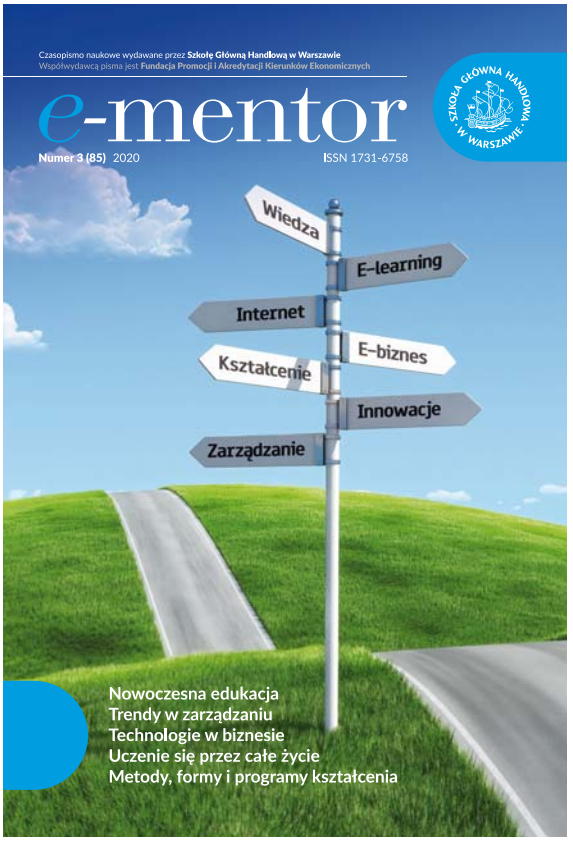
e-mentor
DWUMIESIĘCZNIK SZKOŁY GŁÓWNEJ HANDLOWEJ W WARSZAWIE
WSPÓŁWYDAWCA: FUNDACJA PROMOCJI I AKREDYTACJ KIERUNKÓW EKONOMICZNYCH



2020, nr 3 (85)

Liwarska-Fulczyk, K. (2020). Internet rzeczy – implikacje organizacyjne. *e-mentor, 3*(85), 23–31. https://doi.org/10.15219/em85.1470

Katarzyna Liwarska-Fulczyk

Internet rzeczy – implikacje organizacyjne

The Internet of Things – organizational implications

Abstract

The Internet of Things, which is another ICT solution and a consequence of the development of the global computer network, is one of the key technologies that has been leveraging organizations' capabilities to drive new business growth. It constitutes a priority for business innovation in the broader sense. Beyond the range of benefits and new opportunities for contemporary organizations, it creates some consequences, new conditions as well as challenges. The article aims to identify significant organizational implications related to the implementation of the concept of the Internet of Things. In this context, based on a literature review and the analysis of the existing research, an author analyzes the barriers and constraints resulting from its adaptation. The analysis shows that data protection and privacy issues, interoperability, real-time data analysis, the lack of standardization, and high financial investments are emerging as major barriers to deploying this technology. Legal and technical issues, the competence gap, and the lack of operational readiness and ability of the organization to change may equally substantially hinder the development of the phenomenon of the Internet of Things in organizations. On the scale of the whole organization, adapting the development to this new concept requires verification of existing business models and modification of operational models taking into account activities related to the potential occurrence of several risks.

Keywords: Internet of Things, new technologies, technology adoption, technology management, organizational implications of IoT

Wprowadzenie

Technologie informacyjne (ang. ICT), cyfryzacja otaczającego świata oraz pozyskiwanie i analiza ogromnej liczby danych płynących z otoczenia są obecnie nośnikami głębokich przemian społecznych i gospodarczych. Ciągła konwergencja rzeczywistego i wirtualnego świata sprawia, że technologie cyfrowe coraz bardziej przenikają do gospodarki, stanowiąc jej spiritus movens. Wynikiem przeobrażeń wywołanych ogromnym tempem postępu technologicznego i przyspieszającą cyfryzacją otoczenia jest transformacja cyfrowa, która w znacznym stopniu determinuje funkcjonowanie i rozwój współczesnych organizacji i wymaga od nich błyskawicznej adaptacji. W rezultacie przedsiębiorstwa muszą nieprzerwanie rewidować i dostosowywać swoje modele biznesowe oraz operacyjne. Fundamentem i siłą wiodącą transformacji cyfrowej jest internet rzeczy (ang. ***Internet of Things***, ***IoT***), który, jak wynika z badań przeprowadzonych przez firmę konsultingową KPMG (2019), jest obok robotyzacji i blockchain kluczową technologią napędzającą proces transformacyjny współczesnych organizacji. PwC (2019) na podstawie wyników badań również wskazuje na IoT jako główny nurt cyfrowych transformacji przedsiębiorstw, które są rdzeniem czwartej rewolucji przemysłowej. Nie dziwi więc fakt, że firmy wydają coraz więcej na tę technologię. Zebra Technologies (2019) w raporcie będącym rezultatem badań przeprowadzonych wśród decydentów w zakresie inwestycji technologicznych wskazuje, że zdecydowana większość ankietowanych – 86%, zamierza zwiększyć nakłady finansowe swoich przedsiębiorstw na internet rzeczy w ciągu najbliższych lat. Co więcej, organizacje zwiększyły inwestycje w internet rzeczy o 4% w 2018 r. w stosunku do 2017 r., wydając średnio 4,6 mln dolarów (Zebra Technologies, 2019).

Katarzyna Liwarska-Fulczyk, Uniwersytet Ekonomiczny we Wrocławiu, https://orcid.org/0000-0001-8148-5043

Dzieje się tak dlatego, że organizacje dostrzegają szerokie spektrum możliwości i korzyści płynących z implementacji IoT. Przede wszystkim internet rzeczy wnosi ogromny potencjał innowacyjny (Nicolescu i in., 2018), pozwala na tworzenie nowych sposobów zdobywania przewagi konkurencyjnej (Suppatvech i in., 2019) i stwarza nowe szanse rozwoju biznesu. Ovidiu Vermesan i Peter Fries (2014) zwracają uwagę, iż jego wykorzystywanie może spowodować nie tylko wzrost efektywności działań przedsiębiorstwa czy poprawę działań operacyjnych, lecz także powstawanie zupełnie nowych modeli biznesowych lub modyfikowanie istniejących. Nowe modele biznesowe są naturalną konsekwencją nieprawdopodobnej liczby danych generowanych i przetwarzanych w czasie rzeczywistym przez internet rzeczy (Vermesan i Fries, 2014). Innymi słowy jego strategiczny wymiar korzyści stanowią dane i ich analiza. Na podstawie gromadzonych, przesyłanych i przetwarzanych danych organizacje otrzymują pożyteczne informacje we właściwym czasie i w związku z tym mogą szybko i sprawnie przeprojektowywać procesy, podejmować trafne decyzje oraz weryfikować istniejące modele biznesowe czy tworzyć nowe. Z kolei Michael Porter i James Heppelmann (2014) przedstawiają cztery podstawowe obszary korzyści wynikające z wykorzystania przez organizacje połączonych inteligentnych produktów:

- monitorowanie – możliwości samodzielnej obserwacji i kontroli stanu przedmiotu, zbieranie informacji i danych o otoczeniu i swoim działaniu;
- kontrola – inteligentne przedmioty uczą się swoich użytkowników oraz kontrolują swoje funkcje;
- optymalizacja – zwiększenie wydajności produktu, wczesna diagnostyka, obsługa i naprawa;
- autonomia (niezależność) – inteligentny przedmiot może samodzielnie zwiększać swoją wydajność i efektywność.

Na szczególne możliwości, jakie stwarza internet rzeczy w sektorze prywatnym, zwracają uwagę Leszek Kiełtyka i Ola Zygoń (2018) podkreślając, że implementacja nowej technologii może umożliwić organizacjom gospodarczym zwiększenie produktywności pracowników, lepszą alokację kapitału, redukcję kosztów a także poprawę relacji z klientami. Dodatkowo dzięki internetowi rzeczy przedsiębiorstwa mogą lepiej zrozumieć wymagania klientów oraz szybciej wprowadzać zmiany w łańcuchu dostaw (Rot, 2017).

Jednak internet rzeczy to też źródło implikacji i wyzwań, które zarządzający powinni wziąć pod uwagę, decydując się na jego adaptację. Jest to o tyle istotne, że w badaniu Microsoft (2019) 25% ankietowanych przyznało, że implementacja internetu rzeczy w ich firmach zakończyła się niepowodzeniem ze względu na brak jasnej strategii jego wdrożenia.

Wobec powyższego celem tego opracowania jest identyfikacja kluczowych implikacji organizacyjnych związanych z zastosowaniem koncepcji internetu rzeczy w organizacjach.

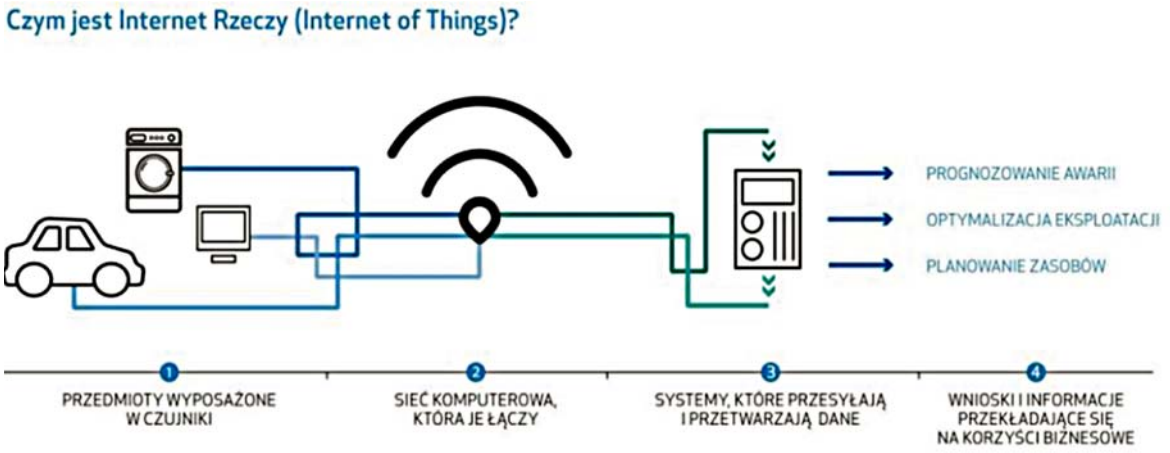
W pierwszej części artykułu zaprezentowano ujęcie definicyjne internetu rzeczy oraz dane liczbowe celem zobrazowania skali występowania tej technologii. W dalszej części opracowania przedstawiono czynniki stanowiące bariery i ograniczenia w rozwoju internetu rzeczy w organizacjach wraz z wyzwaniami stojącymi przed tą koncepcją. Zastosowana metoda badawcza to przegląd aktualnej literatury przedmiotu oraz analiza istniejących badań. W końcowej części artykułu stworzono obraz implikacji strategicznych i wewnątrzorganizacyjnych wynikających z przeprowadzonej analizy.

Ujęcie definicyjne i dane liczbowe

W świetle rosnącej liczby publikacji i badań na temat koncepcji internetu rzeczy, brak jest jednej spójnej jego definicji i w dalszym ciągu wzbudza wiele sporów interpretacyjnych (Höller i in., 2014). Co więcej, zjawisko to wciąż ewoluuje ze względu na ciągły rozwój technologii (możliwe jest łączenie coraz większej liczby mniejszych i tańszych urządzeń w coraz łatwiejszy sposób).

Pojęcie internetu rzeczy (przedmiotów) użyte przez Kevina Ashtona w 1999 roku odnosiło się do systemu komunikowania się urządzeń (świata materialnego) z komputerami przy wykorzystaniu czujników w standardzie RFID (Ashton, 2009). W tym miejscu należałoby jednak przywołać Andrego Whitmore'a i in. (2015), którzy podkreślają, iż system komunikowania się urządzeń (M2M, machine-machine) nie jest niczym nowym. Ze względu na swoją specyfikę internet umożliwia komunikację nie tylko między ludźmi, ale i serwerami oraz ruterami. Zatem internet rzeczy stanowi kolejny etap ewolucji internetu, gdzie nowe rodzaje urządzeń łączą się wzajemnie poprzez globalną sieć (Whitmore i in., 2015). Według Portera i Heppelmanna (2015) internet rzeczy powstał wskutek rosnącej liczby inteligentnych, połączonych ze sobą produktów oraz ich możliwości. Charakteryzując IoT, badacze odnoszą się do sfery technologicznej, podkreślając, że są to inteligentne produkty, które mają dostęp do internetu i składają się z elementów: fizycznych, inteligentnych (czujniki, procesory, nośniki danych, mechanizmy sterujące, oprogramowanie) oraz umożliwiających łączność (porty, anteny, protokoły do transmisji danych w formie bezprzewodowej i przewodowej). Z kolei Richard Dobbs i in. (2015) definiują internet rzeczy jako sensory i urządzenia umieszczone w maszynach i innych obiektach fizycznych, zastosowane celem gromadzenia danych, zdalnego monitorowania, podejmowania decyzji oraz prowadzenia procesów optymalizacji we wszystkich obszarach począwszy od produkcji, poprzez infrastrukturę a skończywszy na opiece medycznej. Według McKinsey Global Institute (2015) IoT sprowadza się do czujników i systemów komunikacyjnych, które są wbudowane w rozmaite obiekty i urządzenia, umożliwiając tym samym koordynację działań tychże w ramach sieci online. Z kolei IDC (2020a) podkreśla, że internet rzeczy stanowi

Rysunek 1. Idea funkcjonowania rozwiązań internetu rzeczy



Źródło: *Kluczowe zagadnienia związane z Internetem Rzeczy*, SAS (b.d.). (Pobrano 29 maja 2020 z https://www.sas.com/pl_pl/insights/internet-of-things.html).

złożony ekosystem technologii obejmujący moduły i urządzenia, środki łączności, platformy konstruowane specjalnie pod jego kątem, pamięci masowe, serwery, oprogramowanie analityczne, usługi IT oraz zabezpieczenia. Ideę funkcjonowania rozwiązań internetu rzeczy przedstawiono na rysunku 1.

W dzisiejszej dobie dostęp do globalnej sieci przestał być domeną wyłącznie ludzi. W zależności od źródła prognoz, do 2025 roku do internetu ma być podłączonych od ponad 40 mld (Newman, 2020) do 75 mld (Horwitz, 2019) rozmaitych urządzeń i czujników. Zatem urządzeń, które pracują w trybie online, jest więcej niż ludzi na kuli ziemskiej, a zważywszy na tempo i dynamikę rozwoju technologii, różnica ta z dnia na dzień znacząco będzie się pogłębiać. Odnosząc się do wartości rynkowej, jak prognozuje Alexandre Ménard (2017), potencjalny wskaźnik wzrostu ekonomicznego dla internetu rzeczy wyniesie od 3,9 do 11,1 tryliona USD do końca 2025 roku. Z kolei firma badawcza IDC (2020b) prognozuje, że w 2020 roku globalny rynek internetu rzeczy na świecie osiągnie wartość 7,4 tryliona USD. Warto podkreślić, iż bierze ona pod uwagę wartość całego ekosystemu przedstawianej technologii – nie tylko urządzeń końcowych, sensorów czy liczników, ale również oprogramowania, usług IT i telekomunikacyjnych czy też infrastruktury IT. Dodatkowo IDC (2020b) szacuje, że w czteroletnim okresie prognozy (2020–2024) wydatki na oprogramowanie dla internetu rzeczy będą charakteryzowały się najszybszym wzrostem, CAGR (skumulowany roczny wskaźnik wzrostu) osiągnie poziom 13,5%. Z kolei wydatki na usługi w obszarze internetu rzeczy będą rosły szybciej niż ogólne wydatki na internet rzeczy, których wskaźnik CAGR wyniesie 12,6%. Branże, które w czteroletnim okresie prognozy odnotują największe stopy wzrostu CAGR to opieka zdrowotna – 14,5% oraz smart home (inteligentny dom) – 14,4%.

Kluczowe bariery, zagrożenia i wyzwania dla rozwoju internetu rzeczy w organizacjach

Poza wspomnianymi na wstępie tego artykułu możliwościami i korzyściami, jakie stwarzają innowacje technologiczne, takie jak internet rzeczy, istnieje szereg ograniczeń, ryzyk i wyzwań z nim związanych. Na podstawie literatury przedmiotu wyodrębniono siedem głównych czynników hamujących rozwój internetu rzeczy w organizacjach: bezpieczeństwo, ochrona danych i prywatność, interoperacyjność, standaryzacja i integracja, skalowalność, regulacje prawne oraz luka kompetencyjna. Barierami o mniejszym znaczeniu, ale mogącymi również w istotny sposób utrudnić zastosowanie tej technologii są kwestie związane z wysokimi nakładami finansowymi, własnością gromadzonych danych (własność intelektualna) oraz przeszkody o charakterze behawioralnym.

Bezpieczeństwo

Złożoność elementów infrastruktury internetu rzeczy sprawia, że zagwarantowanie odpowiedniego poziomu bezpieczeństwa jego systemom jest bardzo trudne. W związku z tym istnieje ogólny konsensus, że obszar bezpieczeństwa stanowi kluczową przeszkodę w implementacji koncepcji internetu rzeczy w organizacjach (Babar i in., 2010; Butun i in., 2019; Conti i in., 2018; Kouicem i in., 2018, Miorandi i in., 2012; Podgórski, 2017; Porter i Heppelmann, 2014; Poudel, 2016; Rot, 2017; Sicari i in., 2015; Whitmore i in., 2015; Zdravković i in., 2018). Badania przeprowadzone przez DZone (2018), KPMG (2019), Microsoft (2019) oraz PwC (2019) również wykazały, że głównym ograniczeniem w rozwoju tej innowacyjnej technologii są obawy dotyczące bezpieczeństwa. Ponadto, jak podkreślają Artur Rot i Bartosz Blaicke (2017), bezpieczeństwo ma kluczowe znaczenie, ponieważ wraz

ze stale rosnącą liczbą połączonych urządzeń, które stanowią nowe punkty nieautoryzowanych dostępów, wzrasta ryzyko cyberataków na urządzenia internetu rzeczy i nieuprawnionego dostępu do danych.

Ochrona danych i prywatność

Obok bezpieczeństwa, ochrona danych i prywatność wyłaniają się jako jedne z najistotniejszych barier rozwojowych dla internetu rzeczy w organizacjach. Przyrost i mnogość urządzeń podłączonych do internetu jest przyczyną rosnącej liczby generowanych i dystrybuowanych przez nie danych. Stąd w coraz większej liczbie publikacji podkreśla się kwestię ryzyka wynikającego z istnienia inteligentnych obiektów gromadzących ogromne zasoby prywatnych danych oraz potrzebę ich skutecznej ochrony (Atzori i in., 2010; Hsu i Lin, 2016; Lee i Lee, 2015; Lopez i in., 2017; Ng i Wakeshaw, 2017; Porter i Heppelmann, 2014; Poudel, 2016; Saarikko i in., 2017; Sicari i in., 2015; Weinberg i in., 2015; Whitmore i in., 2015; Ziegeldorf i in., 2014). W podobnym tonie wypowiadają się eksperci w badaniach przeprowadzonych przez Accenture Digital (2017), Ernst&Young (2015), GrowthEnabler (2017), McKinsey (2015) i PwC (2019), którzy wskazują na obszar ochrony danych i prywatności jako jedne z najważniejszych czynników hamujących rozwój internetu rzeczy w organizacjach. Urządzenia IoT zbierają szczegółowe metadane, które wnikają w życie prywatne użytkowników. Luka w zabezpieczeniach może być wykorzystywana przez hakerów uzyskujących dostęp do prywatnych danych (DZone, 2018). Porter i Heppelmann (2014) zwracają uwagę na konieczność ochrony danych zarówno produktu, jak i użytkownika, co stwarza prawdziwe wyzwania w kontekście zarządzania nimi.

Interoperacyjność, standaryzacja i integracja

Kolejnymi czynnikami, które w istotny sposób ograniczają powodzenie wdrożenia koncepcji internetu rzeczy jest brak interoperacyjności pomiędzy istniejącymi urządzeniami, systemami, platformami IoT (Al-Fuqaha i in., 2015; Butun i in., 2019; Poudel, 2016; Rot i Sobińska, 2018; Suppatvech i in., 2019; Whitmore i in., 2015; Zdravkovicì i in., 2018) oraz brak standaryzacji w jego obszarze (Čolaković i Hadžialić, 2018; Nord i in., 2019; Porter i Heppelmann, 2014; Rot i Sobińska, 2018). Wynika to z heterogenicznego charakteru tej koncepcji (Whitmore i in., 2015). Według Alema Čolakovića i Mesuda Hadžialića (2018) brak kompleksowych ram standaryzacji (dotyczy to szczególnie bezpieczeństwa danych oraz prywatności) i zróżnicowanie wdrażanych technologii stwarza poważne wyzwania w zapewnieniu pełnej integracji środowiska internetu rzeczy. Wobec faktu, iż coraz więcej organizacji przenosi przechowywanie i przetwarzanie dużych danych do chmury w celu ich lepszej analizy, kwestia integracji internetu rzeczy z chmurą obliczeniową również zyskuje na znaczeniu (Botta i in., 2016; Stergiou, 2018). Zadbanie o stworzenie i zdefiniowanie odpowiednich standardów zwiększy skalowalność i elastyczność zastosowań internetu rzeczy (Poudel, 2016). W badaniach zrealizowanych przez PwC (2019), GrowthEnabler (2017), McKinsey (2015) oraz Ernst&Young (2015) osoby zarządzające również wskazały na brak interoperacyjności oraz standaryzacji jako istotne ograniczenia dla zastosowania tej koncepcji.

Skalowalność

Wśród najważniejszych ryzyk dla rozwoju internetu rzeczy w organizacjach Sachin Babar i in. (2010), Denise Lund i in., (2014) oraz Grzegorz Podgórski (2017) wymieniają skalowalność i zarządzanie miliardami obiektów w ekosystemie IoT. Związane jest to głównie z faktem, że, jak podkreślają Artur Rot i Małgorzata Sobińska (2018), prawdziwym wyzwaniem jest zapewnienie bezpiecznej infrastruktury skalowalnej na tyle, aby mogła obsługiwać miliardy urządzeń, zachowując przy tym wysoki poziom bezpieczeństwa przechowywanych, przetwarzanych i przesyłanych danych.

Regulacje prawne

W kontekście barier i zagrożeń nie bez znaczenia pozostają ograniczenia o charakterze prawnym. Składają się na nie zarówno zagadnienia związane z własnością intelektualną, przepisami i regulacjami dotyczącymi ochrony danych, jak i stosowalność prawa w tym zakresie (Koo i Kim, 2018; Peppet, 2014; Podgórski, 2017; Poudel, 2016; Whitmore i in., 2015; Zdravković i in., 2018). Z opinii ekspertów zawartych w raporcie Ernst&Young (2015) wyłania się wniosek, iż istniejące regulacje i przepisy prawne są niedostosowane do rzeczywistości kreowanej przez nowe technologie, co może hamować rozwój koncepcji internetu rzeczy w organizacjach.

Luka kompetencyjna

Patrząc na dynamiczny rozwój omawianej technologii w kontekście znaczących ograniczeń, badacze Porter i Heppelmann (2014) zwracają uwagę na wyzwanie związane z pozyskiwaniem pracowników o nowych umiejętnościach (specjaliści ds. oprogramowania, specjaliści ds. analizy danych). Z niedoborem wyspecjalizowanej kadry w zakresie oprogramowania i analizy danych mierzą się również ankietowani w badaniach przeprowadzonych przez Microsoft (2019), PwC (2019), DZone (2018) oraz Accenture Digital (2017), gdzie respondenci przyznali, że nie dysponują wystarczającą liczbą wykwalifikowanych pracowników w zakresie technologii internetu rzeczy.

Inne obszary zagrożeń dla implementacji internetu rzeczy:

- wysokie nakłady finansowe – koszty zakupu rozwiązań internetu rzeczy, koszty z tytułu zarządzania technologią IoT (Accenture Digital, 2017), wysokie koszty wdrożenia (GrowthEnabler, 2017), wysoki koszt aktualizacji, koszty z tytułu podnoszenia kwalifikacji pracowników (Accenture Digital, 2017; GrowthEnabler, 2017; Microsoft, 2019; PwC, 2019; Podgórski, 2017; Rot i Sobińska, 2018);

- kwestie behawioralne – brak akceptacji zmian wywołanych przez implementację technologii internetu rzeczy (Accenture Digital, 2017; McKinsey, 2015);
- złożoność technologiczna i wyzwania techniczne (KPMG, 2019; Microsoft, 2019; Rot i Sobińska, 2018; Wielki, 2016).

Identyfikacja priorytetowych działań organizacji w procesie implementacji internetu rzeczy

Spojrzenie na najważniejsze korzyści oferowane przez internet rzeczy oraz rozpoznanie barier, zagrożeń i wyzwań z nim związanych pozwala wskazać kluczowe implikacje strategiczne i wewnątrzorganizacyjne, które wymuszają podjęcie określonych działań ze strony organizacji w procesie wdrożenia wspomnianej technologii i jej dalszego rozwoju. Oceniając własne możliwości, zasoby i doświadczenie, firmy muszą podjąć decyzję dotyczącą swojego miejsca w ekosystemie internetu rzeczy. Uwaga przedsiębiorstw powinna również koncentrować się na działaniach dążących do zapewnienia bezpieczeństwa, ochrony prywatności i praw własności oraz wspierania standaryzacji i interoperacyjności rozwiązań IoT. Ponadto skuteczna implementacja wspomnianej technologii wymaga właściwego podejścia do aspektu zarządzania danymi, sprawnej i efektywnej adaptacji procesów biznesowych, przeobrażeń w strukturze i kulturze organizacyjnej, a także inwestycji w systemy analizy danych i talenty.

Implikacje strategiczne

Omówione na wstępie tego artykułu możliwości wynikające z rozwiązań internetu rzeczy przekładają się na powstawanie nowych modeli biznesowych. Projektując je, organizacje muszą określić, jaką rolę będą pełnić w ekosystemie IoT. Pod tym względem mogą one zdecydować się na działalność strategiczną w ramach następujących kategorii (Wielki, 2016, s. 135):

- podmioty rozwijające i implementujące technologie niezbędne do funkcjonowania ekosystemów internetu rzeczy (*enablers*);
- podmioty projektujące, tworzące, integrujące i dostarczające usługi internetu rzeczy klientom *(engagers);*
- podmioty projektujące własne usługi dodające wartość, rozszerzające i integrujące ofertę stworzoną przez przedsiębiorstwa należące do poprzedniej kategorii (*enhancers*).

Korzyści związane z zastosowania internetu rzeczy stwarzają perspektywę konstruowania przez organizacje nowych modeli biznesowych, które są oparte na różnych rozwiązaniach. Mogą one bazować między innymi na (Wielki, 2016):

- danych i ich wykorzystaniu;
- oferowaniu klientom korzystania z oprogramowania udostępnianego w formie usługi (model SaaS);
- wykorzystaniu nowych form outsourcingu;
- profilowaniu behawioralnym;
- oferowaniu inteligentnych produktów będących źródłem dodatkowych korzyści dla klienta;
- oferowaniu klientom dodatkowych usług związanych z fizycznym produktem;
- oferowaniu platform IoT czy kompleksowych rozwiązań infrastrukturalnych IoT.

Jeżeli chodzi o strategiczne pola konkurowania na rynku internetu rzeczy, McKinsey (2015) wyróżnia następujące źródła zdobywania przewagi konkurencyjnej, na bazie których organizacje mogą budować swoją pozycję:

- posiadanie wyróżniającej technologii (*distinctive technology*);
- posiadanie wartościowych zbiorów danych (*distinctive data*);
- posiadanie własnej platformy (*software platforms*);
- zdolność do stworzenia kompleksowych rozwiązań (*complete solutions*).

Aspekty wewnątrzorganizacyjne

Rozważając swoje zaangażowanie w sferę internetu rzeczy, organizacje będą musiały maksymalizować wysiłki wokół licznych wyzwań i modyfikacji związanych z wewnętrznym aspektem swojego funkcjonowania. Z racji tego, że wartość internetu rzeczy jest w dużej mierze kreowana poprzez pozyskiwane i przetwarzane dane, kwestie związane z bezpieczeństwem, ochroną danych i prywatnością stanowią istotny element w działaniach na rzecz jego rozwoju i implementacji, zwłaszcza że utrata danych lub ich prywatności może spowodować znaczne szkody finansowe i wizerunkowe. Zatem planując implementację wspomnianej wyżej technologii, każda organizacja musi skoncentrować się na działaniach związanych z bezpieczeństwem celem zapewnienia prywatności danych gromadzonych przez sensory i przesyłanych przez sieć globalną. Kwestią zasadniczą pozostaje wdrażanie w organizacji odpowiednich procedur dotyczących ochrony informacji wrażliwych i danych osobowych czy weryfikacji autoryzacji dostępu. Dodatkowo ogromna liczba podłączonych do globalnej sieci urządzeń to pole do działania dla cyberprzestępców, którzy mogą przeprowadzać cyberataki. Dlatego konieczne są odpowiednie zabezpieczenia w rozumieniu procesów i rozwiązań technologicznych zapewniających skuteczną ochronę infrastruktury internetu rzeczy. Pozwolą one zminimalizować ryzyko ataku i zapobiec przejęciu kontroli przez cyberprzestępców nad inteligentnymi urządzeniami. Dodatkowo internet rzeczy będzie wymuszać na przedsiębiorstwach uwzględnienie faktu, iż jego adaptacja wiąże się z powołaniem opiekuna danych (ang. *Chief Data Officer*) odpowiedzialnego za strategię zarządzania danymi w organizacji. W świetle powyższego stworzenie i wdrożenie odpowiednich rozwiązań dotyczących gromadzenia, przechowywania, wykorzystywania danych oraz dzielenia się nimi pozostaje kwestią priorytetową.

Dodatkowo organizacjom nie powinien umknąć fakt, że internet rzeczy to ekosystem, na który składają się różne złożone rozwiązania techniczne i technologiczne, dla których konieczna jest odpowiednia warstwa infrastrukturalna. Dlatego ważne jest, aby organizacje decydujące się na jego implementację przeanalizowały kwestie związane z interoperacyjnością. Niezbędne jest wypracowanie otwartych standardów we wszystkich obszarach i na wszystkich poziomach, co pozwoli zapewnić zarówno skuteczną komunikację urządzeń pochodzących od różnych dostawców, jak i współpracę wszystkich podmiotów w ekosystemie internetu rzeczy. Zagadnienie to wydaje się być szczególnie istotne, gdyż właśnie brak interoperacyjności i standaryzacji w obszarze wspomnianej technologii pojawia się jako jedna z zasadniczych barier hamujących rozwój tej innowacyjnej technologii. Ponadto, aby uzyskać przewagę konkurencyjną, organizacje powinny skoncentrować swoje wysiłki na zapewnieniu elastycznej, wydajnej i skalowalnej infrastruktury IT, którą da się łatwo zarządzać (Rot i Sobińska, 2018). Stanowi ona fundament dla efektywnej pracy na dużych zbiorach danych.

Zasobem strategicznym dla każdej organizacji decydującej się na implementację internetu rzeczy są dane. Płynie stąd fundamentalny wniosek: celem uzyskania przez przedsiębiorstwo wartości biznesowej z tej technologii konieczne jest właściwe podejście do analizy danych i co się z tym wiąże – umiejętne przetwarzanie danych w czasie rzeczywistym, gdyż prawdziwy potencjał internetu rzeczy tkwi w pozyskiwaniu i szybkim przetwarzaniu danych. Dlatego jednym z największych wyzwań IoT w organizacjach jest przetwarzanie danych i generowanie wniosków. Poza wydajną infrastrukturą, adaptacji rozwiązań internetu rzeczy muszą towarzyszyć zaawansowane narzędzia i platformy analityczne wielkich zbiorów danych oraz integracja z systemami już istniejącymi. Każda organizacja powinna dysponować odpowiednimi technologiami do wydobywania wartości ze swoich danych, na przykład systemami opartymi na sztucznej inteligencji i uczeniu maszynowym. Co więcej, odbiorcy tych analiz, czyli kadra zarządzająca musi wiedzieć, jak te dane czytać i je interpretować. Dlatego niezwykle ważna jest otwartość menedżerów i ich gotowość do uczenia się interpretacji danych. Jednocześnie przedsiębiorstwa powinny uwzględnić wysokie nakłady finansowe niezbędne, aby uzyskać wartość gospodarczą z tytułu inwestycji w internet rzeczy. Poza wydatkami na systemy do analizy danych trzeba wziąć pod uwagę również wysokie koszty zakupu urządzeń i ich aktualizacji, nakłady na rozbudowywanie sieci internetowych oraz koszty związane z pozyskaniem wyspecjalizowanej kadry i szkoleniami pracowników.

Istotną rolę w kontekście zastosowania koncepcji internetu rzeczy w przedsiębiorstwach pełnią ograniczenia o charakterze prawno-legislacyjnym. Zagadnienia związane ze stworzeniem i wdrożeniem odpowiednich rozwiązań dotyczących gromadzenia, przechowywania, wykorzystywania danych i dzielenia się nimi oraz własnością zgromadzonych danych, jak i ograniczeniami biurokratycznymi mogą w znacznym stopniu wyznaczać kierunek działań organizacji w tym zakresie.

Przystosowując istniejące modele operacyjne do koncepcji internetu rzeczy, każda organizacja powinna kierować swoją uwagę na wewnętrzne działy IT. To właśnie one zapewniają standaryzację i przepływ procesów wewnątrz firmy oraz bezpieczeństwo i ciągłość działania systemów. W rezultacie specjaliści posiadający wiedzę specjalistyczną w zakresie oprogramowania i analizy danych pełnią kluczową rolę podczas realizacji projektów z obszaru IoT. Kwestia ta zyskuje na znaczeniu, tym bardziej że, jak wynika z przeglądu wyników wspomnianych wcześniej badań, organizacje stoją wobec wyzwania niedoboru kadry wyspecjalizowanej w zakresie omawianego rozwiązania technologicznego.

O powodzeniu implementacji internetu rzeczy w organizacji w znacznej mierze będą stanowić możliwości przedsiębiorstwa w zakresie sprawnej adaptacji, modyfikacji, przeprojektowywania obecnych oraz kreowania nowych procesów biznesowych. Brak dojrzałości procesowej firmy i gotowości do wprowadzenia kompleksowych zmian z tytułu wdrożenia internetu rzeczy znacznie zmniejszają szanse na jego powodzenie. W związku z tym stworzenie klimatu organizacji uczącej się, otwartej na daleko idące zmiany i dojrzałej do ich wprowadzenia wydają się być kluczowe w poddawaniu jej przeobrażeniom cyfrowym poprzez adaptację wspomnianej technologii. Odpowiedzialność w tej kwestii spoczywa w dużej mierze na kadrze zarządzającej oraz liderach cyfrowych zmian. Stąd proces rozwoju i adaptacji internetu rzeczy powinien być realizowany przy aktywnym udziale kadry menedżerskiej. Na rolę kadry zarządzającej w tym aspekcie wskazywał już Peter F. Drucker (2010), który podkreślał, że ludzie biznesu nie muszą być technologami czy twórcami technologii. Powinni być raczej zarządzającymi, co wymaga od nich zrozumienia, w jaki sposób technologia dynamizuje działalność biznesową i wyznacza jej kierunek. To na przedstawicielach kadry zarządzającej spoczywa bezpośrednia odpowiedzialność za nadanie tonu kultury organizacji uczącej się, zdolnej do wprowadzania zmian i podejmowania nowych wyzwań. Istotnym jest, aby nakreślili oni jasną wizję kierunku cyfrowego rozwoju przedsiębiorstwa oraz stanowili fundamentalne wsparcie w kompleksowym procesie rozwoju i implementacji innowacyjnej technologii, jaką jest internet rzeczy.

Podsumowanie

W świetle zaprezentowanych rozważań wykorzystanie technologii internetu rzeczy jest szansą dla współczesnych organizacji na podniesienie ich potencjału innowacyjnego oraz efektywne zmierzenie się z dynamicznie zmieniającymi się uwarunkowaniami rynkowymi. Jednak w celu pełnego wykorzystania jej potencjału zastosowań konieczne jest, aby organizacje

podejmowały zasadnicze działania dążące do zapewnienia bezpieczeństwa, ochrony prywatności i praw własności oraz wspierania standaryzacji, interoperacyjności i skalowalności rozwiązań IoT. Ponadto skuteczna implementacja wspomnianej technologii wymaga właściwego podejścia do aspektu zarządzania danymi, sprawnej i efektywnej adaptacji procesów biznesowych, przeobrażeń w strukturze i kulturze organizacyjnej, a także inwestycji w systemy analizy danych i talenty.

Podjęta w pracy problematyka rozwoju koncepcji internetu rzeczy w organizacjach łączy wiedzę zarówno techniczną, jak i organizacyjną. Literatura przedmiotu jest nasycona publikacjami szeroko omawiającymi ogólne korzyści, bariery i wyzwania, jakie wynikają z zastosowania IoT w przedsiębiorstwach. Jednak stosunkowo niewiele jest prac, które jako płaszczyznę rozważań przyjmują głównie kontekst organizacyjny i zarządczy. W powyższym świetle niniejsze opracowanie zawiera praktyczne wskazówki dla organizacji i zarządzających technologią w zakresie działań, jakie powinny zostać podjęte w procesie wdrożenia internetu rzeczy do firmy i jego dalszego rozwoju. Całościowe ujęcie priorytetowych aktywności na rzecz zastosowania wspomnianej koncepcji w organizacjach zostało poprzedzone dogłębną analizą barier, zagrożeń i wyzwań. Warto podkreślić, że znaczna część analizowanej literatury koncentrowała się na ograniczeniach i wyzwaniach natury technicznej, kładąc tym samym większy nacisk na aspekt techniczny aniżeli zarządczy. Może to dowodzić tego, że internet rzeczy w organizacjach znajduje się wciąż na początkowych etapach swojego rozwoju, stąd literatura przedmiotu zdominowana jest przez badania, w których wyakcentowana została głównie strona techniczna związana z wykorzystaniem przez przedsiębiorstwa internetu rzeczy.

Przeprowadzona analiza treści literaturowych ujawnia wieloaspektowosìcì problematyki podjętej w niniejszym opracowaniu i wskazuje konieczność koordynacji wielu działań odbywających się na różnych poziomach organizacyjnych przedsiębiorstwa. W ocenie autorki zdolność organizacji do dynamicznej i efektywnej adaptacji procesów biznesowych może determinować w znacznym stopniu powodzenie implementacji koncepcji internetu rzeczy. W związku z tym przyszłe badania mogłyby rozszerzyć zakres niniejszej pracy badawczej, przyjmując perspektywę spojrzenia opartego na procesach. Przeanalizowanie rozwoju koncepcji internetu rzeczy w organizacjach w ujęciu procesowym pozwoli zaprezentować szersze spojrzenie na omawiane zagadnienie oraz rozpoznać czynniki, które wpływają na poszczególne działania. Wysiłki badawcze w tym zakresie pozwolą na opracowanie modelu wdrożenia IoT do organizacji, który będzie uwzględniał podejście procesowe do zarządzania technologią. Działania zawarte w modelu mogłyby zostać potwierdzone poprzez badania empiryczne. Wyniki tych prac powinny stanowić realne wsparcie dla organizacji w procesie adaptacji internetu rzeczy.

Bibliografia

Accenture Digital i CXP Group (2017). *Digital industrial transformation with the Internet of Things*. https://www.accenture.com/_acnmedia/PDF-49/Accenture-Digital-Industrial-Transformation-with-the-Internet-of-Things.pdf

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. i Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

Ashton, K. (2009, 22 czerwca). That 'Internet of Things' Thing. *RFID Journal*. https://www.rfidjournal.com/that-internet-of-things-thing

Atzori, L., Iera, A. i Morabito, G. (2010). The internet of things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Babar, S., Mahalle, P., Stango, A., Prasad, N. i Prasad, R. (2010). Proposed security model and threat taxonomy for the Internet of Things (IoT). W: N. Meghanathan, S. Boumerdassi, N. Chaki i D. Nagamalai (red.), Recent trends in network security and applications. CNSA 2010. *Communications in Computer and Information Science, 89*. https://doi.org/10.1007/978-3-642-14478-3_42

Botta, A., de Donato, W., Persico, V. i Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future Generation Computer Systems*, *56*, 684–700. https://doi.org/10.1016/j.future.2015.09.021

Butun, I., Österberg, P. i Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks and countermeasures. *IEEE Communications Surveys & Tutorials, 22*(1), 616–644. https://doi.org/10.1109/COMST.2019.2953364

Čolaković, A. i Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks*, *144*, 17–39. https://doi.org/10.1016/j.comnet.2018.07.017

Conti, M., Dehghantanha, A., Franke, K. i Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems, 78*(2), 544–546. https://doi.org/10.1016/j.future.2017.07.060

Dobbs, R., Manyika, J. i Woetzel, J. (2015). *No ordinary disruption: the four global forces breaking all the trends*. PublicAffairs.

Drucker, P. F. (2010). *Toward the next economics and other essays*. Harvard Business Press.

DZone. (2018). *Internet of Things. Harnessing device data*. https://dzone.com/guides/iot-harnessing-device-data

Ernst&Young. (2015). *Internet of Things. Human-machine interactions that unlock possibilities*. https://www.ey.com/Publication/vwLUAssets/ey-m-e-internet-of-things/$FILE/ey-m-e-internet-of-things.pdf

GrowthEnabler. (2017). *Market pulse report, Internet of Things (IoT)*. https://growthenabler.com/flipbook/pdf/IOT%20Report.pdf

Horwitz, L. (2019, 19 lipca). *The future of IoT miniguide: The burgeoning IoT market continues*. https://www.cisco.com/c/en/us/solutions/internet-of-things/future-of-iot.html

Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S. i Boyle, D. (2014). *From machine-to-machine to the Internet of Things: Introduction to a new age of intelligence*. Academic Press. https://doi.org/10.1016/B978-0-12-407684-6.00001-2

Hsu, Ch-L. i Lin, J. Ch-Ch. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior, 62*, 516–527. https://doi.org/10.1016/j.chb.2016.04.023

IDC. (2020a, 11 sierpnia). *Internet of Things ecosystem and trends*. https://www.idc.com/getdoc.jsp?containerId=IDC_P24793&pageType=PRINTFRIENDLY

IDC. (2020b, 18 czerwca). *Worldwide spending on the Internet of Things will slow in 2020 then return to double-digit growth*. https://www.idc.com/getdoc.jsp?containerId=prUS46609320

Kiełtyka, L. i Zygoń, O. (2018). Współczesne formy komunikacji – jak zarządzać z wykorzystaniem Internetu Rzeczy i Wszechrzeczy. *Przegląd Organizacji*, *2*(937), 24–33. https://doi.org/10.33141/po.2018.02.04

Koo, C. i Kim, J. (2018). Enforcing high-level security policies for Internet of Thing. *The Journal of Supercomputing*, *74*, 4497–4505. https://doi.org/10.1007/s11227-017-2201-9

Kouicem, D. E., Bouabdallah, A., Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks*, *141*(4), 199–221. https://doi.org/10.1016/j.comnet.2018.03.012

KPMG. (2019). *The top 10 technologies for business transformation*. https://assets.kpmg/content/dam/kpmg/ie/pdf/2019/05/ie-top-10-technologies-for-business-transformation.pdf

Lee, I. i Lee, K. (2015). The internet of things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431–440. https://doi.org/10.1016/j.bushor.2015.03.008

Lopez, J., Rios, R., Bao, F. i Wang, G. (2017). Evolving privacy: From sensors to the Internet of Things. *Future Generation Computer Systems*, *75*, 46–57. http://doi.org/10.1016/j.future.2017.04.045

Lund, D., MacGillivray, C., Turner, V. i Morales, M. (2014). *Worldwide and regional Internet of Things (IoT) 2014–2020 forecast: A virtuous circle of proven value and demand.* International Data Corporation. http://branden.biz/wp-content/uploads/2017/06/IoT-worldwide_regional_2014-2020-forecast.pdf

McKinsey Global Institute. (2015). *The Internet of Things: Mapping the value beyond the hype*. https://mck.co/2D5v5Qq

Ménard, A. (2017, 15 listopada). How can we recognize the real power of the Internet of Things? *McKinsey Digital.* https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/how-can-we-recognize-the-real-power-of-the-internet-of-things

Microsoft. (2019). *IoT Signals. Summary of research learnings 2019*. https://azure.microsoft.com/en-us/resources/iot-signals

Miorandi, D., Sicari, S., De Pellegrini, F. i Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516. https://doi.org/10.1016/j.adhoc.2012.02.016

Newman, P. (2020, 6 marca). *THE INTERNET OF THINGS 2020: Here's what over 400 IoT decision-makers say about the future of enterprise connectivity and how IoT companies can use it to grow revenue*. Business Insider. https://www.businessinsider.com/internet-of-things-report?IR=T

Ng, I. C. L. i Wakenshaw, S. Y. L. (2017). The internet-of-things: Review and research directions. *International Journal of Research in Marketing*, *34*(1), 3–21. https://doi.org/10.1016/j.ijresmar.2016.11.003

Nicolescu, R., Huth, M., Radanliev, P. i De Roure, D. (2018). Mapping the values of IoT. *Journal of Information Technology*, *33*(4), 345–360. https://doi.org/10.1057/s41265-018-0054-1

Nord, J. H., Koohang, A. i Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, *133*, 97–108. https://doi.org/10.1016/j.eswa.2019.05.014

Peppet, S. R. (2014). Regulating the Internet of Things: First steps toward managing discrimination, privacy, security and consent. *Texas Law Review, 93*(1), 85–178. https://texaslawreview.org/wp-content/uploads/2015/08/Peppet-93-1.pdf

Podgórski, G. (2017). Zagrożenia związane z Internetem Rzeczy. W: K. Kolasińska-Morawska (red.), Zarządzanie logistyczne-informacja, procesy, technologie. *Przedsiębiorczość i Zarządzanie*, *18*(4), cz. 3, 247–256.

Porter, M. E. i Heppelmann, J. E. (2015). How smart, connected products are transforming companies. *Harvard Business Review*, *October*, 96–114.

Porter, M. E. i Heppelmann, J. E. (2014). How smart, connected products are transforming competition. *Harvard Business Review*, *November*, 64–88.

Poudel, S. (2016). Internet of Things: Underlying technologies, interoperability and threats to privacy and security. *Berkeley Technology Law Journal*, *31*(2), 997–1022. https://doi.org/10.15779/Z38WW0V

PwC. (2019). *IoT Survey: Speed operations, strengthen relationships and drive what's next*. https://www.pwc.com/us/en/services/consulting/technology/emerging-technology/iot-pov.html

Rot, A. (2017). Bezpieczeństwo jako najważniejsze wyzwanie koncepcji Internetu rzeczy. W: K. Kolasińska-Morawska i P. Morawski (red.), Agile Commerce – technologie przyszłości. *Przedsiębiorczość i Zarządzanie, 18*(4), cz. 2, 285–296.

Rot, A. i Blaicke, B. (2017). Bezpieczeństwo Internetu Rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych. *Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie*, *26*, 188–198. DOI:10.17512/znpcz.2017.2.17

Rot, A. i Sobińska, M. (2018). Skalowalność, bezpieczeństwo i interoperacyjność jako kluczowe wyzwania dla projektowania systemów Internetu rzeczy. *Zeszyty Naukowe Politechniki Częstochowskiej. Zarządzanie*, *31,* 212–221. DOI:10.17512/znpcz.2018.3.18

Saarikko, T., Westergren, U. i Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming? *Business Horizons*, *60*(5), 667–676. https://doi.org/10.1016/j.bushor.2017.05.010

Sicari, S., Rizzardi, A., Grieco, L. A. i Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Stergiou, Ch., Psannis, K., Kim, B-G. i Gupta, B. (2018). Secure integration of IoT and Cloud Computing. *Future Generation Computer Systems*, *78*(3), 964–975. https://doi.org/10.1016/j.future.2016.11.031

Suppatvech, Ch., Godsell, J. i Day, S. (2019). The roles of internet of things technology in enabling servitized business models: A systematic literature review. *Industrial Marketing Management*, *82*, 70–86. https://doi.org/10.1016/j.indmarman.2019.02.016

Vermesan, O. i Friess, P. (red.). (2014). *Internet of Things – from research and innovation to market deployment*. River Publishers.

Weinberg, B. D., Milne, G. R., Andonova, J. G. i Hajjat, F. M. (2015). Internet of Things: Convenience vs. privacy and secrecy. *Business Horizons*, *58*(6), 615–624. https://doi.org/10.1016/j.bushor.2015.06.005

Whitmore, A., Agarwal. A. i Da Xu, L. (2015). The Internet of Things: A survey of topics and trends. *Information System Frontiers*, *17*, 261–274. https://doi.org/10.1007/s10796-014-9489-2

Wielki, J. (2016). Analiza szans, możliwości i wyzwań związanych z wykorzystaniem Internetu Rzeczy przez współczesne organizacje gospodarcze. W: R. Patora i P. Morawski (red.), Agile Commerce – zarządzanie informacją. *Przedsiębiorczość i Zarządzanie*, *17*(11), cz. 1, 127–140.

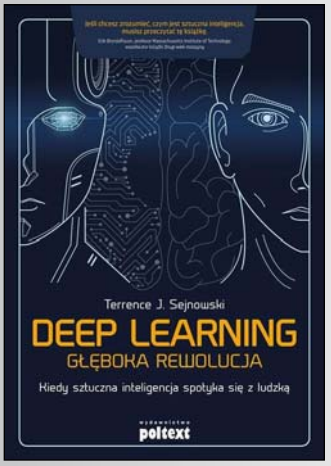
Zdravković, J., Zdravković, M., Aubry, A., Moalla, N., Guedria, W. i Sarraipa, J. (2018). Domain framework for implementation of open IoT ecosystems. *International Journal of Production Research*, *56*(7), 2552–2569. https://doi.org/10.1080/00207543.2017.1385870

Ziegeldorf, J. H., Morchon, O. G. i Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728–2742. https://doi.org/10.1002/sec.795

Zebra Technologies. (2019). *The intelligent enterprise index*. https://www.zebra.com/content/dam/zebra_new_ia/en-us/campaigns/brand-campaign/harvard-symposium/how-intelligent-enterprise-survey-index-en-us.pdf

Katarzyna Liwarska-Fulczyk jest doktorantką Wydziału Zarządzania na Uniwersytecie Ekonomicznym we Wrocławiu. Główny obszar jej zainteresowań badawczo-naukowych to zastosowanie metod i technik sztucznej inteligencji w procesach zarządzania, ludzie i maszyny jako zintegrowane zespoły oraz transformacja cyfrowa przedsiębiorstw. Jest konsultantem w zakresie komercjalizacji technologii. Na co dzień współpracuje z polskimi i międzynarodowymi organizacjami gospodarczymi.

Polecamy



Terrence J. Sejnowski, *Deep learning. Głęboka rewolucja. Kiedy sztuczna inteligencja spotyka się z ludzką*

Terrence Sejnowski, jeden z twórców koncepcji głębokiego uczenia, przedstawia jak na przestrzeni lat ewoluował sposób rozumienia sztucznej inteligencji i jak uczą się maszyny. W przedmowie stwierdza, że napisana przez niego książka stanowi „przewodnik po przeszłości, teraźniejszości i przyszłości głębokiego uczenia". A że autor jest zaangażowany w prace nad sztuczną inteligencją od lat osiemdziesiątych ubiegłego stulecia, może na ten temat powiedzieć naprawdę dużo, i – co szczególnie warte podkreślenia – naukowy wywód ilustruje licznymi zdjęciami i ciekawostkami. Dzięki lekturze tej pozycji dowiemy się nie tylko jak rozwijała się ta dziedzina wiedzy, ale też jacy ludzie byli zaangażowani w ten proces.
Więcej informacji na temat książki można znaleźć na stronie wydawcy:
http://www.poltext.pl/b2390-deep-learning-gleboka-rewolucja.htm

Raport SGH i Forum Ekonomicznego 2020

Podczas niedawnego Forum Ekonomicznego w Karpaczu (8–10.09.2020) został zaprezentowany kolejny raport opracowany przez ekspertów ze Szkoły Głównej Handlowej w Warszawie, w którym przedstawiono wybrane problemy oraz wyzwania stojące przed krajami Europy Środkowo-Wschodniej. Tegoroczna publikacja zawiera podsumowanie reform społecznych i gospodarczych, które dokonały się w Polsce oraz w innych krajach regionu w ciągu ostatnich 30 lat.
Jak można przeczytać na stronie SGH: „Wybuch globalnej pandemii COVID-19 i jej dalekosiężne konsekwencje sprawiły, że autorzy raportu zdecydowali się odnieść wyniki swoich badań również do bieżącej sytuacji. Pokazują, w jaki sposób zjawisko to wpłynęło i nadal może wpływać na procesy społeczne i gospodarcze tak w Polsce, jak i w pozostałych krajach Europy Środkowej i Wschodniej. Starają się również ocenić, w jakim stopniu reformy przygotowały kraje regionu na obecny kryzys".
Więcej informacji pod adresem:
https://ssl-www.sgh.waw.pl/pl/Strony/forumekonomiczne2020.aspx