

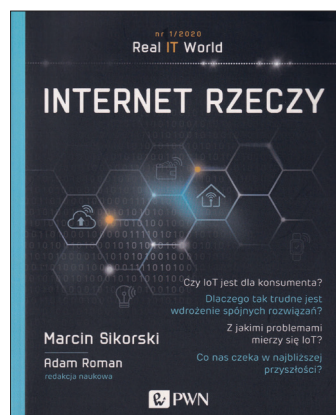
Karol Popiołek
(Poznań-Gniezno)
<https://orcid.org/0000-0001-6674-9899>

INTERNET RZECZY – ROZWÓJ, PROBLEMY I PRZYSZŁOŚĆ

Marcin Sikorski, Internet rzeczy, Wydawnictwo Naukowe PWN, Warszawa 2020, ss. 104.

Internet rzeczy (ang. *Internet of Things*, IoT) to sieć połączonych urządzeń, które mogą wymieniać i analizować dane za pomocą Internetu, w tym także bez ingerencji człowieka. Pozwala to na automatyzację i sprawniejsze wykonywanie różnych zadań przez te urządzenia: od sprzętów domowych (pralki, lodówki), przez elektronikę użytkową (zabawki, głośniki), po zaawansowane zastosowania przemysłowe (inteligentne fabryki, różnego typu czujniki).

Omawiająca ten obszar recenzowana książka składa się z czterech rozdziałów. Pierwszy jest wprowadzeniem w zagadnienie Internetu rzeczy oraz wyjaśnia fenomen popularności tej technologii pomimo często niewielkiej wiedzy użytkowników na ten temat. Rozdział drugi omawia aspekty regulacyjne i prawne dotyczące IoT. Wskazuje problemy w tym zakresie, takie jak niespójne w wielu krajach przepisy. Rozdział trzeci dotyczy szeroko pojętego bezpieczeństwa. Autor porusza najważniejsze problemy w tym obszarze oraz zwraca uwagę na kwestię przetwarzania danych. Ostatni rozdział dotyczy przyszłości urządzeń IoT. Autor przedstawia w nim swoje prognozy co do rozwoju Internetu rzeczy.



Autor stawia pytania badawcze dotyczące rozwoju IoT, zaufania do technologii, regulującego ją prawa, bezpieczeństwa użytkowników oraz przyszłości tego typu urządzeń. Publikacja ma za zadanie zwrócić uwagę na tę tematykę, oferując perspektywę ekspercką. Konstrukcja książki jest uporządkowana i logiczna.

Omawiając jakieś zagadnienie, autor zwykle jednak porzeka na jednym przykładzie. Na przykład prezentując urządzenie działające wadliwie, autor wymienia tylko jeden konkretny typ sprzętu (interaktywna lalka obciążona wadami technicznymi oraz prawnymi, s. 47-48). Podobnie omówienie urządzeń sprawiających użytkownikom trudności w zrozumieniu zasad ich działania przywołuje tylko jeden przykład (żarówka typu *smart*, s. 60). Podane w publikacji przykłady są wybrane i opisane poprawnie, ale brakuje możliwości porównania opisu lub sposobu działania urządzenia A z urządzeniem B.

Autor traktuje język, jakim omawia problematykę pracy, dość swobodnie. W kilku miejscach rejestr zdaje się nadto potoczny („To prawda, że liczby wyrwane z kontekstu robią wrażenie, a morze (no, ewentualnie jezioro) możliwości jest bezsprzecznie argumentem przemawiającym za technologią”, s. 18). Niekiedy ton komentarza jest nadmiernie emocjonalny („Jest to o tyle zabawne, że mniej niż 5% zawodów może być w 100% zautomatyzowane”, s. 51). W innych przypadkach razi brawurowa metaforyka („Nie jest trudno stać się samozwańczym ewangelistą”, s. 57). Te i inne językowe wybory sprawiają, że ogólny ton bliższy jest publicystyce niż pracy naukowej.

Autor celnie podnosi problem nadmiernej produkcji coraz to nowszych wersji tego samego produktu, bez dokonywania realnych zmian w zasadach jego działania. Skutkuje to zalewaniem rynku: „wieloma podobnie wyglądającymi i zachowującymi się urządzeniami, które w oczach klienta stapiają się w nierozróżnialny produkt” (s. 19). Użytkownik ma wówczas problem z porównaniem produktów oraz dokonaniem optymalnego wyboru. Wiąże się to także z tym, że – jak autor słusznie zauważa – cykl życia produktu jest zbyt krótki. Składa się pięciu faz: idea i prototyp, bezpieczna produkcja, udostępnienie i wdrożenie, zarządzanie i monitoring, aktualizacje i monitoring. Czas przeznaczony na poszczególne fazy jest jednak różny. Może to powodować dyskomfort u użytkownika, który miewa poczucie, że jego produkt był wspierany technicznie przez producenta zbyt krótko (s. 36).

Niezbyt trafnie autor zaliczył do nietypowych metod komunikacyjnych standard IEEE 802.11 (podstawa działania Wi-Fi) oraz protokół IP (podstawa łączności przewodowej i bezprzewodowej). Zdecydowanie nie są to technologie używane rzadko czy mało znane. Mechanizm ich działania jest znany od lat, jasny dla wszystkich osób choć trochę interesujących się technologiami informatycznymi – i z powodzeniem używany przez miliardy ludzi każdego dnia. Dynamiczny rozwój Internetu rzeczy faktycznie jednak sprawia, że niektóre opisy technologii mogą

szybciej tracić aktualność. Dotyczy to szczególnie standardów komunikacyjnych oraz platform sprzętowych (s. 20).

Słusznie natomiast publikacja punktuje zbyt dużą ilość informacji gromadzonych i przetwarzanych przez urządzenia IoT. Powoduje to niepotrzebny ruch sieciowy oraz nadmierne przechowywanie danych. Kolejną kwestią jest bezpieczeństwo tak dużej ilości przetwarzanych informacji. Stąd słusznie autor podkreśla kluczowe zagrożenia wynikające z gwałtownego rozwoju IoT bez odpowiedniej infrastruktury (s. 21), poczynszy od sposobów autoryzacji, a skończywszy na protokołach sieciowych¹.

W ciągu ostatnich dwóch lat w sektorze wyraźnie widać zmianę trendu. Internet rzeczy przestał być technologią numerem jeden, aktualnie prym wiodzie sztuczna inteligencja. Obie technologie uzupełniają się jednak w wielu miejscach. Książka trafnie podnosi ten sam problem, który aktualnie porusza się, omawiając zagrożenia ze strony sztucznej inteligencji – utratę miejsc pracy z powodu rozwoju technologii i zastąpienia ludzi bardziej wydajnymi i wyspecjalizowanymi urządzeniami. Tekst wspomina o pięciu procentach zawodów zagrożonych całkowitą automatyzacją (s. 51). Szacunki OECD (Organizacji Współpracy Gospodarczej i Rozwoju, ang. Organisation for Economic Co-operation and Development) z 2024 roku podają, że nawet około dwadzieścia siedem procent zatrudnienia w jej krajach członkowskich przypada na zawody o najwyższym ryzyku automatyzacji². Aktualnie wiele firm wdraża lub planuje wdrożyć rozwiązania z obszaru IoT (s. 17).

W publikacji nakreślono też problemy etyczne dotyczące IoT. Wskazano na wątpliwości wokół ilości przetwarzanych danych, poziomu autonomii urządzeń, potencjalnych konsekwencji przerw w dostawach prądu, a także zagadnienia odpowiedzialności za urządzenia medyczne oraz cyfrowego wykluczenia (s. 27). Choć autor słusznie podniósł te wątki, brakuje szerszego rozwinięcia tej tematyki. Jej omówienie jest dość pobieżne i nie daje jasnej odpowiedzi, jakie potencjalne rozwiązania autor widzi.

Zastrzeżeń nie budzi natomiast omówienie kwestii wpływu systemów operacyjnych, platform, serwerów oraz usług zewnętrznych na działanie urządzeń IoT (s. 35). Tekst trafnie kataloguje i opisuje kluczowe typy zdarzeń w tym zakresie (takie jak aktualizacja systemu operacyjnego lub zmiana polityki prywatności firmy zewnętrznej).

Autor przedstawia też swoje stanowisko na temat koncepcji scalenia funkcjonowania całych miast poprzez zintegrowane urządzenia IoT. Odnosi się do takich pomysłów sceptycznie i nie wróży im sukcesu. Argumentuje, że mieszanek różnych projektów, wdrażanych równocześnie, ma minimalne szanse powodzenia (s. 44).

¹ Ciemcioch 2023, s. 74.

² OECD 2024.

Tekst wprowadza czytelnika w szczegóły dotyczące zagrożenia prywatności przez urządzenia IoT. Producenci teoretycznie zobowiązani są zapewnić odpowiednio wysokie standardy bezpieczeństwa i prywatności (s. 76). Wspomniany już przykład interaktywnej lalki pokazuje jednak, jak to niekiedy wygląda w praktyce, oraz służy autorowi do przyjrzenia się prawnym próbom regulowania urządzeń IoT. Rzeczona lalka w trakcie zabawy zadawała pytania m.in. o imiona rodziców, miejsce zamieszkania i szkołę, a pozyskane informacje przetwarzała w formie niezakodowanych wiadomości, przy wadliwie skonstruowanej polityce prywatności. Autor przeanalizował szczegóły postępowania prawnych mających na celu wycofanie z kilku rynków tego produktu (s. 47-48) i zwrócił przy tym uwagę na problem ochrony nieletnich. To oni są faktycznymi użytkownikami zabawek, mimo że nie są przecież w stanie w pełni rozumieć zagrożeń związanych z ochroną prywatności ani świadomie przeciwdziałać wyciekom danych osobowych (s. 48).

Jak zatem będzie wyglądała przyszłość Internetu rzeczy w przyszłości? Autor zakłada dalszy stały rozwój rynku IoT, ale także rozwój świadomości konsumentów. Wymusi to dostosowanie produkowanych rzeczy do realnych potrzeb rynkowych (s. 88). Przewiduje też zajęcie pozycji lidera IoT przez Chiny. Tak sugerują i możliwości tego państwa, i jego plany oraz konsekwencja w ich realizacji (m.in. poprzez finansowanie oraz patentowanie kolejnych rozwiązań technicznych, s. 93).

Recenzowana publikacja wpisuje się w rosnącą potrzebę uporządkowania wiedzy o świecie, w którym usługi, urządzenia i informacje wiążą się ze sobą coraz bardziej, kreując nowe przestrzenie technologiczne i społeczne. Książka Marcina Sikorskiego stanowi solidne, przystępne wprowadzenie do tematyki Internetu rzeczy, nakierowane wprawdzie na odbiorcę mającego już jakąś wiedzę technologiczną, ale napisane tak, by nie odstraszać mniej zaawansowanego czytelnika. Jej największym atutem jest klarowność i porządek merytoryczny, a głównym ograniczeniem – poziom ogólności, zbyt duży dla osób o wyższych kwalifikacjach technicznych (brak szczegółowych opisów architektury systemów, protokołów czy rozbudowanych badań szczegółowych).

Podsumowując, książka jest dobrze ustrukturyzowana oraz odpowiada na postawione pytania badawcze. Pomimo drobnych mankamentów jest ważnym wkładem w literaturę dotyczącą Internetu rzeczy. To naprawdę solidne wprowadzenie, choć zapewne zbyt ogólne dla ekspertów.

Bibliografia

- Ciemcioch K. 2023, Internet rzeczy – zastosowanie, zagrożenia, bezpieczeństwo, *Zbliżenia Cywilizacyjne* XIX (3), s. 61-85.
- Dhar S., Khare A., Dwivedi A. 2024, Securing IoT devices: A novel approach using blockchain and quantum cryptography, *Internet of Things* 25, 101019, s. 1-16.

Kaur R. 2024, Internet of Things: An Overview, International Journal for Multidisciplinary Research 6, 2, s. 1-6.

OECD 2024, OECD Artificial Intelligence Papers, 26, October [online]. OECD [dostęp: 2025-11-13]. Dostępny w Internecie: <https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/10/who-will-be-the-workers-most-affected-by-ai_fb7fcccd/14dc6f89-en.pdf>.