DOI: 10.52694/ThPSR.121.5

Małgorzata Such-Pyrgiel
Edyta Rosińska-Wielec

Zachowanie bezpieczeństwa społeczeństwa cyfrowego na przykładzie projektu IoT przedsiębiorstwa Lingaro[1]

The security of the digital society on the example of the Lingaro IoT project

Rewolucja cyfrowa przyniosła wiele innowacyjnych rozwiązań, tworząc nową rzeczywistość, w której społeczeństwo, świat biznesu i regulator muszą się odnaleźć. Nowa technologia to nie tylko łatwiejsze życie, ale też zagrożenia, jakie niesie dla praw człowieka i jego wolności. Zgodnie z prawem Hypponena, czym bardziej skomplikowany system, tym bardziej narażony na dysfunkcyjność. Co należy zrobić, aby ustrzec się przed tym? – to pytanie, które coraz częściej pojawia się zarówno w dyskursie powszechnym, jak i naukowym. Próbę udzielenia odpowiedzi na nie podejmują nie tylko socjologowie, prawnicy, ludzie biznesu, ale także sami twórcy nowych cyfrowych technologii. Internet rzeczy to najszybciej rozwijająca się technologia sektora IT. Daje możliwości komunikacji, jakie do tej pory dedykowane były tylko ludziom. Przesyłające sobie sygnały urządzenia zaczynają tworzyć nowe ekosystemy, które niekontrolowane mogą stanowić zagrożenie dla bezpieczeństwa systemu, jak i samego człowieka. Celem artykułu jest pokazanie na przykładzie projektu przedsiębiorstwa z branży IT skomplikowanego procesu tworzenia projektu IoT w sposób uniemożliwiający powstanie w przyszłości zagrożeń.

[1] Niniejszy artykuł jest prezentacją podjętych badań na potrzeby projektu IoT realizowanego przez przedsiębiorstwo Lingaro Sp. z o.o., który był realizowany w ramach badania z dofinansowania Unii Europejskiej ze środków RPO Województwa Mazowieckiego o numerze RPMA 01.02.00-14-9403/17 pod nazwą Platforma Internetu Rzeczy – LINGARO IoT Cloud Platform. Jego celem było przygotowanie prototypu platformy do zarządzania i analizy IoT. Przedmiot projektu obejmował badania i prace rozwojowe w obszarze informatyki.

Wypracowanie generalnych reguł zapewniających bezpieczeństwo cyfrowe wydaje się być kluczowe dla dalszej ekspansji internetu wszechrzeczy.

Słowa kluczowe: internet rzeczy, rewolucja cyfrowa, cyfrowa transformacja, prawo Hypponena, bezpieczeństwo cyfrowe

The digital revolution has brought many innovative solutions, creating a new reality, where the society, the business world and the state regulator must find their way. The new technology does not only mean an easier life, but there is also the threats as it brings to human rights and freedoms. According to Hypponen's law, the more complex a system is, the more vulnerable it is to dysfunctionality. What should be done to guard against them? – is a question that is increasingly being asked in both popular and academic discourse. The attempt to answer this question is being made not only by academics, politics, lawyers or business people, but also by the developers of new digital technologies themselves. The Internet of Things is the fastest growing technology in the IT sector. It offers possibilities for communication that until now were dedicated only to people. The devices transmitting signals to each other are beginning to create new ecosystems, which, if uncontrolled, can pose a threat to the security of both the system and humans themselves. The aim of this article is to show, on the example of a project of an IT company, the complex process of creating an IoT project in a way that prevents the emergence of threats at the stage of its implementation. The development of general rules to ensure the digital security seems to be crucial for the further expansion of the Internet of All Things.

Key words: Internet of Things, IoT, digital revolution, digital transformation, Hypponen's law, cybersecurity

Wprowadzenie

Cyfrowa rewolucja to współczesne zjawisko intensywnie wpływające na globalną cywilizację, czyniące z niej społeczeństwo postinformacyjne, sieciowe, ucyfrowione czy 4.0. Zagadnienie to dotyka licznych dyscyplin naukowych i jest analizowane w aspektach społecznych, gospodarczych,

ekonomicznych czy kulturowych. Tendencje do zwiększenia wykorzystania technologii cyfrowych coraz silniej oddziałują zarówno na specyfikę funkcjonowania różnego rodzaju organizacji, jak i jakość życia konsumentów, a ich finalny kształt jest trudny do opisania nawet przez futurologów.

W literaturze przedmiotu odnajdujemy problemy badawcze wskazujące na pozytywne zmiany, jakie za sobą niesie, oraz zagrożenia, jakie może wywoływać. Technologie oparte na zapisie cyfrowym otworzyły przed człowiekiem ogrom niespotykanych dotąd możliwości. Do języka powszechnego niemalże przeszły takie terminy jak cyfrowa transformacja, sztuczna inteligencja, Big Data, druk 3D, zapis w chmurze, inteligentny dom czy nawet boty. Ta szybka transformacja technologiczna wymusza wiele zmian w działaniach producentów, zachowaniach konsumentów i prawodawstwie. Coraz trudniej pojedynczej osobie ukryć swoje zainteresowania, zwyczaje, preferencje, nawyki czy możliwości. Zbierane przez wiele systemów dane pozwalają opisać nasze życie często lepiej niż mogą to zrobić znajome nam osoby. Generuje to wiele zagrożeń z zakresu praw człowieka, ale także prowadzi do możliwości niekontrolowanego paraliżu naszego życia poprzez blokady systemów technologicznych.

Rewolucja cyfrowa i rozwiązania IoT spowodowały, że wielu z dotychczasowych producentów, np. artykułów gospodarstwa, stało się przedsiębiorstwami IT zbierającymi dane o zwyczajach swoich konsumentów. Wbudowane w urządzenie nowe funkcje IoT pozwalają na zbieranie informacji, np. ile filiżanek i jakiej kawy dziennie pije się w danym gospodarstwie domowym, jak często i w jakich godzinach odbywa się tam pranie, co i ile zamawiają domownicy do lodówki, nie wspominając już o rozeznaniu w konsumpcji treści audio i audiowizualnych.

IoT to nowe pole ochrony danych, których szczegółowość i mnogość źródeł pochodzenia daje możliwość identyfikacji osób, ich zachowań i potrzeb, a także infekowanie setek tysięcy urządzeń. Rodzi to wiele problemów związanych w prywatnością i bezpieczeństwem, co wraz z ogromem zebranych informacji (BigData) jest istotną przeszkodą do trwałego technologicznego i prawnego zapanowania nad tym systemem. IoT to system bardzo złożony, a tym samym narażony na błędy i generujący zagrożenia. Duża liczba czynników oddziaływujących na siebie wzajemnie czyni układ trudno kontrolowalnym. Ta delikatność systemu IoT jest potwierdzeniem prawa Hypponena *Smart means vulnerable*, mówiącym, że zawsze, gdy urządzenie jest opisywane jako „inteligentne",

jest ono podatne na ataki[2]. Badacz, wykładowca i aktywny popularyzator technologii cyfrowych zwraca uwagę na rolę, jaką odgrywają w procesie tworzenia zabezpieczeń zarówno producenci, jak i konsumenci. Kluczowe jest tu stosowanie inżynierii bezpieczeństwa zarówno na poziomie projektowania, jak i użytkowania. Równolegle do niej powinna rozwijać się regulacja prawna dotycząca komunikacji M2M (*Machine to Machine*).

Artykuł ukazuje przykład realizowania projektu IoT przez polskie przedsiębiorstwo branży IT i ma na celu zwrócenie uwagi na konieczność wypracowania reguł, jakimi powinni kierować się wszyscy twórcy projektów IoT. Brak doświadczenia w tym zakresie przedsiębiorstw produkcyjnych, które niejako przez przypadek technologiczny stały się twórcami oprogramowania, jest powodem wielu zagrożeń wynikających z przeoczenia zastosowania koniecznych zabezpieczeń systemu.

Internet of Things (IoT)

Dotychczasowe formy komunikacji międzyludzkiej są wypierane przez wirtualny przekaz informacji. Rozmawiają ze sobą zdalnie już nie tylko istoty ludzkie, ale w procesie tym uczestniczą także urządzenia, przesyłając sobie strumienie danych, a w wyniku ich interakcji pojawia się, określone wcześniej przez twórcę tego rodzaju komunikacji, konkretne działanie. Zjawisko to jako pierwszy zdefiniował i nazwał Kevina Ashtona w 1999 r. Internetem rzeczy (z ang. *Internet of Things,* dalej: IoT) w uproszczeniu określa on ekosystem, w którym wyposażone w sensory przedmioty komunikują się z komputerami[3].

Definicja w dokumencie standaryzującym wymagania wobec IoT w krajach UE określa IoT jako dynamiczną globalną infrastrukturę sieciową z samokonfigurujacymi się możliwościami, opartą na standardowych i interoperacyjnych protokołach komunikacyjnych, gdzie fizyczne i wirtualne „rzeczy" mają tożsamość, cechy fizyczne i wirtualną osobowość oraz używają inteligentnych interfejsów i są płynnie zintegrowane w ramach

[2] M. Hypponen, L. Nyman, *The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation* [w:] *Technology Innovation Management Review*, 2017 Vol. 7, Issue 4, s. 5. Hypponen-Nyman_TIMReview_April2017.pdf.

[3] K. Ashton, *That 'Internet of Things' Thing*, June 22, 2009. RFIDjournal-That Internet of Things Thing.pdf (itrco.jp).

sieci informacyjnej[4]. Część z badaczy uważa jednak, że do prawdziwych „narodzin" tego pojęcia doszło około 2008 r., kiedy to, według firmy Cisco, liczba urządzeń podłączonych do sieci przekroczyła liczbę żywych użytkowników[5]. W roku obecnym liczba ta to ponad 15 miliardów, a jej wielkość ma podwoić się do 2030 r.[6]. W 2021 r. wartość światowego rynku IoT przekroczyła 300 mld USD. Szacunki na 2026 r. mówią o wielkości przeszło dwa razy większej, tj. o 650 mld USD[7], a w 2032 r. wartość ta ma urosnąć nawet do 1,562 mld USD[8].

Obecnie liczba komunikujących się ze sobą w opisywanym systemie urządzeń jest o wiele większa niż łączna liczba połączonych komputerów i smartfonów używanych do komunikacji przez ludzi. Zakres zastosowania IoT ogromnie się poszerza, obejmując nie tylko duże systemy obronne i środowiskowe, inteligentne miasta i budynki, ale także zarządzanie gospodarstwem domowym, czy ułatwiając konsumpcję różnych dóbr. Liczba zalet tej technologii wzrasta wraz z połączeniem jej z zaawansowaną analityką i sztuczną inteligencją. Z tego też powodu coraz częściej mówi się o internecie wszechrzeczy, a ekosystem, jaki go tworzy, inteligentnym otoczeniem.

Silna tendencja wzrostowa jest odnotowywana także na rynku polskim. Liczba wszystkich urządzeń podłączonych do sieci w ciągu kilku ostatnich lat podwoiła się. Szacunki wskazują, że w obecnym roku jest to 261 milionów, co oznacza, że na jednego mieszkańca Polski przypada 7 podłączonych do sieci urządzeń. Za pięć lat wskaźniki te mają się co najmniej podwoić[9]. Niemniej jednak badania wśród Polaków nad znajomością pojęcia IoT pokazują, że jest ona niskim poziomie[10]. Zagadnienie to rozpoznaje

---

[4] IERC (2015) *Internet of Things. Position Paper on Standarization for IoT technologies*, European Research Cluster on the Internet of Things, January/2015, s. 13.

[5] M. Sikorski, A. Roman (red.), *Internet rzeczy* [w:] Real IT World, nr 1/2020, PWN, s.91–94.

[6] Exploding Topics (2023) *Number of IoT Devices*, Number of IoT Devices (2023–2030) (explodingtopics.com).

[7] *IoT Market by Component (hardware, Software Solutions and Services), Organization Size, Focus Area (Smart Manufacturing, Smart Energy and Utilities, and Smart Retail) and Region – Global Forecats to 2026.* (2022) Feb 2022, by marketsandmarkets.com, Internet of Things (IoT) Market Size, Statistics, Trends, Forecast, Industry Report -2030 (marketsandmarkets.com).

[8] Precedence Research (2022) *Industrial IoT Market (By Component: Solution, Services, Platform; By End-Use: Manufacturing, Energy & Power, Oil & Gas, Healthcare, ogistics & Transport, Agriculture, Others) – Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2023-2032*, Industrial IoT Market Size To Surpass USD 1,562.35 Bn By 2032 (precedenceresearch.com).

[9] M. Marszycki, *Internet Rzeczy jednym z najszybciej rozwijających się obszarów polskiego rynku IT*, 14 kwietnia 2023, itwiz.pl, Internet Rzeczy jednym z najszybciej rozwijających się obszarów polskiego rynku IT | ITwiz.

[10] *Analiza funkcjonowania rynku usług telekomunikacyjnych w Polsce oraz ocena preferencji konsumentów. 2022 rok. Badanie klientów indywidualnych.* (15.11.2022) IBC Advisory S.A. Sektor Publiczny, s. 62–63.

jedynie 16% społeczeństwa, ale konkretne zastosowania są już niemal powszechnie znane. Prawie 82% badanych rozpoznawało zastosowania IoT w inteligentnych domach, prawie 80% w inteligentnych miastach, a 76% w monitorowaniu środowiska, jak np. pomiar temperatury wiatru, poziomu rzek itp. Bardzo podobny procent respondentów uznał je także za pożyteczne. Podobnie oceniano przydatność inteligentnych sieci zdrowia, inteligentne przedsiębiorstwa i przemysł, inteligentne systemy energetyczne czy inteligentne systemy pomiarowe. Wszystko wskazuje na to, że IoT jako najszybciej rozwijający się sektor rynku IT będzie jednym z kluczowych kół zamachowych światowej gospodarki przyszłości.

Zagrożenia to luki w systemie bezpieczeństwa

Celem stworzenia bezpiecznego systemu IoT jest uniknięcie luk, które pozwalałyby na stworzenie połączeń pomiędzy siecią prywatną a publiczną, pozwalając na dostęp do prywatnych danych, w tym haseł osobom z zewnątrz ekosystemu lub dających możliwość do połączeń z innymi urządzeniami podłączonymi do sieci mogące powodować paraliż sieci lokalnej, a nawet wyjść poza nią. Istotne jest zatem, aby każde przedsiębiorstwo biorące udział w tworzeniu oprogramowania do IoT korzystało z wypracowanych już przez innych reguł inżynierii bezpieczeństwa. Koniecznym jest zatrudnianie wysoko wykwalifikowanych w tym zakresie pracowników i inwestowanie w ich ciągły rozwój.

W państwach UE od maja 2018 r. obowiązuje ogólne rozporządzenie o ochronie danych[11] (Rozporządzenie PE i Rady), które wzmacnia ochronę danych osób fizycznych społeczeństw tych krajów. Dokument ten wyznacza obowiązki i odpowiedzialność producentów w tym zakresie, przewidując wysokie sankcje za ich niedotrzymanie. Jednym z kluczowych problemów w IoT jest uwierzytelnianie, czyli ustanowenie mechanizmu potwierdzającego zaufanie do tożsamości rzeczy podłączonej do sieci (np. urządzenia, aplikacji, usługi w chmurze) i próbującej wchodzić w interakcję z innymi podobnymi obiektami. Ponadto sprawne działanie IoT musi uwzględniać potencjalne ograniczenia zasobów IoT, ograniczenia

[11] *Rozporządzenie Parlamentu Europejskiego i Rady* (UE) 206/679 z dn. 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Rozporządzenie 2016/679 (RODO) i akty towarzyszące – UODO.

w przepustowości sieci, a także charakter podejmowanych przez urządzenia interakcji.

Obok problemów technicznych, których konieczność rozwiązania leży po stronie producentów, istnieją bariery wynikające z czynników ludzkich. Świadomość społeczna na temat negatywnych efektów, jakie może przynieść korzystanie z urządzeń podłączonych do IoT, jest ciągle bardzo mała. Konsumentom trudno wyobrazić sobie nawet dla jakiego celu mogą być wykorzystane cyfrowe ślady jakie zostawiają w IoT. Tym bardziej trudno odnaleźć u nich wiedzę i chęć poszukiwania zabezpieczeń przed tego typu inwigilacją.

Cel i pytania badawcze

Niniejszy artykuł jest próbą zdiagnozowania przyczyn występowania luk w bezpieczeństwie systemów IoT oraz próbą znalezienia rozwiązania dla producentów reguł określających, jakie zachowania należałoby podjąć w procesie tworzenia podobnych projektów[12]. Celem działania było wdrożenie na rynek nowego, innowacyjnego w skali globalnej produktu o nazwie Lingaro Cloud IoT Platform. Cel badań koncentrował się wokół następujących pytań badawczych:

- Czy i jak można zabezpieczyć interes społeczny w projektach IoT oraz czy mogą one wspierać rozwój społeczeństwa cyfrowego w bezpieczny sposób?
- Czy i jak można zrealizować projekt w oparciu o istniejące dane, aby mógł w pełni zabezpieczyć ochronę danych w systemach IoT?

Chociaż samo rozwiązanie IoT jest coraz bardziej obecne w naszym życiu, to polskie publikacje naukowe temu poświęcone nie świadczą o dużym zainteresowaniu tym zagadnieniem badawczym. O ile społeczne konsekwencje cyfryzacji są częstym przedmiotem dyskursu socjologicznego, to o zagrożeniach technologicznych najwięcej treści odnajdujemy w publikacjach nienaukowych, redagowanych przez przedsiębiorstwa branży IT. O zmianie zachowań użytkowników technologii cyfrowych,

[12] Za przykład takiego rozwiązania posłużył projekt przedsiębiorstwa Lingaro Sp. z o.o. realizowany w ramach projektu „RPMA .01.02.00-14-9403/17 „Platforma Internetu Rzeczy – LINGARO IoT Cloud Platform" współfinansowanego przez Unię Europejską ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014–2020 Oś Priorytetowa RPO WM I Wykorzystanie działalności badawczo-rozwojowej w gospodarce Działanie w ramach Osi Priorytetowej RPO WM 2014–2020 1.2 Działalność badawczo-rozwojowa przedsiębiorstw".

jej wpływu na budowanie nowych modeli społecznych i kulturowych oraz niepokoju z tego wynikającego od wielu lat pisze polska socjolog Magdalena Szpunar[13]. O nowych technologiach i cyfrowej transformacji w nurcie socjologicznym, ekonomicznym i humanizmu cyfrowego pisze także druga polska socjolog Małgorzata Such-Pyrgiel[14]. W kwestii zagrożeń technologicznych, jakie niesie za sobą dynamiczny rozwój IoT, pojawiło się kilka prac naukowych. Ireneusz Maj[15] wyodrębnia luki, które są najbardziej podatne na rozszczelnienie bezpieczeństwa. Zauważał także, że problemy IoT o charakterze społecznym to nie tylko zagrożenie wolności i prywatności, ale także bezrobocie. Rot i Blaicke[16] zwracają uwagę na zagrożenia wynikające z zastosowania IoT w zarządzaniu infrastrukturą miasta, domu, czy w handlu i usługach. Podają przykłady ataków i sposoby ochrony przed nimi. Podkreślają, że istnieje niewiele wyspecjalizowanych rozwiązań potrafiących dać odpór wszelkim atakom hackerskim na IoT. Puślecki zwraca uwagę, że nowe technologie stwarzają narzędzia do inwigilacji społeczeństwa, z drugiej strony dają impuls do zmian w zakresie zbierania danych do badań naukowych. Przywołuje przypadek pandemii Covid-19, która miała kluczowe znaczenie dla

[13] Zob. M. Szpunar (red.), *Paradoksy internetu. Konteksty społeczno-kulturowe*, Toruń 2011, Wyd. Adam Marszałek; M. Szpunar, *Imperializm kulturowy internetu*, Kraków 2017, IDMiKS UJ; M. Szpunar, *Kultura algorytmów*, Kraków 2019, IDMIKS UJ; M. Szpunar, *Pomiędzy antropomorfizacją maszyn a technomorfizacją człowieka* [w:] Journal of Modern Science, 2023 nr 3, s. 24–38.

[14] Zob. M. Such-Pyrgiel, A. Gołębiowska, D. Prokopowicz, *The role of Big Data and Data Science in the context of information security and cybersecurity*, Journal of Modern Science 4/2023 vol. 53, ss. 9–42, ISSN 17342031; zob. A. Gołębiowska, M. Such-Pyrgiel, D. Prokopowicz, *The postpandemic reality and the security of information technologies ICT, Big Data, Industry 4.0, social media portals and the Internet*, 2022, Journal of Modern Science 42/2022 vol. 49, ss. 10–43, ISSN 17342031; zob. M. Such-Pyrgiel, *Nowe technologie edukacyjne w dobie cyfrowej transformacji – wybrane konteksty* [w:] Bezpieczeństwo w dobie cyfrowej transformacji – aspekty prawne, organizacyjne i społeczne, Wydawnictwo SGSP 2021; zob. M. Such-Pyrgiel, A. Gołębiowska, *Socio-economic and legal dimensions of digital transformation. Selected contexts,* Wydawnictwo SGSP 2021; zob. M. Such-Pyrgiel, *Fourth industrial revolution, new communication technologies and the human right to good administration* [in:] Crisis as a challange for human rught, Bratysława, 2020, s. 447–462; zob. M.Such-Pyrgiel, *Człowiek w dobie cyfrowej transformacji. Studium socjologiczne*, Toruń, Wydawnictwo Adam Marszałek 2019; zob. M. Such-Pyrgiel, *Nowe modele biznesu w dobie transformacji cyfrowej* [w:] M. Sitek, M. Such-Pyrgiel (red.), *Społeczne i ekonomiczne aspekty zarządzania w organizacjach przyszłości*, Wyd. WSGE, Józefów 2018, s. 39–56.

[15] I. Maj, *Internet rzeczy i zagrożenia z nim związane* [w:] Bezpieczeństwo, Teoria i praktyka, 2015 nr 3.

[16] Zob. A. Rot, B. Blaicke, *Bezpieczeństwo internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych* [w:] *Zeszyty Naukowe Politechniki Częstochowskiej, Zarządzanie*, 2017 Nr 26, s. 188–198; por. A. Rot, B. Blaicke, *Zagrożenia wynikające z implementacji koncepcji internetu rzeczy w wybranych obszarach zastosowań*, w: *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, 2017 Nr 341.

szerokiego zastosowania nowoczesnych technologii, w tym IoT w zarządzaniu procesami przemysłowymi[17].

Jedną z pierwszych polskojęzycznych książek o tej tematyce było opracowanie pod redakcją naukową Marcina Sikorskiego i Adama Romana w 2020 r. Książka przybliża nie tylko samo techniczne rozwiązanie IoT, ale również wskazuje na trudności wynikające z wdrożenia spójnych rozwiązań regulujących ten rynek w celu zwiększenia bezpieczeństwa jego użytkowników[18]. Inną obszerną i zwartą publikacją, jaka pojawiła się na polskim rynku wydawniczym, był przedruk książki z 2015 roku Michela Millera uznanego amerykańskiego propagatora nowości technologicznych[19]. Za jedną z najważniejszych pozycji opisującej IoT, która ukazała się także w polskim przekładzie, jest bardzo gruntownie napisana praca pod redakcją naukową egipskiego uczonego Qusay F. Hassana[20]. W badaniach nad rozwojem IoT zwraca on uwagę na cyberbezpieczeństwo, kwestie regulacyjne oraz włączenie w system przemysłu cyfrowego gospodarek wschodzących jako główne determinanty przyszłości tej technologii. Na polskie tłumaczenie czeka praca Sean'a Smith, w której autor zachęca do stosowania rozwiązań pozwalających uniknąć błędów przy rozbudowie IoT, jakich ciężko doświadczyliśmy, rozwijając internet w ogóle, a w szczególności z zakresie przechowywania pamięci, kodowania, uwierzytelniania czy kryptografii[21]. Temat bezpieczeństwa wynikający z zastosowania IoT jest opisany w anglojęzycznych publikacjach naukowych także za sprawą m.in. Abomhara, Køien (2015), Patton, Gross, Chinn, Forbis, Walker, Chen (2014). Pisali o tym także w prasie popularnej (np. Franceschi-Biccierai, 2016; Greenberg & Zetter, 2015; Schneier, 2014).

Podstawowym źródłem wiedzy o przykładowym projekcie IoT był *Raport z realizacji badań w ramach Zadań numer 2 i 4. Dobór i optymalizacja narzędzi, algorytmów, IoT Hub urządzeń i rozwiązań do zbierania i przetwarzania danych."* przygotowany przez pracowników Lingaro Sp. z o.o. przeprowadzających badania.

---

[17] W.Z. Puślecki, *Sztuczna inteligencja (AI), Internet Rzeczy (IoT) i sieć piętej generacji (5G) w nowoczesnych badaniach naukowych* [w:] *Człowiek i społeczeństwo*, 2021 T. LII. bmrowicka,+{$userGroup},+06-Puslecki.pdf.

[18] M. Sikorski, A. Roman (red.), *Internet rzeczy*, w: Real IT World, nr 1/2020, PWN.

[19] M. Miller, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat.* Warszawa 2016, PWN.

[20] F.Q. Hassan, *Internet of Things A to Z: Technologies and applications*, Wiley-IEE Press 2018.

[21] S. Smith, *The Internet of Riski Things. Trusting the Devices That Surround US*. O'Reilly Media, Inc., Sebastopol 2017.

Krótka charakterystyka projektu Lingaro

Celem projektu Lingaro było opracowanie m.in. prototypu wysoce innowacyjnego oprogramowania platformy do zarządzania urządzeniami działającymi w oparciu o paradygmat chmury IoT (Cloud IoT/CoT) będący połączeniem paradygmatów obliczeń w chmurze (Cloud Computing) i IoT. Takie zestawienie umożliwia zbieranie ogromnej ilości danych z szerokiego zakresu urządzeń i systemów, dalsze ich przetwarzanie i analizowanie w zakresie osiągania celów danego systemu IoT. Rozwiązanie to jest dedykowane do wykorzystania zarówno w obszarze procesów produkcyjnych i usługowych w przedsiębiorstwach, jak i do użycia przez indywidualnych konsumenckich. Obok niewątpliwych walorów, jakimi są zwiększenie wydajności, poprawa jakości czy zapewnienie oszczędności w zakładach przemysłowych, platforma może także dbać o bezpieczeństwo budynków, w tym prywatnych domów.

Rozumienie i możliwości smart budownictwa dynamicznie zwiększają monitorowane obszary. O poprawną eksploatację i bezpieczeństwo dba już nie tylko system zarządzania temperaturą czy światłem, ale także kontroling jakości powietrza, monitoring ruchu, technologia produkcji i magazynowania energii odnawialnej, układ kontroli dostępu itp. Dodatkową atrakcją tych rozwiązań jest zastosowanie technologii samouczących się urządzeń poprzez zapamiętywanie preferencji ustawień kolejnych cykli.

Przygotowanie tego projektu wymagało nie tylko znawstwa potrzeb przemysłowych czy społecznych, ale także wnikliwego rozeznania w kwestiach technologicznych pozwalających na wdrażanie innowacyjnych rozwiązań. Wiedzy z tego zakresu należy szukać nie tylko w wydawnictwach naukowych, ale także w publikacjach popularnych. Opisywany w artykule projekt Lingaro bazował m.in. na pracy przedstawiającej koncepcję integracji obliczeń chmurowych z IoT, a tym samym określającej nowy paradygmat Chmury Internetu Rzeczy (ang. *Cloud IoT*) obejmujący zupełnie nowe zastosowania, wyzwania i kwestie badawcze[22]. Posiłkowano się także wynikami analizy dotyczącej zaangażowania w technologię mgły obliczeniowej w projektowaniu infrastruktury *Cloud of Things* (dalej: CoI). Celem tej pracy było opracowanie matematycznego modelu trójwarstwowego czujnika CoT dla oceny zastosowania warstwy

[22] A. Botta, W. de Donato, V. Persico, A. Pescapé, *Integration of Cloud computing and Internet of Things: A survey*, 2015.

przeciwmgielnej w kontekście systemu oraz wykazanie, że jest to kluczowy czynnik spełniający wymagania aplikacji ograniczonych czasowo[23]. Inną kluczową analizą była praca dotycząca integracji platform chmurowych, infrastruktury chmurowej oraz oprogramowania IoT. Omawiała ona możliwość integracji i techniki analizy danych możliwych do zastosowania w takich systemach[24].

Obok tych kluczowych prac i szeregu innych naukowych opracowań, twórcy posiłkowali się wiedzą zgromadzoną na wielu anglojęzycznych portalach internetowych, zarówno tych publikujących przykłady nowych zastosowań IoT, jak i tych udostępniających raporty opisujące ten rynek. Te najwięcej wnoszące to prowadzone pod nazwą m.in. Stacey on IoT. com, Altop, TechCrunch, IoT One czy Venture Beat. Ponadto dla wszystkich zainteresowanych budowaniem infrastruktury koniecznym jest stałe obserwowanie stron wiodących producentów tejże technologii, nie tylko takich gigantów jak Amazon, Apple, Cisco, Google, IBM czy Microsoft, ale także podobnie kluczowych jak np. BSQuare, Bluetooth Special Interest Group, Cloudera Enterprise, Enterprise Hadoop, Treasure Data czy Wi-Fi Alliance.

Zakres prac w projekcie Lingaro

Założone w projekcie wymagane cechy platformy IoT to prosta architektura jej centralnych komponentów, a w niej niemalże nieograniczona skalowalność, agnostyczność chmurowa i łatwość implementacji. Przygotowanie docelowej architektury rozwiązania wymagało zatem przygotowania i przeprowadzenia szeregu badań. Obejmowały one zagadnienia skalowalności infrastruktury, stałego dostępu do niegraniczonych zasobów obliczeniowych i nośników danych oraz fizycznej defragmentacji elementów systemu.

Badaniu podlegały także bazy danych zarówno relacyjne, przedstawiające dane w postaci tabel oraz bazy NoSQL tzw. obiektowe zapisane w formie dokumentów. Kluczowymi kryteriami ich wyboru były dostępność, uaktualnianie, backup, szyfrowanie, skalowanie, przechowywanie,

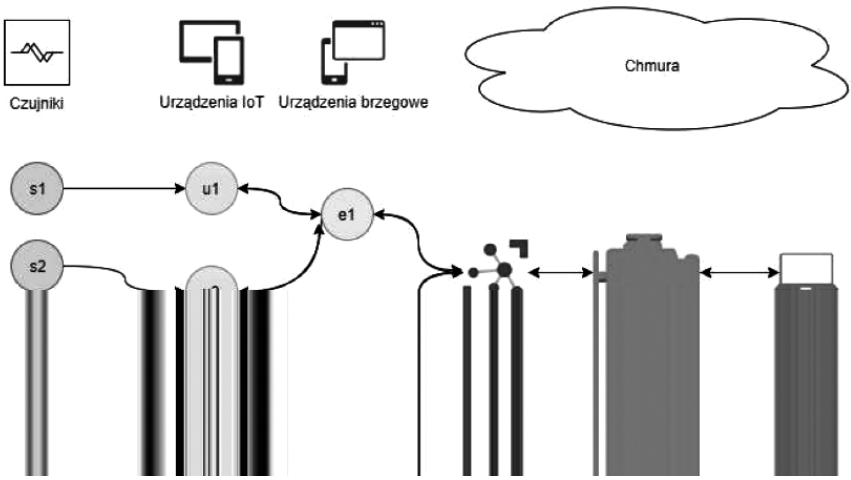
[23] W. Li, I. Santos, F.C. Delicato, Paulo F. Pires, L. Pirmez, W. Weic, H. Song, A. Zomaya, S. Khan, *System modelling and performance evaluation of a three-tier Cloud of Things*, 2016.

[24] M. Díaz, C. Martín, B. Rubio, *State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing*, 2016.

georeplikacja, okres zapytania, migracja danych, zarządzanie użytkownikami i bezpieczeństwo na poziomie wiersza, integracja z narzędziami do raportowania i wizualizacji, wdrożenie oraz wsparcie i zamrażanie.

W projekcie dokonano analizy architektury danych w oparciu o teorię grafów standardowo używaną do modelowania relacji między ludźmi i sieciami społecznymi. Niniejszy rysunek jest wizualizacją takiej relacyjności rozwiązań IoT.

Rysunek 1: Relacyjność urządzeń w rozwiązaniu systemowym IoT.



Źródło: Opracowanie własne na podstawie badań.

Ważna była także kwestia implementacji u różnych dostawców infrastruktury. W celu wyboru optymalnego rozwiązania przeprowadzono test poprzez wygenerowanie obciążenia symulowanego przez 10 000 urządzeń. Każde z nich wysyłało wiadomości bez żadnych dodatkowych opóźnień, tak szybko jak to możliwe. W sumie dało to 10 000 000 wiadomości. Każda z nich miała około 270 bajtów. Wykorzystana baza danych MongoDB była skonfigurowana w postaci 4 mongos i 2 replicasetów. Testy zostały przeprowadzone na maszynie wirtualnej klasy D4s v3, 4 procesory wirtualne, 16 GB RAM. W ten sposób przetestowano zapisywanie wiadomości do bazy danych i procesowanie wiadomości. Osobno przeprowadzono badania w zakresie przesyłania komunikatów pomiędzy urządzeniami a platformą chmurową celem ustandaryzowania treści i specyfikowania pól dla każdej wiadomości jak np. typ, wersja, data wysłania itp.

Celem określenia sposobu składowania danych w archiwum w systemie plików HDFS zapisano 20 000 wiadomości na sekundę, o rozmiarze 1 KB. Dokonano tym samym analizy skutecznego grupowania danych w większych pakietach dla danego interwału czasowego oraz dla logicznego klucza, minimalizując dzięki temu koszt zapisu do absolutnego minimum. Z racji tego, że urządzenia działające w systemie IoT badają otoczenie w czasie rzeczywistym, natychmiastowo reagując na zebrane dane, to istotne jest wykorzystanie przetwarzania strumieniowego dla danych odbieranych z urządzenia. Do tego celu użyto jednego z najpopularniejszych narzędzi framework Spark z rozszerzeniem Spark Streaming umożliwiającego działanie w platformach kluczowych jakimi są: AWS (usługa Amazon EMR), Azure (usługa Azure HDInsight) oraz Google Cloud Platform (usługa Dataproc).

W ramach projektu dokonano także badań w zakresie analizy dużej ilości danych zgromadzonych na platformie, a pochodzących z różnych źródeł. Do tego celu wytypowano silnik DataBricks oferowany w modelu PaaS (P*latform as a Service*) umożliwiającym analizowanie i przetwarzanie danych technikami BigData oraz z wykorzystaniem klastrów opartych o GPU. Jedną z wyróżniających się danych jest informacja o zdarzeniu, które wymaga szybkiej reakcji. Z ogromu ilości wpływających danych należy zatem wyłuszczyć te najbardziej alarmujące. Do tego celu przygotowano szereg kryteriów filtrowania zdarzeń pozwalających na osiągnięcie elastycznych reguł określania alertu, m.in. nazwa sensora monitorującego wybraną grupę zdarzeń czy zakres dozwolonej temperatury. Kolejnym krokiem było zdefiniowanie różnych rodzajów powiadomień dla określonych zdarzeń. Za najpraktyczniejszą wersje dostarczenia takiej wiadomości uznano formę tekstową w postaci SMS, gdyż telefon jest urządzeniem, z którym człowiek pozostaje najdłużej w ciągu dnia w stałym kontakcie.

W ramach projektu wykonano także badania w zakresie sprzętu. Próba konfiguracji urządzeń została wykorzystana na dwa sposoby. W pierwszym rozwiązaniu urządzenia pomiarowe zostały podłączone do płytek deweloperskich ESP-32S WROOM, które dane zebrane z czujników przekazują do urządzenia brzegowego Raspberry Pi 3B. Ono z kolei komunikuje się z wybraną na potrzeby badań usługą systemu chmurowego Azure IoT Hub w celu przesłania zebranych danych do dalszej obróbki, a także w celu konfiguracji i wydania poleceń do wykonania. W drugim przypadku urządzenia pomiarowe zostały bezpośrednio spięte z usługą Azure IoT.

Analizie poddane zostały także takie zagadnienia jak synchronizacja oprogramowań układowych dla urządzeń brzegowych, takich jak np. kamery, czujniki i urządzenia rejestrujące z innymi elementami systemu, w tym i platformami chmurowymi. Wytypowano cztery możliwe sposoby komunikacji z kamerami rejestrującymi wszelkie zdarzenia w środowisku oraz ustalono sposób rejestracji i konfiguracji nowych urządzeń. Analizie podlegał także dobór sensorów, jak czujniki ultradźwiękowe, jakości powietrza czy smogu wedle wcześniej opracowanych przez zespół kryteriów, czujników ultradźwiękowych.

Zasadniczym elementem badań było sprawdzenie bezpieczeństwa platformy, a głównie danych, jakie są pozyskiwane w ramach jej funkcjonowania. Celem uniknięcia konieczności przesyłania kluczy poprzez sieć założono, że komunikacja z Azure IoT odbywać się będzie za pomocą tokenów bezpieczeństwa, których działanie jest ograniczone czasowo i zakresowo, a ich generowanie odbywa się automatycznie i nie wymaga specjalnej konfiguracji. Innym elementem zapewnienia bezpieczeństwa było sprawdzenie możliwości integracji zewnętrznych zapór sieciowych, tzw. firewall. Ponadto przeprowadzono badania w zakresie OPC-DA (OPC Data Access), czyli protokołu z grupy standardów OPC, zawierającego specyfikę dostępu generowanych danych w czasie rzeczywistym w sposób synchroniczny lub asynchroniczny w sterownikach urządzeń przemysłowych.

Narzędzia raportowe to kolejny element projektu, który wymagał opracowania. To część, z punktu widzenia użytkownika, najbardziej wyróżniająca produkt. Wybrane narzędzie Grafana do wizualizacji danych telemetrycznych w czasie zbliżonym do rzeczywistego umożliwia raportowanie z wielu różnych baz.

Innym filarem badań były testy w zakresie Machine Learning, które pozwoliły na określenie warunków, w jakich system najsprawniej sam modyfikowałby wprowadzone algorytmy w oparciu o doświadczenie. Założono, że pomieszczenie powinno być wyposażone w ultradźwiękowe czujniki odległości i pozbawione jakichkolwiek źródeł mogących generować zakłócenia. Do modelu wprowadzono zmienne typu objętość pomieszczenia, lokalizacje obiektów w nim się znajdujących czy rozpoznawanie obecności człowieka. Finalnie wybrano model regresji logistycznej pomagającej w nauczaniu zachowania dostarczonej zmiennej wejściowej i zapewniający prognozy w postaci zajętości/nie zajętości pomieszczenia.

Przeprowadzono także badania w zakresie aplikacji webowych, które za pomocą sieci internetowej pozwalałyby użytkownikom na podjęcie określonych działań w zakresie działania platformy. Ich krytycznym elementem był wybór zastosowania bibliotek komponentów składowych interfejsów.

Nie bez znaczenia dla projektu były analizy dotyczące procesu wytwarzania oprogramowania pozwalające na usprawnienie zarządzania nim. Przeprowadzono na tym polu weryfikacje dostępnych na rynku narzędzi i wybrano Azure Devops z możliwością skalowania w miarę rozwoju projektu oraz intuicyjnym i przyjaznym interfejsem. Ponadto określono zakres prac w ramach funkcjonowania platformy IoT, dokonano podziału na role i zakres obowiązków w zespole pracującym na platformie oraz rozpisano strukturę zadań.

Ważne było także określenie, jak zewnętrzne systemy mogą być integrowane z platformą IoT poprzez wykorzystanie API (Application Gateway) oraz oprogramowania BMS (Building Management System). Rozpatrywana była opcja użycia generycznego API lub serwisu domenowego dedykowanego konkretnemu przypadkowi biznesowemu.

Kluczowe obszary bezpieczeństwa wg Michaela Millera

Michael Miller w swojej obszernej pracy wskazuje na takie elementy systemów IoT, które są obszarem najbardziej narażonym na rozszczelnienie bezpieczeństwa systemu. Zauważa takie drażliwe obszary jak np. zasilanie w energie elektryczną, sposób zbierania i przechowywania danych, zakres odpowiedzialności za nie czy wykorzystywane w systemie normy i certyfikacje. Poniższa tabela jest zestawieniem pytań, na jakie według tego badacza należy odpowiedzieć podczas prac nad tego typu rozwiązaniami oraz odpowiedziami na nie zgodnie z założeniami projektowymi Lingaro, co stanowi swoistym jego opis[25].

[25] M. Miller, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat.* Warszawa 2016, PWN.

Tabela 1. Opis projektu Lingaro w kontekście kluczowych wg Micheal'a Millera zagadnień dotykających bezpieczeństwa systemu IoT.

Lp.	Pytanie	Odpowiedź
1	Czy rozwiązanie należy do większego ekosystemu, czy stanowi niezależne smart rozwiązanie?	Oprogramowanie platformy IoT Lingaro jest samodzielnym rozwiązaniem.
2	Jak zachowuje się rozwiązanie w przypadku braku energii elektrycznej?	W przypadku braku łączności z urządzeniem IoT z powodu braku prądu lub łączności, platforma zsynchronizuje wszelkie parametry zmienione w tym czasie przy pierwszym udanym połączeniu się z urządzeniem.
3	Jak zbierane są dane?	Urządzenia IoT komunikują się z Platformą IoT za pomocą bezpiecznych interfejsów udostępnionych w sieci Internet.
4	Z jakiej łączności korzysta rozwiązanie (radiowa, komórkowa, WiFi, Bluetooth, kablowa)?	Platforma IoT Lingaro dostarcza rozwiązanie softwarowe, urządzenia IoT podłączone do platformy muszą posiadać łączność z internetem bezpośrednio lub za pomocą urządzeń brzegowych.
5	Jakiego rodzaju dane zbiera system?	Wszelkie dane alfanumeryczne generowane przez urządzenia IoT.
6	Jak system przechowuje dane?	Dane są zbierane i przechowywane w bezpiecznym kontenerze danych ulokowanym w chmurze Microsoft Azure.
7	Jak system analizuje zebrane dane pod kątem opisania schematów działań, pewnych trendów czy wyłapania punktów krytycznych? Czy można z pozyskanych danych wyłapać dodatkowe, niekonieczne dla Lingaro, analizy?	Platforma IoT Lingaro jest rozwiązaniem typu self-service. Lingaro nie oferuje obsługi i analizy danych klienta jako część platformy. Klient ma możliwość tworzenia automatyzacji w postaci reguł i zależności między urządzeniami opartych na danych przez nie generowanych.
8	Co się dzieje z tymi danymi? Jak są przechowywane? – gdzie, na jak długo, kto ma do nich dostęp?	Dane zebrane z urządzeń są zapisywane i przechowywane w chmurze Azure i dostępne jedynie dla klienta poprzez samą platformą, API pozwalające na zintegrowanie z rozwiązaniami zewnętrznymi i automatyzację będące częścią platformy.
9	Kto bierze odpowiedzialność za bezpieczeństwo budynku monitorowanego przez system Lingaro?	Lingaro nie oferuje kompleksowej obsługi i ochrony budynków, dostarcza rozwiązanie softwarowe służące monitorowaniu i automatyzacji pracy urządzeń IoT. Platforma nie ogranicza się do urządzeń instalowanych w budynkach, ale może być wykorzystana do dowolnych urządzeń IoT.

Lp.	Pytanie	Odpowiedź
10	Jakie jest bezpieczeństwo użycia systemu Lingaro dla konsumenta?	Platforma jest oparta o sprawdzone i bezpieczne rozwiązania platformy chmurowej Microsoft Azure.
11	Jakie jest bezpieczeństwo przetwarzania danych? Jak są zabezpieczane dane osobowe? Czy jest plan na wypadek wycieku danych?	Platforma nie przechowuje danych osobowych, jedynie dane generowane przez urządzenia IoT.
12	Czy istnieje możliwość na szybkie i bez daleko idących konsekwencji odłączenie się od wdrożnego systemu?	Tak, komunikacja z urządzeniami IoT odbywa się za pomocą standardowych interfejsów.
13	Czy zanotowano przekłamania w agregacji danych i jeśli tak, to jak sobie z tym dano radę?	Platforma zbiera wszystkie dane generowane przez urządzenia. Agregaty jeżeli są wymagane, tworzone są dopiero na danych zgromadzonych wewnątrz platformy. Eliminuje to potencjalne problemy z jakością danych.
14	Czy system jest – i ewentualnie jak – zabezpieczony przed atakami z zewnątrz?	Urządzenia IoT łączą się platformą poprzez rozwiązania dostarczone przez Microsoft w ramach platformy Azure, zapewniając najwyższy poziom bezpieczeństwa i natychmiastowe łatanie potencjalnych problemów.
15	Czy system jest stabilny, powtarzalny i przewidywalny?	Zachowanie platformy jest w pełni determistyczne. Dostępność jest gwarantowana poprzez użycie platformy chmurowej Azure i redundancji elementów infrastruktury.
16	Czy system jest samouczący się?	Platforma IoT na tym etapie nie oferuje rozwiązań AI. Może być rozbudowana o moduły AI w zależności od potrzeb klienta.
17	Czy system oparty jest o jakiekolwiek standardy, normy i certyfikacje?	Platformy wykorzystują standard X.509 w celu zabezpieczenia komunikacji z urządzeniami IoT.
18	Kto produkuje urządzenia pozwalające na wykorzystanie systemu Lingaro?	Platforma nie wymaga dedykowanych urządzeń.

Źródło: opracowanie własne na podstawie książki Michela Miller (2016) i raportu Lingaro.

Wnioski i rekomendacje

Dynamiczny rozwój technologii IoT przybiera na sile. Z roku na rok wzrasta liczba podłączonych do sieci urządzeń komunikujących się wzajemnie. Każde nowe połączenie stanowi wrażliwy obszar dla bezpieczeństwa całego ekosystemu, jak i zbieranych w jego ramach danych. Równolegle do rozwoju tej technologii pojawia się nowe pole badawcze, jakim są luki w zabezpieczeniach. Są one integralnym zagadnieniem IoT. Pojawiają się w dyskursie technicznym, ekonomicznym i społecznym.

Podmioty zaangażowane w ich wyeliminowanie to obok twórców systemów IoT, naukowcy zajmujący się inżynierią bezpieczeństwa, regulatorzy państwowi czy decydenci polityczni. Walka z lukami to jednak proces permanentny, trwający tak długo, jak tylko będą pojawiać się nowe rozwiązania. Czym bardziej zaawansowany technologiczne system IoT, tym wymaga wyższego poziomu jego bezpieczeństwa oraz wyeliminowania większej liczby mankamentów, które mogą negatywnie wpływać na zachowanie bezpieczeństwa zarówno zbieranych danych, jak i funkcjonowania samego systemu.

Ważne jest utrzymanie stałego procesu tworzenia zasad i reguł ograniczających rozszczelnienie systemów IoT, np. poprzez utrzymywanie platformy dobrych praktyk branżowych umożliwiającej czerpanie z doświadczeń zebranych przez innych.

Istotnym elementem zachowania bezpieczeństwa systemów i danych jest edukacja społeczna w zakresie korzystania z IoT, w tym zrozumienie warunków przekazywania informacji związanych z preferencjami, oczekiwaniami czy możliwościami konsumentów i świadoma zgoda na ich analizowanie przez urządzenia systemu IoT. Ponadto kluczowe jest stałe aktualizowanie oprogramowania systemów zarządzania IoT. To nawyk, który musi posiąść każdy jego użytkownik.

Przed rozwojem IoT nie ma ucieczki. Pomnażane dzięki niemu BigData są kluczowym zasobem przemysłu 4.0. dającym poważne przewagi konkurencyjne. Nowoczesna gospodarka w coraz większym stopniu będzie zależna od komunikacji M2M (*Machine to Machine*).

Zakończenie

Rozwój technologii komunikacyjnych umożliwił wykorzystanie Internetu do łączenia nie tylko ludzi między sobą, ale także ludzi i maszyn oraz samych maszyn. „Obejmuje to wszystko, od telefonów komórkowych, ekspresów do kawy, pralek, słuchawek, lampek, urządzeń do noszenia i prawie wszystko, co można wymyślić. Dotyczy to również elementów maszyn, na przykład silnika odrzutowego samolotu lub wiertnicy platformy wiertniczej (...) jeśli ma on włącznik i wyłącznik, to jest szansa, że może być częścią Internetu rzeczy”[26].

Postęp, dzięki któremu ludzkość gromadzi, przechowuje i zaczyna wykorzystywać dostępne informacje, jest ogromny, a nasze skupienie na wyciąganiu jak największej wartości z ich analizy jest warte podkreślenia. I to właśnie ten trend wyznacza zdaniem badaczki M. Such-Pyrgiel „konieczność stwierdzenia, że społeczeństwo staje się cyfrowe, a nie już tylko informacyjne czy sieciowe. Oczywiście nie ma znaczenia, jaką przyjmiemy nazwę, ważniejsze jest, aby prowadzić ciągłą obserwację otaczającego nas świata i starać się go zrozumieć oraz wyciągnąć wnioski na przyszłość. Tak, abyśmy nie zatracili w tym wyścigu technologicznym swojego człowieczeństwa, aby technologie służyły nam w kreowaniu nowej, lepszej wartości”[27].

Trajektoria zmian współczesnego świata wskazuje, że obecnie wkraczamy w kolejną fazę rozwoju, od społeczeństwa informacyjnego, sieciowego, medialnego czy nawet społeczeństwa wiedzy, do ich cyfrowych form, do cyfrowego społeczeństwa informacyjnego, gdzie rozwój nowych technologii generuje postęp cywilizacji[28].

---

[26] M. Such-Pyrgiel, *Człowiek w dobie cyfrowej transformacji. Studium socjologiczne*, wyd. Adama Marszałek, Toruń 2019, s. 86–87, cyt. za Forbes, *A Simple Explanation Of 'The Internet Of Things*, 2014, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#298636371d09.

[27] M. Such-Pyrgiel, *Człowiek w dobie cyfrowej transformacji. Studium socjologiczne*, Toruń 2019, Wydawnictwo Adam Marszałek, s. 309.

[28] Ibidem, s. 306.

Bibliografia

Opracowania zwarte

Grodner M., Kokot W., Kolenda P., Krejtz K., Legoń A., Rytel P., Wierzbiński R., *Internet Rzeczy w Polsce*, Warszawa 2015, IAB.

Hassan F.Q., *Internet of Things A to Z: Technologies and applications*, Wiley-IEE Press 2018.

Miller M., *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016, PWN.

Sikorski M., Roman A. (red.), *Internet rzeczy* [w:] Real IT World, nr 1/2020, PWN.

Smith S., *The Internet of Riski Things. Trusting the Devices That Surround US*. O'Reilly Media, Inc., Sebastopol 2017.

Such-Pyrgiel M., *Człowiek w dobie cyfrowej transformacji. Studium socjologiczne*, Toruń 2019, Wydawnictwo Adam Marszałek.

Such-Pyrgiel M., Gołębiowska A., *Socio-economic and legal dimensions of digital transformation. Selected contexts*, Wydawnictwo SGSP 2021.

Szpunar M. (red.), *Paradoksy internetu. Konteksty społeczno-kulturowe*, Toruń 2011, Wyd. Adam Marszałek.

Szpunar M., *Imperializm kulturowy internetu*, Kraków 2017, IDMiKS UJ.

Szpunar M., *Kultura algorytmów*, Kraków 2019, IDMIKS UJ.

Artykuły

Abomhara M., Køien G.M., *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security*, 2015 4(1): 65–88. http://dx.doi.org/10.13052/jcsm2245-1439.414.

Ashton K., *That 'Internet of Things' Thing*, June 22, 2009. RFIDjournal-That Internet of Things Thing.pdf (itrco.jp).

Botta A., de Donato W., Persico V., Pescapé A., *Integration of Cloud computing and Internet of Things: A survey*, 2015.

Díaz M., Martín C., Rubio B., *State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing*, 2016.

Forbes, *A Simple Explanation Of 'The Internet Of Things*, 2014, https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#298636371d09.

Franceschi-Biccierai L., *The Looming Disaster of the Internet of (Hackable) Things*, 2016. Motherboard, November 7, 2016. Accessed April 10, 2017: https://motherboard.vice.com/en_us/article/the-looming-disaster-of-the-internet-of-hackable-things.

Greenberg A., Zetter L., *How Internet of Things Got Hacked*. w: *Wired*, December 28, 2015.

Hypponen M., Nyman L., *The Internet of (Vulnerable) Things: On Hypponen's Law, Security Engineering, and IoT Legislation* [in:] *Technology Innovation Management Review*, 2017 Vol. 7, Issue 4. HypponenNyman_TIMReview_April2017.pdf.

Li W., Santos I., Delicato F.C., Paulo F. Pires, Pirmez L., Weic W., Song H., Zomaya A., Khan S., *System modelling and performance evaluation of a three-tier Cloud of Things*, 2016.

Maj I., *Internet rzeczy i zagrożenia z nim związane*, w: *Bezpieczeństwo, Teoria i praktyka*, 2015 nr 3.

Malucha M., *Internet Rzeczy – kontekst technologiczny i obszary zastosowań* [w:] *Studia i Prace WNEIS US*, Uniwersytet Szczeciński, nr 54/2 2018. DOI: 10.18276/sip.2018.54/2-04.

Marszycki M., *Internet Rzeczy jednym z najszybciej rozwijających się obszarów polskiego rynku IT*, 14 kwietnia 2023, itwiz.pl, Internet Rzeczy jednym z najszybciej rozwijających się obszarów polskiego rynku IT | ITwiz.

Patton M., Gross E., Chinn R., Forbis S., Walker L., Chen H., *Uninvited Connections: A Study of Vulnerable Devices on the Internet of Things (IoT)*, September, 24-26, 2014. https://doi.org/10.1109/JISIC.2014.43.

Puślecki W.Z., *Sztuczna inteligencja (AI), Internet Rzeczy (IoT) i sieć piętej generacji (5G) w nowoczesnych badaniach naukowych* [w:] *Człowiek i społeczeństwo*, 2021 T. LII. bmrowicka,+{$userGroup},+06-Puslecki.pdf.

Rot A., Blaicke B., *Bezpieczeństwo internetu rzeczy. Wybrane zagrożenia i sposoby zabezpieczeń na przykładzie systemów produkcyjnych* [w:] *Zeszyty Naukowe Politechniki Częstochowskiej, Zarządzanie*, 2017 Nr 26, s. 188–198.

Rot A., Blaicke B., *Zagrożenia wynikające z implementacji koncepcji internetu rzeczy w wybranych obszarach zastosowań*, w: *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, 2017 Nr 341.

Schneier B., *The Internet of Things is Wildly Insecure – and Often Unpatchable*, January 6, 2014. Essays: The Internet of Things Is Wildly Insecure—And Often Unpatchable – Schneier on Security.

Such-Pyrgiel M. (2021), *Nowe technologie edukacyjne w dobie cyfrowej transformacji – wybrane konteksty* [w:] *Bezpieczeństwo w dobie cyfrowej transformacji – aspekty prawne, organizacyjne i społeczne*, Wydawnictwo SGSP.

Such-Pyrgiel M., *Fourth industrial revolution, new communication technologies and the human right to good administration* [w:] *Crisis as a challange for human rught, Bratysława*, 2020, s. 447–462.

Gołębiowska A., Such-Pyrgiel M., Prokopowicz D., *The postpandemic reality and the security of information technologies ICT, Big Data, Industry 4.0, social media portals and the Internet*, 2022, Journal of Modern Science 42/2022 vol. 49, ss. 10–43, ISSN 17342031.

Such-Pyrgiel M., Gołębiowska A., Prokopowicz D., *The role of Big Data and Data Science in the context of information security and cybersecurity*, Journal of Modern Science 4/2023 vol. 53, s. 9–42, ISSN 17342031.

Such-Pyrgiel M. (2018), *Nowe modele biznesu w dobie transformacji cyfrowej* [w:] Sitek M., Such-Pyrgiel M. (red.), *Społeczne i ekonomiczne aspekty zarządzania w organizacjach przyszłości*, Wyd. WSGE, Józefów 2018, ISBN 978-83-62753-95-6, s. 39–56.

Szpunar M., *Pomiędzy antropomorfizacją maszyn a technomorfizacją człowieka* [w:] *Journal of Modern Science*, 2023 nr 3, s. 24–38.

Dokumenty

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 206/679 z dn. 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE. Rozporządzenie 2016/679 (RODO) i akty towarzyszące – UODO.

IERC (2015) *Internet of Things. Position Paper on Standarization for IoT technologies*, European Research Cluster on the Internet of Things, January, 2015.

Raporty

Analiza funkcjonowania rynku usług telekomunikacyjnych w Polsce oraz ocena preferencji konsumentów. 2022 rok. Badanie klientów indywidualnych. (15.11.2022) IBC Advisory S.A. Sektor Publiczny.

Exploding Topics, *Number of IoT Devices*, Number of IoT Devices (2023–2030) (explodingtopics.com), 2023.

IoT Market by Component (hardware, Software Solutions and Services), Organization Size, Focus Area (Smart Manufacturing, Smart Energy and Utilities, and Smart Retail) and Region – Global Forecats to 2026. (2022) Feb 2022, by marketsandmarkets.com, Internet of Things (IoT) Market Size, Statistics, Trends, Forecast, Industry Report -2030 (marketsandmarkets.com).

Precedence Research, *Industrial IoT Market (By Component: Solution, Services, Platform; By End-Use: Manufacturing, Energy & Power, Oil & Gas, Healthcare, ogistics & Transport, Agriculture, Others) – Global Industry Analysis, Size, Share, Growth, Trends, Regional Outlook, and Forecast 2023-2032*, Industrial IoT Market Size To Surpass USD 1,562.35 Bn By 2032 (precedenceresearch.com) 2022.

Raport z realizacji badań w ramach Zadań numer 2 i 4. Dobór i optymalizacja narzędzi, algorytmów, IoT Hub urządzeń i rozwiązań do zbierania i przetwarzania danych, Opracowanie własne, Warszawa 2023, Lingaro Sp. z o.o.

Rynek Internetu Rzeczy w Polsce w 2023. Analiza rynku i prognozy rozwoju na lata 2023–2028. Wpływ inflacji i wojny w Ukrainie, PMR Market Experts. Rynek internetu rzeczy w Polsce 2023 | PMR Market Experts (mypmr.pro).

Strony internetowe i kanały filmowe

Stacey on IoT: www.staceyoniot.com

Altop: www.internet-of-things.alltop.com

TechCrunch: www.techcrunch.com

Venture Beat: http://venturebeat.com

Profil YouTube: Venture Beat

Profil ouTube: IoT One.