Andrzej Kobyliński

Internet przedmiotów : szanse i zagrożenia

Ekonomiczne Problemy Usług nr 112, 101-109

2014

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 808 EKONOMICZNE PROBLEMY USŁUG NR 112 2014

ANDRZEJ KOBYLIŃSKI
Szkoła Główna Handlowa w Warszawie[1]

INTERNET PRZEDMIOTÓW: SZANSE I ZAGROŻENIA

Streszczenie

Od kiedy na przełomie lat 2008/2009 liczba urządzeń podłączonych do Internetu przekroczyła liczbę mieszkańców Ziemi, uznaje się, że mamy do czynienia z Internetem przedmiotów (rzeczy). Połączenie w jedną, heterogeniczną sieć tak dużej liczby inteligentnych obiektów stwarza niedostępne dotychczas możliwości. Z drugiej strony, niesie też zagrożenia, szczególnie dotyczące bezpieczeństwa i utraty prywatności. Powstaje też kwestia wielu innych problemów, które wymagają rozwiązania (np. standaryzacji). Celem pracy jest prezentacja możliwości i korzyści, jakie możliwe są do uzyskania w efekcie wdrożenia koncepcji Internetu przedmiotów, jak również potencjalnych zagrożeń i wyzwań, jakie są z tym związane.
Słowa kluczowe: Internet przedmiotów, Internet rzeczy, IoT, inteligentne obiekty.

Wprowadzenie

Internet przedmiotów (zwany również Internetem rzeczy, ang. *Internet of Things* – IoT) stanowi kolejny etap w rozwoju ogólnoświatowej sieci Internet. W dotychczasowym znaczeniu Internet rozumiany jest jako sieć współpracujących ze sobą komputerów (serwerów i hostów), wykorzystujących do współpracy protokół TCP/IP, a w szczególności identyfikowanych przy pomocy adresu IP (ang. *IP address*). W dotychczasowej historii swego rozwoju do Internetu podłączone było, poczynając od kilkunastu serwerów w końcu lat 60., aż do ponad miliarda komputerów, jak to ma miejsce obecnie. I o ile przez pierwsze dziesiątki lat rozwo-

[1] Kolegium Analiz Ekonomicznych, Instytut Informatyki i Gospodarki Cyfrowej.

ju Internetu urządzeniami podłączonymi do sieci były zasadniczo komputery, o tyle w ostatnich latach, w związku w rozpowszechnieniem się całej gamy urządzeń sterowanych mikroprocesorami, podłączane są do Internetu kolejne typy urządzeń: smartfony, tablety, telewizory, netbooki, czytniki e-booków i inne. Szacuje się (dokładne obliczenia nie są możliwe ze względu na gwałtowny postęp i ciągle zmieniającą się sytuację), że na przełomie lat 2008/2009 liczba urządzeń podłączonych do sieci przekroczyła liczbę mieszkańców Ziemi (czyli ok. 6,5 mld), a obecnie (stan na początek roku 2014) osiąga wartości zbliżone do 20 mld (Evans 2011, s. 2–3). Właśnie czas, kiedy liczba podłączonych do Internetu urządzeń przekroczyła liczbę mieszkańców Ziemi, przyjmowany jest za symboliczny początek Internetu przedmiotów.

Połączenie w jedną, heterogeniczną sieć tak olbrzymiej liczby urządzeń, i to nie na zasadzie podłączania urządzeń jak do sieci elektrycznej, gdzie podłączane urządzenia są anonimowe, ale na zasadzie „inteligentnej", rozumianej jako możliwość ich jednoznacznej identyfikacji, możliwości komunikowania się urządzeń między sobą i współdziałania, prowadzi do uzyskiwania licznych korzyści, niemożliwych do osiągnięcia bez usieciowienia urządzeń, ale z drugiej strony stwarza wiele problemów, które czekają na rozwiązanie. I właśnie celem tej pracy jest prezentacja możliwości i korzyści, jakie można będzie uzyskać w efekcie wdrożenia koncepcji IoT, ale z drugiej strony – potencjalnych zagrożeń i wyzwań, jakie są z tym związane.

1. Podstawy techniczne

Dotychczas nie została powszechnie zaakceptowana definicja Internetu rzeczy. Przegląd licznych definicji dokonany został w pracy (Perera, Zaslavsky, Christen, Georgakopoulos 2013). Jedną z takich definicji jest Internet inteligentnych obiektów (ang. *Internet of Smart Objects*) (Kortuem, Kawsar, Fitton, Sundramoorthy 2010; Brachman 2013, s. 6).

Historycznie rzecz ujmując, Internet przedmiotów zainspirowany został głównie przez rozwój technologii RFID (ang. *radio-frequency identification*), która stanowiła kolejny etap w rozwoju sposobu identyfikowania obiektów (wcześniejsze to kody paskowe i kody dwuwymiarowe, np. *QR Code*), a która jest z olbrzymim sukcesem wykorzystywana głównie do śledzenia różnego rodzaju obiektów: produktów, zwierząt, a nawet ludzi. W systemie wykorzystującym RFID można wyraźnie wyróżnić dwie klasy urządzeń: znaczniki (transpondery) RFID, które pełnią rolę bierną i uaktywniają się po znalezieniu się w polu odczytu urządzeń o charakterze czynnym: czytników RFID. Rozwiązania tego typu szczególnie dobrze sprawdzają się w sytuacjach, gdy obiekty wyposażone w znaczniki RFID przekraczają ściśle określone granice (np. zakładu przemysłowego, hurtowni, sklepu, państwa, wyciągu

narciarskiego, autobusu, biura, pastwiska…), ale nieszczególnie nadają się do bardziej wyrafinowanych rozwiązań, szczególnie ze względu na konieczność istnienia infrastruktury czytników RFID. Rozwój Internetu rzeczy stanowi kolejny etap rozwoju tego typu aplikacji – jako zdecentralizowanego systemu luźno ze sobą powiązanych inteligentnych obiektów. Inteligencja tych obiektów polega na tym, że nie tylko posiadają informacje o swoim stanie, którą mogą przekazywać elementom aktywnym (czytnikom), jak to jest w rozwiązaniach RFID, ale są na tyle autonomiczne, że oprócz możliwości przechowywania danych mają również możliwość komunikowania się z innymi obiektami, analizowania posiadanych i zdobytych z otoczenia danych, a także podejmowania decyzji i sterowania innymi obiektami. Inteligentne obiekty są to małe urządzenia elektroniczne, składające się z mikroprocesora, jednostki transmisyjnej (zwykle radia małej mocy), sensora (umożliwiającego zbieranie informacji z otoczenia) lub/i urządzenia wykonawczego (ang. *actuator*), umożliwiającego sterowanie, czyli wpływanie na otaczający świat (Brachman 2013, s. 7). Mikroprocesory sterowane są programami, które pozwalają obiektom na rozpoznawanie ich aktualnej sytuacji i na interakcję z ludźmi. Wyczuwają, zapamiętują i interpretują, co dzieje się z nimi i z otaczającym ich światem, działają na własną rękę (zgodnie z zapisanym algorytmem), komunikują się z innymi obiektami i z ludźmi.

Zakłada się, że inteligentne obiekty będą mogły być wbudowane w dowolne urządzenia techniczne, jak urządzenia przemysłowe, sprzęty domowe, liczniki, silniki, przełączniki itp. Daje to perspektywę zaprojektowania najróżniejszych aplikacji, które mogą opierać się zarówno na modelu komunikacji rzecz–człowiek (Thing-To-Person T2P), jak i współpracy maszyna–maszyna (Machine-To-Machine M2M). Aplikacje te znaleźć będzie można w różnych miejscach: w przemyśle, w handlu, w domu; a będą mogły mieć zastosowanie zarówno ograniczone do pewnego obszaru (intranet rzeczy), jak i dostępne publicznie (Internet rzeczy) (Internet of Things 2009).

2. Obszary zastosowań Internetu rzeczy

Możliwe dziedziny zastosowania Internetu przedmiotów są rozliczne i na obecnym etapie rozwoju trudne nawet do wyobrażenia. Ale już na tym wstępnym etapie można sobie wyobrazić liczne zastosowania, przy czym wiele z nich nie jest w sferze przewidywań, a stały się już rzeczywistością.

Klienci wyposażeni w smartfony lub telefony z opcją NFC (ang. *near field communication* – komunikacja krótkiego zasięgu) (NFC 2014) po zrobieniu zdjęcia lub zbliżeniu do transpondera NFC mogą uzyskać dodatkowe informacje na temat kupowanego produktu, np. szczegółowych właściwości technicznych, możliwych własności alergizujących (w przypadku leku lub produktu żywnościowego) itp.

Państwa członkowskie Unii Europejskiej powszechnie wykorzystują unikalne numery seryjne produktów farmaceutycznych (zarejestrowane w kodach kreskowych), umożliwiające weryfikację każdego produktu medycznego, zanim ten dotrze do pacjenta. Zmniejsza to fałszerstwa, oszustwa i błędy dozowania (Stamping 2014). Podobne ogólne podejście dotyczące możliwości śledzenia produktów konsumpcyjnych w ogóle pozwala poprawić zdolność do walki z podrabianiem towarów i do zastosowania środków przeciwko niebezpiecznym produktom (Keeping 2012).

Część przedsiębiorstw w sektorze energetycznym rozpoczęła wdrażanie inteligentnych elektrycznych systemów pomiarowych, które dostarczają odbiorcom informacji w czasie rzeczywistym (np. dotyczących aktualnych cen energii) i umożliwiają zdalne monitorowanie urządzeń elektrycznych dostawcom energii elektrycznej (Mój licznik 2014).

W ramach tradycyjnych gałęzi przemysłu, takich jak logistyka, produkcja i handel, „inteligentne obiekty" ułatwiają wymianę informacji i zwiększenie efektywności cyklu produkcyjnego.

Inteligentne obiekty zastosowane na polach będą mogły poinformować urządzenia irygacyjne, że gleba jest za sucha, rośliny wymagają nawożenia, albo że rośliny zostały zaatakowane przez owady lub chorobę (Finley 2014).

Budzik może wcześniej niż zwykle obudzić człowieka, kiedy dostanie informację o większym niż zazwyczaj nasileniu ruchu samochodowego na drodze do pracy (Brachman 2013, s. 6). Zasobnik na leki może sygnalizować, że nie zażyto leku (Brachman 2013, s. 7).

Podobnych zastosowań może być wiele, wymienione wyżej są często podawane jako przykładowe w literaturze przedmiotu, ich rozbudowaną listę można znaleźć na przykład w (Vermesan, Friess 2013, s. 31–61). Ale wszystkie one bazują na takich wzmiankowanych już technologiach, jak RFID, NFC, bezprzewodowe sensory i urządzenia wykonawcze, adresowanie IP, szerokopasmowe łącza.

3. Niebezpieczeństwa IoT

Ale oczywiście, jak każde nowe rozwiązanie, również Internet przedmiotów niesie ze sobą pewne niebezpieczeństwa. Niewątpliwie na pierwszy plan wysuwa się kwestia prywatności oraz bezpieczeństwa. Inteligentne obiekty, wyposażone | w znaczniki RFID lub inne przekaźniki małej mocy, które mogą być identyfikowane przez różnorodne urządzenia na całym świecie, stanowią ewidentne zagrożenie dla prywatności. Jednoznacznie identyfikowalne obiekty, przypisane do poszczególnych osób (e-paszporty, elektroniczne karty bankowe [karty czipowe, ang. *smart cards*], elektroniczne legitymacje, elektroniczne karty miejskie, telefony komórkowe itp.), pozwalają na stosunkowo dokładną lokalizację każdego człowieka posłu-

gującego się takimi urządzeniami i przewidywanie dotyczące wykonywanych przez niego czynności.

Z drugiej strony, ponieważ większość wymienionych wyżej urządzeń pozwala na odczytywanie przechowywanych przez nie danych przy pomocy technologii bezstykowych, zarówno w formie kart zbliżeniowych (ang. *proximity cards*) o zasięgu do 10 cm (ISO/IEC 14443), jak i kart dystansowych (ang. *vicinity cards*) o zasięgu do 1 m (ISO/IEC 15693), co jest wykorzystywane do wykonywania legalnych transakcji, są one podatne na dokonywanie *skimmingu*[2] i podsłuchy (Hancke 2011). Oczywiste jest, że problem podsłuchów można minimalizować stosując rozwiązania kryptograficzne i inne. Prace badawcze dotyczące bezpieczeństwa rozwiązań prowadzone są na bardzo szeroką skalę. Portal *RFID Security and Privacy Lounge* (RFID 2014) oferuje dostęp do ponad 700 artykułów naukowych poświęconych problematyce prywatności i bezpieczeństwa, które opublikowane zostały w ostatnich 12 latach.

Do kwestii bezpieczeństwa i prywatności bardzo dużą wagę przywiązują instytucje Unii Europejskiej (Internet of Things 2009, s. 5–6; Internet przedmiotów 2010).

Problem prywatności i bezpieczeństwa jest coraz szerzej nagłaśniany medialnie, a zjawisko powszechnej inwigilacji, które do tej pory mogło być jedynie w sferze domysłów, w połowie 2013 r. zostało potwierdzone twardymi dowodami, po ujawnieniu danych dotyczących programu PRISM (Rushe, Ball 2013). Agencja Bezpieczeństwa Narodowego (NSA) ma dostęp do danych gromadzonych przez AOL, Apple, Dropbox, Google, Facebook, Microsoft, PalTalk, Yahoo, Skype (własność Microsoftu) oraz YouTube (własność Google). I można podejrzewać, że na miarę swoich możliwości inne kraje prowadzą podobne projekty. Służby specjalne od dziesiątków lat tłumaczą się, że inwigilacja odbywa się wyłącznie w imię bezpieczeństwa narodowego i jeśli ktoś nie ma nic do ukrycia, to nie powinno mu przeszkadzać, że służby specjalne mogą mieć jakieś dane na jego temat. Ostatecznie każdy może postępować jak Jack Reacher, bohater powieści kryminalnych Lee Childa, który nie ma SSN, telefonu komórkowego, posługuje się wyłącznie gotówką, a podróżuje autobusami, żeby nikt nie mógł go namierzyć. Nie jest to jednak sposób na życie, jaki mogłyby zastosować większe grupy osób.

4. Wyzwania

Powstawanie Internetu rzeczy nastąpiło w zasadzie samoistnie, nie sterowane odgórnymi zaleceniami. Ale rozwój ten nie może następować w sposób całkowicie woluntarystyczny, niektóre sprawy nie mogą pozostać całkiem nieuporządkowane i podlegać prawom wolnego rynku. Niektóre rzeczy muszą podlegać standaryzacji.

[2] Przestępstwo polegające na sczytywaniu kodów z kart magnetycznych lub elektronicznych.

W szczególności dotyczy to problemów związanych z prywatnością, bezpieczeństwem, rozwiązaniami architektonicznymi. Na temat prywatności i bezpieczeństwa było już wspomniane, pora przedyskutować problemy techniczne.

Internet rzeczy ma charakter heterogeniczny – spotykać w nim można bardzo różnorodne pod względem technicznym rozwiązania. I z pewnością sytuacja ta ma charakter trwały – kolejni producenci będą oferowali rozwiązania różniące się technologicznie. I można liczyć na to, że w miarę upływu czasu największą popularność zdobędą rozwiązania oferowane przez największych graczy, jacy wyłonią się na rynku, przekształcając się w standardy *de facto*. Rozwiązanie takie nie jest pozbawione wad – może się zdarzyć, że produkty mniejszych graczy, nie ustępujące rozwiązaniom największych graczy pod względem dojrzałości technologicznej, a nawet je przewyższające, nie zdobędą popularności. W historii informatyki znanych było wiele takich przypadków. Wydaje się, że jest tu do spełnienia rola dla organizacji międzynarodowych, które mogłyby zaproponować takie standardy obowiązujące na polu Internetu rzeczy, które obniżyłyby bariery wejścia dla nowych podmiotów gospodarczych, a użytkownikom obniżyłyby koszty operacyjne, wymuszając już na wstępie interoperacyjność rozwiązań i powodując przez to łatwiejsze uzyskanie efektu skali, co pozwoliłoby lepiej konkurować na szczeblu globalnym (Internet of Things 2009, s. 7). Standardy te, jeśliby powstały, powinny być bardzo elastyczne. Internet rzeczy znajduje się obecnie na bardzo wstępnym etapie i trudno przewidzieć, w jakich kierunkach będzie następował jego dalszy rozwój. Powstające obecnie aplikacje ukierunkowane są na rozwiązywanie pewnych szczególnych problemów. Dostosowanie takich aplikacji do rozwiązywania innych problemów może być utrudnione, jeżeli już na wstępie nie będą uwzględnione elastyczne mechanizmy, szczególnie dotyczące interoperacyjności i możliwości integracji z innymi rozwiązaniami (Brachman 2013, s. 7).

Przykładem takiego braku uzgodnień na poziomie międzynarodowym, utrudniającego handel międzynarodowy, może być technologia RFID. Istnieje na tym polu kilka organizacji standaryzujących, a np. RFID używane w USA są niekompatybilne z używanymi w Unii Europejskiej oraz w Japonii, a co więcej – nie istnieje standard ujednolicający te konkurencyjne rozwiązania (Radio 2014).

Uważa się, że inteligentne obiekty wykorzystywane w IoT powinny być jednoznacznie adresowane. Naturalnym kandydatem takiego schematu adresowania jest adres IP. Obecnie obiekty podłączone do sieci Internet adresowane są przy pomocy adresu IP w wersji 4 (IPv4). Jest to adresowanie 32-bitowe. W związku z ogromną popularnością Internetu pula adresów IPv4 wyczerpała się w lutym 2011 r. (Free 2011). Na szczęście istnieją już od dawna uzgodnienia dotyczące kolejnej, tym razem już 128-bitowej wersji adresowania – *Internet Protocol version 6* (IPv6). Pełne wdrożenie tego sposobu adresowania stanowi kolejne wyzwanie niezbędne do realizacji zamierzenia, by Internet rzeczy mógł w pełni pokazać swe możliwości (Evans 2011, s. 9).

Kolejny problem wiążący się z Internetem inteligentnych obiektów bywa niekiedy niedoceniany, a ma on olbrzymie znaczenie praktyczne. Problemem tym jest zasilanie inteligentnych obiektów w energię elektryczną. Ponieważ inteligentne obiekty mają być mobilne, nie można liczyć na to, że będą mogły być zasilane w energię elektryczną pobieraną ze źródeł stacjonarnych. Mogą one być zasilane z baterii i akumulatorów, ale trzeba zdawać sobie sprawę z konieczności kontrolowania i wymiany baterii w miliardach takich urządzeń. Poza tym baterie i akumulatory są niepraktyczne ze względu na ich masę i rozmiar, dodatkowo postęp w technologii wytwarzania akumulatorów i baterii nie przebiega tak szybko, jak to jest np. w elektronice. W artykule była już mowa o technologii RFID – ale urządzenia zasilane w energię elektryczną indukowaną w antenie znacznika i gromadzoną w kondensatorze mają bardzo mały zasięg komunikowania się i znikome możliwości funkcjonalne (Anderseck, Hengst, Wilken 2013, s. 46). Dlatego trzeba liczyć na niekonwencjonalne rozwiązania, jak korzystanie z energii światła słonecznego, energii termicznej, energii mechanicznej (Vermesan, Friess 2013, s. 98).

Podsumowanie

Firma konsultacyjna Gartner co roku publikuje wykaz najbardziej obiecujących technologii. W roku 2012 Internet przedmiotów po raz pierwszy znalazł się w tym zestawieniu, zajmując 4. pozycję (Gartner 2012), a w kolejnym roku 5. miejsce (Gartner 2013). To wysokie miejsce IoT zostało potwierdzone również w innym rankingu, opracowanym przez (Greengard 2014), który przyznał Internetowi przedmiotów 4. miejsce w 2014 r. Gartner, prognozując trendy technologiczne w 2014 r., idzie dalej – Internetu rzeczy nie ma już w klasyfikacji. Ale nie znaczy to, że jest to technologia dojrzała, stosowana powszechnie (takie wypadają z zestawienia). W rankingu Gartnera pojawiła się za to kolejna nowość – będąca następnym krokiem w ewolucji tej technologii: *Internet of Everything* (IoE – Internet wszechrzeczy). Internet wszechrzeczy to sieć łącząca ludzi, procesy, dane i przedmioty, generująca pewną nową wartość. Kolejne etapy rozwoju technologicznego: mobilna rewolucja, *cloud computing*, Internet rzeczy i rosnące znaczenie *Big Data*, uzupełniając się, pozwalają na korzystanie z możliwości, jakie da Internet wszechrzeczy (Evans 2013).

Literatura

Anderseck B., Hengst C., Wilken M. (2013), *Valuation of hybrid identification processes as an enabler for the Internet of Things*, w: red. U. Clausen, M. ten Hompel, M. Klumpp, *Efficiency and Logistics*, Springer.

Brachman A. (2013), *Internet przedmiotów*, Raport Obserwatorium ICT, Technopark Gliwice.

Evans D. (2011), *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, CISCO IBSG 2011, http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [dostęp 5.01.2014].

Evans D. (2013), *Beyond Things: The Internet of Everything, Explained in Four Dimensions*, The Huffington Post, 24-09-2013, http://www.huffingtonpost.com/ dave-evans/cisco-beyond-things-the-interne_b_3976104.html [dostęp 10.02.2014].

Finley K. (2014), *The Internet of Vegetables: How Cyborg Plants Can Monitor Our World*, Wired, http://www.wired.com/wiredenterprise/2014/01/internet-plants/ [dostęp 4.02.2014].

Free Pool of IPv4 Address Space Depleted, 3 February 2011, http://www.nro.net/news/ipv4-free-pool-depleted [dostęp 23.01.2014].

Gartner (2012), *Gartner Identifies the Top 10 Strategic Technologies for 2012*, Orlando 18-10-2011, http://www.gartner.com/newsroom/id/1826214 [dostęp 10.01.2014].

Gartner (2013), *Gartner Identifies the Top 10 Strategic Technology Trends for 2013*, Orlando 23-10-2012, http://www.gartner.com/newsroom/id/2209615 [dostęp 10.01.2014].

Gartner (2014), *Gartner Identifies the Top 10 Strategic Technology Trends for 2014*, Orlando 8-10-2013, http://www.gartner.com/newsroom/id/2603623 [dostęp 10.01.2014].

Greengard S. (2014), *Six Top Tech Trends to Watch in 2014*, 18-12-2013, http://www.baselinemag.com/innovation/six-top-tech-trends-to-watch-in-2014.html [dostęp 10.01.2014].

Hancke G.P. (2011), *Practical eavesdropping and skimming attacks on high-frequency RFID tokens*, Journal of Computer Security, Vol. 19, No. 2, pp. 259–288, http://iospress.metapress.com/content/xx855446h2kh84r2/ [dostęp 25.01.2014].

Internet of Things — An action plan for Europe (2009), Commission of the European Communities, Brussels, http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF [dostęp 30.01.2014].

Internet przedmiotów. Rezolucja Parlamentu Europejskiego z dnia 15 czerwca 2010 r. w sprawie Internetu przedmiotów (2009/2224(INI)) – 2011/C 236 E/04, Dziennik Urzędowy C236E Unii Europejskiej, http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=OJ:C:2011:236E:FULL:PL:PDF [dostęp 26.01.2014].

ISO/IEC 14443 Identification cards – Contactless integrated circuit cards – Proximity cards (part 1–4) 2001 and 2008.

ISO/IEC 15693 Identification cards – Contactless integrated circuit cards – Vicinity cards (part 1–3) 2006-2010.

Keeping European Consumers Safe. 2012 Annual Report on the operation of the Rapid Alert System for non-food dangerous products RAPEX, http://ec.europa.eu/ consumers/safety/rapex/docs/2012_rapex_report_en.pdf [dostęp 30.01.2014].

Kortuem G., Kawsar F., Fitton D., Sundramoorthy V. (2010), *Smart Objects as Building Blocks for the Internet of Things*, IEEE Internet Computing, No. 1/2.

„Mój licznik". Aplikacja mobilna Energi-Operator umożliwi śledzenie poboru energii, http://gramwzielone.pl/dom-energooszczedny/8199/moj-licznik-aplikacja-mobilna-energi-operator-umozliwi-sledzenie-poboru-energii [dostęp 30.01.2014).

NFC Forum, http://nfc-forum.org/ [dostęp 31.01.2014].

Perera C., Zaslavsky A., Christen P., Georgakopoulos D. (2013), *Context Aware Computing for the Internet of Things: A Survey*, IEEE Communications Surveys & Tutorials, Vol. 16, Issue 1.

Radio-frequency identification, http://en.wikipedia.org/wiki/Radio-frequency_identification [dostęp 25.01.2014].

RFID Security and Privacy Lounge, http://avoine.net/rfid/ [dostęp 2.02.2014].

Rushe D., Ball J. (2013), *PRISM scandal: tech giants flatly deny allowing NSA direct access to servers*, The Guardian, 7-06-2013, http://www.theguardian.com/world/2013/jun/07/prism-tech-giants-shock-nsa-data-mining [dostęp 22.12.2013].

Stamping out Falsified Medicines, http://www.efpia.eu/topics/industry-economy/falsified-medicines [dostęp 30.01.2014].

Vermesan O., Friess P. (ed.) (2013), *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River Publishers, Aalborg.

INTERNET OF THINGS: OPPORTUNITIES AND THREATS

Summary

It is considered that the Internet of things was born in the year 2008/2009, when the number of devices connected to the Internet exceeded the number of inhabitants of the Earth. The aim of the study is to present the opportunities and benefits that can be obtained as a result of the implementation of the concept of the Internet of Things, as well as potential threats and challenges that are associated with it.

Keywords: Internet of things, IoT, smart objects.

Translated by Andrzej Kobyliński