetics Association, BioEM, June 25-29, Piran, Portoroz, Slovenia 2018.

[7] SIKDER, A.U., PETRACCA, G., AKSU, H., JAEGER, T., ULUAGAC, A.S. A Survey on Sensor-based Threats to Internet-of-Things (IoT) Devices and Applications. Published on arXiv.org, Cornell University Library, 2018.

[8] ZRADZIŃSKI, P., KARPOWICZ, J., GRYZ, K., SUAREZ, O.J., TRILLO, A.M., HERNANDEZ, J.A., DE MIGUEL-BILBAO, S., SUAREZ, S.D., CELAYA-ECHARRI, M., AZPILICUETA, L., FALCONE, F., RAMOS, V. Environmental safety aspects of using UHF RFID systems in hospitals. Inżynier i Fizyk Medyczny 2020,9,2: 133-140.

[9] Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 29 czerwca 2016 r. w sprawie bezpieczeństwa i higieny pracy przy pracach związanych z narażeniem na pola elektromagnetyczne. Tekst jednolity (t.j.) Dz.U. 2018, poz. 331.

[10] Rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 12 czerwca 2018 r. w sprawie najwyższych dopuszczalnych stężeń i natężeń czynników szkodliwych dla zdrowia w środowisku pracy. Załącznik 2. Część E „Pole elektromagnetyczne". Dz.U. 2018, poz.1286.

[11] ZRADZIŃSKI, P. Uwarunkowania wykorzystania numerycznych modeli pracowników do oceny zagrożeń bezpośrednich wynikających z narażenia na pole elektromagnetyczne. Podstawy i Metody Oceny Środowiska Pracy, 2016, 90,4: 75-89.

[12] ASHYAP, A.Y.I., ABIDIN, Z.Z., DAHLAN, S.H., MAJID, H.A., KAMARUDIN, M.R., ALOMAINY, A., ABD-ALHAMEED, R.A., KOSHA, J., NORAS, J.M. Highly efficient wearable CPW antenna enabled by EBG-FSS structure for medical body area network applications. IEEE Access, 2018,6: 77529-77541.

[13] ALI, U., ULLAH, S., KHAN, J.F., SHAFI, M., KAMAL, B., BASIR, A., FLINT, J.A., SEAGER, R.D. Design and SAR Analysis of Wearable Antenna on Various Parts of Human Body, Using Conventional and Artificial Ground Planes. Journal of Electrical Engineering and Technology 2016,12,1: 317-328.

[14] International Agency for Research on Cancer (IARC). „Non-ionizing radiation, part 2: Radiofrequency electromagnetic fields". The WHO/IARC, IARC Monographs Volume 102, Lyon, France 2013.

[15] BELAYEV, I. Health Effects of Chronic Exposure to Radiation From Mobile Communication [w:] Mobile Communication and Public Health, ed. M. Markov, CRC Press Taylor & Francis, 2019.

[16] BORTKIEWICZ, A. Skutki zdrowotne działania pól elektromagnetycznych – przegląd badań. Podstawy i Metody Oceny Środowiska Pracy 2008, 4,58: 67-87.

[17] ZRADZIŃSKI, P., KARPOWICZ, J., GRYZ, K., LESZKO, W. Evaluation of the safety of users of active implantable medical devices (AIMD) in the working environment in terms of exposure to electromagnetic fields – Practical approach to the requirements of European Directive 2013/35/EU. International Journal of Occupational Medicine and Environmental Health 2018, 31,6: 795-808.

Publikacja opracowana na podstawie wyników V etapu programu wieloletniego „Poprawa bezpieczeństwa i warunków pracy", finansowanego w latach 2020-2022 w zakresie badań naukowych i prac rozwojowych ze środków Narodowego Centrum Badań i Rozwoju. Koordynator programu: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy (II.PB.15)